ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA SCIENTIARUM MATHEMATICARUM

TOMUS 50

FASC. 3—4

SZEGED, 1986

INSTITUTUM BOLYAIANUM UNIVERSITATIS SZEGEDIENSIS

A JÓZSEF ATTILA TUDOMÁNYEGYETEM KÖZLEMÉNYEI

ACTA SCIENTIARUM MATHEMATICARUM

50. KÖTET

FASC. 3—4

SZEGED, 1986

JÓZSEF ATTILA TUDOMÁNYEGYETEM BOLYAI INTÉZETE

Acta Sci. Math., 50 (1986), 253—286

Abstract Galois theory and endotheory. I

MARC KRASNER

Introduction

Let us consider the situation in the classical Galois theory. Then we have a field extension K/k which is either normal and algebraic or algebraically closed. A permutation $\sigma\colon K\to K$ is called an *automorphism* of K/k if, for each $a, b\in K$ and $\alpha\in k$, we have

(1) $$\sigma\cdot(a+b)=\sigma\cdot a+\sigma\cdot b,$$

(2) $$\sigma\cdot ab=(\sigma\cdot a)(\sigma\cdot b),$$

and

(3) $$\sigma\cdot\alpha=\alpha.$$

Observe that the assumption "bijective" can be replaced by the weaker one "*surjective*", i.e., the automorphisms of K/k are just the surjective mappings $\sigma\colon K\to K$ satisfying (1), (2) and (3). This observation follows readily from the fact that fields have no non-trivial ideals.

The automorphisms of K/k are known to form a group under the composition of mappings. This group, denoted by $G(K/k)$, is called the *Galois group* of K/k. Let A be a subset of K and let $G(K/k;A)$ denote $\{\sigma\in G(K/k);(\forall a\in A)(\sigma\cdot a=a)\}$, which is a subgroup of $G(K/k)$. Then $\bar{A}_k=\{\bar{a}\in K;(\forall\sigma\in G(K/k;A))(\sigma\cdot\bar{a}=\bar{a})\}$, the set of all elements in K preserved by each $\sigma\in G(K/k;A)$, is called the *Galois closure* of A. The classical Galois theory asks and answers the following two questions:

(a) How to characterize $\bar{A}_k$ in terms of A and the field extension structure $(K;x+y,xy,k)$ of K/k? Answer: $\bar{A}_k$ is the closure of $A\cup k$ with respect to the operations $x+y$, xy (defined on $K\times K$), x^{-1} (defined on $K\setminus\{0\}$) and, if the characteristic p of k is not zero, $\sqrt[p]{x}$ (defined on $K^p=\{a^p;a\in K\}$).

Received January 6, 1982. The original version of the paper was revised by the referee. The author could not be asked to agree to the modifications as he passed away in 1985.

(b) Which subgroups of $G(K/k)$ are "Galoisian", i.e. of the form $G(K/k; A)$ for some $A \subseteq K$? When the degree $[K:k]$ is finite then the answer is: all subgroups.

Conditions (1), (2) and (3) in defining automorphisms seem heterogeneous at the first sight since (1) and (2) concern the preservation of some binary operations while (3) concerns the preservation of some elements. Yet, these conditions turn out to be of the same nature when formulated in terms of relations. There are two manners of defining the automorphisms of K/k in this way:

I. An automorphism of K/k is a permutation σ of K such that

$$(\alpha)\ a+b = c \Leftrightarrow \sigma\cdot a+\sigma\cdot b = \sigma\cdot c,$$

$$(\beta)\ ab = c \Leftrightarrow (\sigma\cdot a)(\sigma\cdot b) = \sigma\cdot c, \text{ and}$$

$$(\gamma) \text{ for each } \alpha\in k,\ a = \alpha \Leftrightarrow \sigma\cdot a = \alpha.$$

We can formulate Conditions (α), (β) and (γ) by saying that σ preserves the relations $x+y=z$, $xy=z$ and, for each $\alpha\in k$, $x=\alpha$, where σ is said to preserve a, say ternary, relation ϱ if for any triple $(a, b, c)\in K^3$ we have $(a, b, c)\in\varrho \Leftrightarrow (\sigma\cdot a, \sigma\cdot b, \sigma\cdot c)\in\varrho$.

II. An automorphism of K/k is a self-surjection μ of K such that

$$(\alpha')\ a+b = c \Rightarrow \mu\cdot a+\mu\cdot b = \mu\cdot c,$$

$$(\beta')\ ab = c \Rightarrow (\mu\cdot a)(\mu\cdot b) = \mu\cdot c, \text{ and}$$

$$(\gamma') \text{ for each } \alpha\in k,\ a = \alpha \Rightarrow \mu\cdot a = \alpha.$$

If we drop the condition that μ is surjective and consider self-mappings of K satisfying (α'), (β') and (γ') then we obtain the notion of *endomorphisms* of K/k. It is not hard to show that all the endomorphisms of K/k are automorphisms, provided K/k is normal and algebraic. But in the general case the endomorphisms of K/k form only a monoid, i.e. a unitary semigroup, $D(K/k)$ with respect to the composition of mappings. This monoid always contains 1_K, the identical mapping of K. As previously, $D(K/k, A)$ will denote the set $\{\delta\in D(K/k); (\forall a\in A)(\delta\cdot a=a)\}$, which is a submonoid of $D(K/k)$. Further, it can be proved that $\{\bar{a}\in K; (\forall\delta\in D(K/k))(\delta\cdot\bar{a}=\bar{a})\}$ is the closure of $A\cup k$ with respect to the operations $x+y$, xy, x^{-1} and, if $p\neq 0$, $\sqrt[p]{x}$, as before.

We can formulate Conditions (α'), (β') and (γ') by saying that δ *stabilizes* the relations $x+y=z$, $xy=z$ and, for each $\alpha\in k$, $x=\alpha$, i.e. δ transforms every system of values satisfying any of these relations into a system of values satisfying the same relation, but nothing is required for systems of values not satisfying these relations.

In both of these manners we have a particular case of the following general situation: given a relational system, i.e. a base set A (here $A=K$) and some relations on it (here $x+y=z$, $xy=z$ and $x=\alpha$ for $\alpha\in k$). (In the sequel relational systems will be referred to as *structures* though the term "structure" has a more general meaning in the literature.) We consider the group G of all permutations of the base set preserving the given relations and the monoid D of self-mappings of this set stabilizing these relations. Then in Question (a) we asked what was the set of relations of a certain form (in our case $x=\bar{a}$ for $\bar{a}\in K$) preserved by all $\sigma\in G$ and stabilized by all $\delta\in D$? The answer was that it is the set of relations $x=\bar{a}$ where $\bar{a}$ belongs to the closure of $A\cup k$ with respect to some operations arising from the relations $x+y=z$ and $xy=z$.

The above considerations naturally raise the idea of considering any first order structure E/R where R is a set of (not necessarily finitary) relations on a base set E, the *automorphism group* alias *Galois group* G of E/R (consisting of all permutations of E that preserve each $r\in R$), and the *endomorphism monoid* alias *stability monoid* of E/R (consisting of all self-mappings of E stabilizing each $r\in R$). Then the question analogous to (a) is how to characterize the relations on E that are preserved by all $\sigma\in G$ or that are stabilized by each $\delta\in D$, respectively. Of course, we want the answer be somewhat similar to that in the classical Galois theory. Therefore the answer should be (and, in fact, will be) that they are the relations belonging to the closure of R with respect to some appropriate operations. But, first of all, all such relations do not form a set because any set occurs among their argument sets. So, at least in the first study, we have to limit the argument sets of the considered relations so that we fix a set X^0 (of sufficiently large cardinality) and consider the relations whose argument sets are subsets of X^0. On the other hand, we cannot hope in this general situation that the sets

$$\bar{R}(X^0)=\{r;\ r\subseteqq E^X \text{ for some } X\subseteqq X^0 \text{ and each } \sigma\in G \text{ preserves } r\}$$

and

$$\bar{\bar{R}}(X^0)=\{r;\ r\subseteqq E^X \text{ for some } X\subseteqq X^0 \text{ and each } \delta\in D \text{ stabilizes } r\}$$

are the closures of R with respect to some operations on the base set E arising from the relations $r\in R$. A priori, it may be hoped only that $\bar{R}(X^0)$ and $\bar{\bar{R}}(X^0)$ are closures of R with respect to some set theoretical operations on relations and these operations do not depend on the particular choice of R. Such is the case, indeed: there exists a family of such operations, called *fundamental operations*, so that $\bar{R}(X^0)$ is the closure (within the set of relations with argument sets included in X^0) of R with respect to these operations while $\bar{\bar{R}}(X^0)$ is the closure of R with respect to a part of this family, called the family of *direct fundamental operations*. The theory concerning the preservation of relations by permutations of the base set and the Galois group is called *abstract Galois theory* while that dealing with the stability of relations by arbitrary self-mappings of E and with the stability monoid is called *abstract Galois endotheory*. Although Question (a) has the same answer for both theories in the classical Galois theory, it has quite different answers in the general case. Question (b) in the general case asks: which permutation groups on E are the Galois groups of appropriate structures E/R and which monoids of self-mappings of E are endomorphism monoids of some structures E/R? The answer is that *any* group and *any* monoid on E are such.

Once this study with a fixed X^0 has been done we can introduce the classes $\bar{R}$ and $\bar{\bar{R}}$ of *all* relations preserved by each $\sigma \in G$ and stabilized by each $\delta \in D$, respectively, and we can study them in a non-axiomatic way. In the present paper we will do it roughly within the frame of Bernays—Gödel axiomatic set theory albeit this is not the only possibility. On the deep analogy of the terminology of classical Galois theory, the classes $\bar{R}$ and $\bar{\bar{R}}$ will be called *abstract fields* and *abstract endofields*, respectively. With some precaution, it is possible to consider and to study certain mappings between them. In particular, a bijection of an abstract field or endofield onto another one (with a different base set in general) which commutes with all fundamental operations is called an isomorphism. It will be proved that any isomorphism between abstract fields or, under certain conditions, between abstract endofields is of a special form called transportation of structures. After these so-called isomorphism theorems the notion of abstract endofield homomorphisms is also introduced and a much more difficult homomorphism theorem is proved in order to characterize these homomorphisms.

Let k be an abstract endofield (which may be, in particular, an abstract field), and let A be a subset of the corresponding base set E. Denote by $k(A)$ the endo-extension of k by the set of relations $\{x=a;\ a \in A\}$, i.e., the abstract endofield generated by $k \cup \{x=a;\ a \in A\}$. Then $k(A)$ does not depend on the particular choice of x. Such extensions $k(A)$ of k are called its *set extensions*, and their study is called *abstract Galois set theory*. A theorem is proved, which describes the relations in $k(A)$ in terms of A and the relations in k. As a consequence of this theorem, a family of partial operations on E is defined from k such that $\bar{A}_k = \{e; (x=e) \in k(A)\}$, the so-called *rationality domain* of $k(A)$, is just the closure of A with respect to these partial operations. This result can be considered as the first step of deducing the answer to (a) in the classical Galois theory from that given in the general Galois theory. The second step is the theory of "eliminating structures", which will not be exposed in this paper. The third step starts from the main result of the second one and allows us to understand and to foreseee the deep reasons why $\bar{A}_k$ is the closure of $A \cup k$ with respect to $x+y$, xy, x^{-1} and $\sqrt[p]{x}$ in the classical Galois theory.

While dealing with the theory concerning $\bar{R}(X^0)$ and $\bar{\bar{R}}(X^0)$ then X^0 is of sufficiently large cardinality means that card $X^0 \geqq$ card E. In particular, when the base set E is finite, we can take a finite X^0. Then the fundamental operations become the realisations of operations in the (first order) predicate calculus with equality for

X^0 as the set of object variables on the model E/R. Similarly, the direct fundamental operations are just the realizations of a "strongly positive" part of this calculus, which is generated by $\vee$, &, $\exists x$ for $x \in X^0$, adjunctions of variables belonging to X^0, equalities $x_i = x_j$ ($x_i, x_j \in X^0$, $x_i \neq x_j$), and the identity. So in the general case the fundamental operations can be considered as infinitary generalizations of the previous finitary operations.

Except for certain points our approach is independent from the axiom of choice, but this is not the case for the afore-mentioned theory of "eliminating structures".

In Section 1 we give the precise notions of points, relations, structures, etc., define the action of mappings of the base set on them, and introduce the Galois group, the stability monoid and their "invariants". The fundamental operations are defined and studied in Section 2. In Section 3 we study the interaction between mappings (and, in particular, self-mappings) of base sets and fundamental operations. In Section 4 we prove the main theorems, i.e. the equivalence and existence theorems, of the abstract Galois theory and endotheory, but considering only relations whose argument sets are included in some fixed set X^0 such that card $X^0 \geqq$ card E. In Section 5 we introduce the abstract fields and endofields, study their mappings and, in particular, prove isomorphism and homomorphism theorems. Finally, Section 6 is devoted to the abstract Galois set theory.

Historical remarks. I found the abstract Galois theory during the summer vacation of 1935, submitted it to the jubelee volume of Journal des mathématiques pures at appliquées dedicated to J. Hadamard in 1936, and this first exposition [1] of the theory appeared in 1938. It is the following question that was the intuitive origin of this research: Let $z_1, \ldots, z_n$ be the roots of a polynomial $f(X)$ of degree n over some base field k, and let G be the Galois group of $f(X)$; how can the system of equations satisfied by the n-tuples $(\sigma \cdot z_1, \ldots, \sigma \cdot z_n)$ $(\sigma \in G)$, and only by these n-tuples, be obtained from the rational relations among the roots $z_1, \ldots, z_n$? (This situation is somewhat obscured in the usual treatments of the classical Galois theory because of the use of the so-called "Galois resolvent", i.e. the replacement of the n-tuple $(z_1, \ldots, z_n)$ by a convenient linear combination $\xi = \Sigma \lambda_i z_i$ $(\lambda_i \in k)$ of z_i, and, in more modern treatments, because of the emphasis put on the field structure and the normal case.) This question led me to the fundamental operations and gave me the key idea to the proof of the equivalence theorem, i.e., the idea of considering the relation r^* (cf. Section 4, later).

This theory, as elaborated in a set theoretical frame, had certainly no precursors. Yet, it might be connected with some vague ideas or projects expressed before in much narrower contexts. A rather enigmatic phrase in the last letter by Galois to his friend Auguste Chevalier ("Tu sais, mon cher Auguste que ces sujets ne sont pas les seuls que j'aie explorés. Mes principales méditations depuis quelque temps étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté. Il s'agissait de voir à priori dans une relation entre les quantités ou fonctions transcendantes quelles échanges on pouvait faire, quelles quantités on pouvait substituer aux quantités données sans que la relation pût cesser d'avoir lieu. Cela fait reconnaître tout de suite l'impossibilité de beaucoup d'expressions que l'on pourrait chercher. Mais je n'ai pais le temps et mes idées ne sont pas bien développées sur ce terrain, qui est immense") suggests that he had a vague feeling that his theory for roots of polynomial equations is, maybe, only a particular case of a much wider theory, where the polynomial relations among roots are replaced by some more or less arbitrary relations on convenient domains. Clearly, these domains and relations could be only as general as conceivable for him and his contemporaries. However, the mathematics of that time was not set theory but a science of magnitudes, i.e., of real and complex numbers and sufficiently smooth functions (in the quoted phrase Galois speaks, among others, of the "quantités ou fonctions transcendantes"), and the relations used in this mathematics were differential, functional, etc. equations and systems of equations. Some people see, in this phrase, an allusion to what he knew about abelian functions. But if it had been so, he would not have spoken of his "méditations" and he certainly would not have written "cela faît reconnaitre tout de suite l'impossibilité de *beaucoup* d'expressions ..."; in fact, he would have spoken rather of the results known by him.

Cayley and Silvester's theory of invariants may be considered as a vague precursor of the abstract Galois theory in some very particular case. Indeed, if A is an invariant of some "generic" form (i.e., its coefficients are independent variables), a is a value of A, and the set of all points (in some field) of all projective varieties for which a is the value of A is assigned to a, then this set of points is preserved by all elements of the projective group or some of its subgroups. So, an invariant A can be interpreted by the set $\{r_{A,a}\}$ consisting of relations of the form $r_{A,a}$ which are invariant with respect to some (very particular) groups. Remarkably enough, Cayley raised the problem of determining *all* the invariants. Yet, he could not consider the definition of these groups as that of Galois groups with respect to a system of invariants.

The "Galois type theories" which appeared for differential equations at the end of the nineteenth century (S. Lie, Picard—Vessiot, etc.) can hardly be considered as the beginning of the abstract Galois theory because they were developed, like the classical Galois theory, by using quite particular methods, specific for each case and without any more general spirit. Nevertheless they created a vague feeling that Galois' ideas were, in some unknown manner, applicable in a wider framework.

In some very faint sense the abstract Galois theory for arbitrary (first order) structures can be considered analogous to F. Klein's "Erlangener Programm" for geometries (1872), though the former goes far beyond this program. Klein's main idea is that a geometry is a system of "all invariants" of an "arbitrary" permutation group of a "Mannigfaltigkeit" ("variety"). As no set theory existed that time (the first results on abstract sets were obtained by Cantor in 1873), Klein could not express his ideas in a precise manner. In particular, he did not give any precise meaning of "all invariants" of "Mannigfaltigkeit" (which seems to be a riemannian variety or something stronger), and his "arbitrary" groups are far from being arbitrary as their elements must be automorphisms of the structure of "Mannigfaltigkeit". Anyhow, though the abstract Galois theory deals with the duality between permutation groups and classes of their invariant relations, it is much more than a simple idea of this duality.

In my first paper [1] on abstract Galois theory the fundamental operations are defined almost in the same way as in this paper, but in a rather misleading manner: *instead of arbitrary argument sets canonical argument sets, indexed by ordinals,* are used, whence the axiom of choice is widely used without real necessity. In later publications ([2] and other papers, which I do note quote) I only formulated the results of the theory in a clearer form by using canonical identifications (cf. Section 3 later), but without giving new proofs because of those in [1] being easily adaptable to the new manner. There the essential part of the theory is developed for relations with a fixed, sufficiently large (i.e., of cardinality not smaller than card E) argument set X. The defect of this approach is that certain rather complicated and not very intuitive fundamental operations (called "mutations") have to be considered as well. That is why I return to the first manner, but without its past imperfections.

I found the abstract Galois endotheory, if my memory is good, in 1964, and formulated it in printed form first in the paper [3] of the International Congress of Mathematicians, Moscow, 1966. I found the first but not completely true version of the homomorphism theorem of this theory in 1966, before the above-mentioned congress. The gap in its proof was remarked by some my 3rd year students in 1973, After having tried to fill this gap unsuccessfully I found the necessary modification which made the theorem correct, i.e., I replaced norms by regular pseudo-norms, and published it in [5]. Yet, until the present paper, the abstract Galois endotheory (even without its homomorphism theorem) has never been published with complete proofs. Only some rough ideas of certain proofs were indicated in [4].

The idea of abstract Galois set theory (in relation with eliminative structures and the passage from the abstract Galois theory to the classical one) goes back as early as to the end of thirties. However, the proof of its main theorem was put in a clear form only in the first years after the second world was (1946? 1947?). This theorem and the characterization of rationality domains (in case of abstract fields) were formulated in several papers, but never with proofs. I exposed the abstract

Galois theory and, after it had come to existence, the abstract Galois endotheory in my Seminar (1953—1959) and in my courses for 3rd year students (Clermont-F^d, 1960—1965, and Paris, 1965—1980).

Terminology and notations. We shall use the ordinary notations of set theory and mathematical logic. The set difference $\{x\in A;\ x\notin B\}$ will be denoted (in Russian manner) by $A\setminus B$, though personally I prefer the notations $A\cdot\cdot B$ or $A\urcorner B$ to $A\setminus B$ as they cannot interfere with algebraic notations. When $a\in A$, $\bar{A}\subseteqq A$ and $\varphi\colon A\to B$ is a mapping, the φ-image of a and $\bar{A}$ will be denoted by $\varphi\cdot a$ and $\varphi\cdot\bar{A}$, respectively. This will be the only mathematical use of the dot "$\cdot$". The product of two objects, say x and y, will be denoted by xy. Similarly, the composition of mappings ψ and φ will be denoted by $\varphi\psi$ or sometimes, following Bourbaki's notation, by $\varphi\circ\psi$. The mappings $\psi\colon C\to D$ and $\varphi\colon A\to B$ are considered composable iff $\varphi\cdot A\subseteqq C$; in this case $\psi\varphi$ (or $\psi\circ\varphi$) is the mapping $A\to D$ such that $\psi\varphi\cdot a= =\psi\cdot(\varphi\cdot a)$ for every $a\in A$. If $\varphi\colon A\to B$ is a mapping, $a\in A$ and $b=\varphi\cdot a$, then we write $\varphi\colon a\to b$ if a is an arbitrary element of A while $\varphi\colon a\mapsto b$ is reserved for the case of fixed a. The equivalence relation $\{(x,y);\ \varphi\cdot x=\varphi\cdot y\}$ on A, referred to as the kernel of φ in the literature, will be called the *type* of φ and will be denoted by $T(\varphi)$. If $\varphi\colon A\to B$ is a mapping and C is an equivalence relation on A then φ is said to be *compatible* with C iff $T(\varphi)$ is thicker than C, i.e., iff $x\equiv y \pmod C$ always implies $x\equiv y \pmod{T(\varphi)}$. Similarly, a mapping $\gamma\colon A\to C$ is called compatible with a mapping $\beta\colon A\to B$ iff it is compatible with $T(\beta)$, i.e., if for every $a\in A$ the image $\gamma\cdot a$ depends only on $\beta\cdot a$.

Let F and G be two families of subsets of A and B, respectively, and suppose F and G are complete semilattices with respect to the union $\bigcup$. Consider a mapping $\Phi\colon F\to G$. This mapping is said to be *additive* if $\Phi\cdot\bigcup_{X\in\bar{F}}X=\bigcup_{X\in\bar{F}}\Phi\cdot X$ holds for every subfamily $\bar{F}$ of F, i.e., if Φ commutes with the operation $\bigcup$. If $\Phi\colon F\to G$ is additive and, in addition, F is the family of all subsets of some subset $\bar{A}$ of A, then Φ is called $\bar{A}$-*hyperpunctual*. Then we have $\Phi\cdot X=\bigcup_{x\in X}\Phi\cdot\{x\}$ for $X\subseteqq\bar{A}$, and we shall write $\Phi\cdot x$ instead of $\Phi\cdot\{x\}$. If $\Phi\colon F\to G$ is an $\bar{A}$-hyperpunctual mapping and the image $\Phi\cdot\{x\}$ of any singleton in F is a singleton (denoted by $\{\varphi\cdot x\}$) in G, then Φ is called *punctual* and the mapping $\bar{A}\to B$, $x\to\varphi\cdot x$ is called the *point-mapping* of Φ. If φ is injective, Φ is called an *injectively punctual* mapping. Then φ induces a bijection φ^0 of $\bar{A}$ onto $\varphi\cdot\bar{A}\subseteqq B$, and if Φ^0 is the mapping of the family $P(\bar{A})$ of all subsets of $\bar{A}$ onto $P(\varphi\cdot\bar{A})$ which prolongs φ^0 (i.e., induced by Φ), then Φ^0 clearly commutes with all boolean operations. So, if $\bar{P}$ is a subfamily of $P(\bar{A})$, we have

$$\Phi\cdot\bigcup_{X\in\bar{P}}X=\Phi^0\cdot\bigcup_{X\in\bar{P}}X=\bigcup_{X\in\bar{P}}\Phi^0\cdot X=\bigcup_{X\in\bar{P}}\Phi\cdot X,$$

$$\Phi\cdot\bigcap_{X\in\bar{P}}X=\Phi^0\cdot\bigcap_{X\in\bar{P}}X=\bigcap_{X\in\bar{P}}\Phi^0\cdot X=\bigcap_{X\in\bar{P}}\Phi\cdot X$$

and, for $X \subseteq \bar{A}$,

$$\Phi \cdot (\bar{A} \setminus X) = \Phi^0 \cdot (\bar{A} \setminus X) = \varphi \cdot \bar{A} \setminus \varphi \cdot X = \Phi \cdot \bar{A} \setminus \Phi \cdot X.$$

Sometimes, in order to define certain notions or to formulate certain results with elegance and well, we shall have to deal not only with sets but with classes as well. This will be done only for the sake of convenience and better understanding, but not for raising any question of Foundations. In fact, all we do could be done in the language of sets, though in a longer and more complicated way. In principle, the word "class" will be understood in Bernays' sense*) but in a freer and more naive manner of speaking. However, as it can be shown, this manner of speaking is only an "abuse of the language" from the point of view of Bernays' theory, since the existence of classes and their mappings occurring in this paper can be proved based on Bernays—Gödel axioms.

1. Relations, structures and mappings

Let E and X be two sets called *base set* and *argument set*, respectively. Generally, for the sake of some of the proofs, we assume that E consists of at least two elements, though our results are trivially valid for a one-element base set E, too. The elements of E^X are called *X-points* while subsets of E^X are called *X-relations*. I.e., X-points are mappings of X into E (denoted by, e.g., $P: X \to E$ or $X \xrightarrow{P} E$) and X-relations are sets of such points. When there is no danger of ambiguity, we often do not indicate the argument set X. An (ordered) pair $S = (E, R)$ is called a (first order) *structure* on E (or *with base set* E) provided R is a non-empty set of relations on E. (The argument set X_r of $r \in R$ may depend on r.) In particular, when all the relations in R have the same argument set, say X, then $S = (E, R)$ is called an *X-structure*. By the *arity* of an X-point, X-relation or X-structure we mean the cardinal $\operatorname{card} X$ of X. We say that a structure $S = (E, R)$ is *under* a set X^0 if $X_r \subseteq X^0$ for all $r \in R$.

Let $d: E \to E'$ be a mapping between the sets E and E'. This mapping can be extended to points, relations, sets of relations and structures on E in the following evident way: put $d \cdot P = d \circ P$ (Bourbaki's notation!), $d \cdot r = \{d \cdot P;\ P \in r\}$, $d \cdot R = \{d \cdot r;\ r \in R\}$, $d \cdot (E, R) = (E', d \cdot R)$. In particular, when δ is a self-mapping of E (i.e. $E' = E$), we say that δ *stabilizes* a relation r on E (or, in other words, r is *stable* by δ) iff $\delta \cdot r \subseteq r$. We say that a permutation σ of E *preserves* r (in other

*) But this does not mean that I consider the foundation of mathematics based on the Bernays—Gödel axioms (and, generally, based on any predicative calculus formalism) as an adequate one.

words, r is *preserved* by σ or *invariant* by σ) iff $\sigma \cdot r = r$. More generally, a self-mapping δ of E is said to preserve r iff it stabilizes both r and its complement $E^{X_r} \setminus r$. We say that δ is *stabilizing* or *preserving on* a set R of relations if it stabilizes or preserves each $r \in R$, respectively. For a structure $S=(E, R)$ the set of all self-mappings of E that are stabilizing on R constitutes a monoid with respect to the composition of mappings. This monoid is called the *stability monoid* or *endomorphism monoid* of E/S (or S), and it is denoted by $D(E/S)$ or, sometimes, by $D(E/R)$. The endomorphism monoid is never empty for it always contains the identical mapping of E. The set of all permutations of E that are preserving on R is called the *Galois group* or *automorphism group* of E/S (or S) and is denoted by $G(E/S)$ or $G(E/R)$.

Remark 1. $G(E/S)$ is the largest permutation group contained in $D(E/S)$. Indeed, a permutation σ belongs to $G(E/S)$ iff σ and σ^{-1} belong to $D(E/S)$, whence the assertion follows.

Remark 2. Suppose R is a set of relations on E such that $r \in R$ implies $\neg r = E^{X_r} \setminus r \in R$. Then $G(E/S)$ consists of the permutations that belong to $D(E/S)$. This remark is a straightforward consequence of the definitions.

Particular relations. Firstly, we mention the *empty relation* $\emptyset$, which is the only relation without a unique argument set and base set. I.e., $\emptyset$ can be considered an X-relation on E for any X and E. The *X-identity* on E is E^X and is also denoted by $I(X, E)$. Let C be an equivalence relation on X. Then

$$I_C(E) = \{P \in E^X;\ (\forall x \in X)(\forall x' \in X)(x \equiv x' \pmod{C} \Rightarrow P \cdot x = P \cdot x')\}$$

is called the *C-multidiagonal* on E. It consists of all X-points that are compatible with C. In particular, if $\bar{X} \subseteqq X$ is a C-class and all C-classes but $\bar{X}$ are singletons then

$$D_{\bar{X}}(E) = I_C(E) = \{P \cdot E^X;\ (\forall x \in \bar{X})(\forall x' \in \bar{X})(P \cdot x = P \cdot x')\}$$

is called the $\bar{X}$-diagonal of E. When $\bar{X} = \{x, y\}$,

$$D_{x,y}(E) = D_{\{x,y\}}(E) = \{P \in E^X;\ P \cdot x = P \cdot y\}$$

is called the (x, y)-diagonal on E, and such diagonals are called *simple*. The relation

$$I_C^0(E) = \{P \in I_C(E);\ T(P) = C\}$$

is called the *strict C-multidiagonal* on E, while $E^X \setminus I_C(E)$ is referred to as the C-antidiagonal on E.

A relation r will be called *semi-regular* iff there exists an equivalence relation C on its argument set X such that $r \subseteqq I_C(E)$ and $C = T(P)$ for some $P \in r$. When r is semi-regular then this C is unique, is denoted by $T(r)$, and is called the type of r. Further, $t(r) = \{P \in r;\ T(P) = T(r)\}$ is called the *head* of the semi-regular relation r. If $r \subseteq I_C^0(E)$ for some C, i.e. r is semi-regular and $r=t(r)$, then r is said to be *regular*.

An X-point $P\colon X \to E$ is said to be *surjective, injective* and *bijective* if it is such as a mapping, while a relation r is said to be such if every $P \in r$ is such. In particular, r is injective iff it is regular and $T(r)$ is the discrete equivalence relation on X.

In case $X=\emptyset$ there is only one $\emptyset$-point $P_\emptyset(E)\colon \emptyset \to E$ (indeed, no two mappings can differ at any argument belonging to $\emptyset$). Hence there are only two $\emptyset$-relations: $\emptyset$ and $I(\emptyset, E)=\{P_\emptyset(E)\}$.

Let $D(E)$ denote the monoid consisting of all self-mapping of E, called the *symmetric monoid* of E, and let $S(E)$ stand for the (full) *symmetric group* of E, consisting of all permutations of E. For a subset Δ of $D(E)$ the *class* of all relations on E that are stabilized resp. preserved by each $\delta \in \Delta$ will be denoted by s-Inv Δ resp. p-Inv Δ, and will be called the *stability invariant* resp. *preservation invariant* of Δ. (Note that these classes are never sets.) When the context shows clearly what kind(s) of invariants is considered, the letters s or p before Inv may be omitted. Clearly, the mappings $\Delta \mapsto \text{s-Inv}\,\Delta$ and $\Delta \mapsto \text{p-Inv}\,\Delta$ are decreasing. Further, if Θ is a family of subsets of $D(E)$ and Inv stands for any of our two invariants, we have $\operatorname{Inv}\big(\bigcup_{\Delta\in\Theta} \Delta\big)=\bigcap_{\Delta\in\Theta} \operatorname{Inv}\Delta$. For a set X^0 let $R(E; X^0)$ denote the set of all relations on E under X^0. Now the *sets*

$$\text{s-Inv}^{(X^0)}\Delta = \text{s-Inv}\,\Delta \cap R(E; X^0) \quad \text{and} \quad \text{p-Inv}^{(X^0)}\Delta = \text{p-Inv}\,\Delta \cap R(E; X^0)$$

are called the stability and preservation invariants of Δ *under* X^0, respectively.

If R is a set of relations on E then $\bar{R}=\text{s-Inv}\,D(E/R)$ and $\bar{R}=\text{p-Inv}\,G(E/R)$ are called the *stability* and *preservation closures* of R, respectively, while

$$\bar{R}^{(X^0)} = \text{s-Inv}^{(X^0)}D(E/R) \quad \text{and} \quad \bar{R}^{(X^0)} = \text{p-Inv}^{(X^0)}G(E/R)$$

are called the stability and preservation closures of R *under* X^0, respectively. The main problem of the next two paragraphs is to characterize these closures in terms of R but without any intervention of self-mappings of E.

2. Fundamental operations

In order to characterize the above-mentioned closures of R in terms of relations we have to introduce certain operations acting on relations. Some of these operations act on sets of relations while others on single relations, but any of these operations results in single relations. Some of these operations are only partial, i.e. they are defined for (sets of) relations satisfying some prescribed conditions.

While defining our fundamental operations in the sequel, all relations are assumed to have a fixed base set E.

I. *Infinitary boolean operations:*

Ia. *Infinitary union,* Ib. *Infinitary intersection.* Both of these operations act on non-empty sets R of relations, and are defined iff all $r \in R$ have the same argument set, say X. These operations are denoted by $\bigcup \cdot R = \bigcup_{r \in R} r$ and $\bigcap \cdot R = \bigcap_{r \in R} r$, and their results are relations with the same argument set X.

Ic. *Negation.* This fundamental operation acts on any single relation r, and is denoted by $\neg$. If X denotes the argument set of r then $\neg \cdot r = E^X \setminus r$, the complement of r in E^X, has the same argument set X.

Remark 1. The above three fundamental operations are not independent. Indeed, if $\neg \cdot R$ denotes $\{\neg \cdot r; r \in R\}$, we have $\bigcup \cdot R = \neg(\bigcap \cdot \neg R)$ and $\bigcap \cdot R = \neg(\bigcup \cdot \neg R)$. However, $\bigcup$ and $\bigcap$ are independent.

Remark 2. Two well-known properties of these operations, namely $r \cap (\neg \cdot r) = \emptyset$ and $r \cup (\neg \cdot r) = E^X$, where X is the argument set of r, will be of relevance later.

Remark 3. When E and X are finite then there are only a finite number of X-relations, whence the infinitary boolean operations are in fact the ordinary (finitary) ones.

Remark 4. We define the following preorder for sets R and R' of relations. Put $R \leqq R'$ iff there exists a surjective mapping $\varphi \colon R' \to R$ such that for every $r' \in R'$ we have $r' \supseteq \varphi \cdot r'$. A (possibly partial) operation ω, acting on sets of relations, will be said *increasing* if for arbitrary sets R and R' of relations $R \leqq R'$ implies $\omega(R) \subseteq \omega(R')$, provided that ω is defined for R and R'. Further, an operation ω (possibly partial) that acts on relations is said to be *increasing* if for any two relations r and r' belonging to the domain of ω, $r \subseteq r'$ implies $\omega \cdot r \subseteq \omega \cdot r'$. It is easy to see that the infinitary union and intersection are increasing, while the negation is not.

II. *Projective operations,* which act on relations:

IIa. *Projections* (or *restrictions*) $\mathrm{pr}_{\bar{X}}$. This operation is defined for a relation r iff the argument set X of r contains $\bar{X}$ as a subset. For an X-point $P \colon X \to E$ let $(P|\bar{X})$ denote the restriction of P onto $\bar{X} \subseteq X$, and define $\mathrm{pr}_{\bar{X}} \cdot r$ as $\{(P|\bar{X}); P \in r\}$. This relation will also be denoted by $\mathrm{pr}_{\bar{X}}^X \cdot r$, $r_{\bar{X}}^X$ and, abusing the scripture, even by $(r|\bar{X})$. This fundamental operation transforms a relation with argument set $X \supseteq \bar{X}$ into a relation with argument set $\bar{X}$.

IIb. *Antiprojections* (or *extensions*) $\mathrm{ext}_{X'}$. This operation is defined for relations r with argument set $X \subseteq X'$, and $\mathrm{ext}_{X'} \cdot r$ is the cartesian product $r \times E^{X' \setminus X}$.

With the usual identification in cartesian products, $\mathrm{ext}_{X'}\cdot r$ is the set of all points (P, P') such that $P\in r$ and P' is an arbitrary $(X'\setminus X)$-point. This relation will also be denoted by $\mathrm{ext}^{X}_{X'}\cdot r$ and ${}^{X}_{X'}(r)$.

Remark 5. *We can extend the operations* $\mathrm{pr}_{\bar{X}}$ *and* $\mathrm{ext}_{X'}$ *to any relation* r with an arbitrary argument set X via defining $\mathrm{pr}_{\bar{X}}\cdot r$ as $\mathrm{pr}^{X}_{X\cap\bar{X}}\cdot r$ and $\mathrm{ext}_{X'}\cdot r$ as $\mathrm{ext}^{X}_{X\cup X'}\cdot r$. Then we have $\mathrm{pr}_{\bar{X}}\,\mathrm{pr}_{X'}=\mathrm{pr}_{\bar{X}\cap X'}$ and $\mathrm{ext}_{X'}\,\mathrm{ext}_{X''}=\mathrm{ext}_{X'\cup X''}$.

Remark 6. We have $\mathrm{pr}_{\emptyset}\cdot r=\{P_{\emptyset}\}$ for $r\neq\emptyset$ and $\mathrm{pr}_{\emptyset}\cdot r=\emptyset$ for $r=\emptyset$.

Remark 7. Both projections and extensions are increasing.

Remark 8. When relations are considered as sets of points, extensions are hyperpunctual mappings and projections are even punctual, if relations with a fixed argument set are considered. Therefore, the projections commute with $\cup$, and it is easy to see that the extensions commute with all boolean operations.

Remark 9. While $\mathrm{pr}^{X'}_{X}\,\mathrm{ext}^{X}_{X'}\cdot r=r$ is always true, r is only a subset of $\mathrm{ext}^{\bar{X}}_{X}\,\mathrm{pr}^{X}_{\bar{X}}\cdot r$. If $\mathrm{ext}^{\bar{X}}_{X}\,\mathrm{pr}^{X}_{\bar{X}}\cdot r=r$ then r is said to be *identical* on $X\setminus\bar{X}$ or outside $\bar{X}$, and the arguments belonging to $X\setminus\bar{X}$ are called *fictitious*. The operation $c_{\bar{X}}=\mathrm{ext}^{\bar{X}}_{X}\,\mathrm{pr}^{X}_{\bar{X}}$, which preserves the argument set, is called the $\bar{X}$-cylindrification. For $X\subseteq X'$ we have $E^{X'}=\mathrm{ext}^{X}_{X'}\cdot E^{X}$ and, in particular, $I(X, E)=E^{X}=\mathrm{ext}_{X}\cdot E^{\emptyset}=\mathrm{ext}_{X}\cdot\{P_{\emptyset}\}$.

Canonical identification. Let r and r' be relations on E with argument sets X and X'. Let $r\sim r'$ mean that there exists a set $X''\supseteq X\cup X'$ such that $\mathrm{ext}_{X''}\cdot r=\mathrm{ext}_{X''}\cdot r'$. If this equality holds for some set $X''\supseteq X\cup X'$ then it holds for every $X''\supseteq X\cup X'$. Consider $\sim$ as a relation on the class of all relations on E; then $\sim$ is easily seen to be an equivalence relations, i.e., $\sim$ is reflexive, symmetric and transitive. As infinitary boolean operations commute with extensions, they are compatible with this equivalence. For $X''\supseteq X\supseteq\bar{X}$ we have $\mathrm{pr}^{X}_{\bar{X}}=\mathrm{pr}^{X}_{\bar{X}}(\mathrm{pr}^{X''}_{X}\,\mathrm{ext}^{X}_{X''})=(\mathrm{pr}^{X}_{\bar{X}}\,\mathrm{pr}^{X''}_{X})\,\mathrm{ext}^{X}_{X''}=\mathrm{pr}^{X''}_{\bar{X}}\,\mathrm{ext}^{X}_{X''}$, whence $\mathrm{pr}_{\bar{X}}\cdot r=\mathrm{pr}_{\bar{X}}(\mathrm{ext}_{X''}\cdot r)$. Hence it is easy to conclude that if an X-relation r and an X'-relation r' are equivalent modulo $\sim$ and $\bar{X}\subseteq X\cap X'$ then $\mathrm{pr}_{\bar{X}}\cdot r=\mathrm{pr}_{\bar{X}}\cdot r'$. So projections are also compatible with this equivalence. Further, we have $\mathrm{ext}_{X'}\cdot r\sim r$. It is also obvious that if r and r' have the same argument set X and $r\sim r'$ then r and r' must coincide. Therefore, for any X-relation r and X', there is at most one X'-relation equivalent to r, and there is certainly such an X'-relation if $X'\supseteq X$.

Relations on E can be considered modulo $\sim$, i.e., we may identify relations that are equivalent. This means that if a relation can be obtained from another one via omitting and adding some fictitious arguments then these two relations are considered the same. This identification will be called *canonical*. Since infinitary boolean operations and projections are compatible with $\sim$, they are meaningful after canonical identification. It is trivial that $\mathrm{ext}_{X'}$ becomes the identical operation when relations are canonically identified. Further, the infinite union and intersection become defined for every set R of relations in this case. Indeed, take a sufficiently large set X that includes the argument set of any $r \in R$. Then for each $r \in R$ there is exactly one X-relation r' such that $r \sim r'$, so we can and must define $\bigcup \cdot R$ and $\bigcap \cdot R$ as $\bigcup_{r \in R} r'$ and $\bigcap_{r \in R} r'$, respectively.

III. *Contractive operations.*

IIIa. *Contraction* (φ). Given a surjection $\varphi\colon X \to Y$ and an X-point $P\colon X \to E$ which is compatible with φ, we can define a Y-point $Q\colon Y \to E$ by the condition $Q \cdot y = P \cdot x$ where $x \in \varphi^{-1} \cdot y$. The mapping that sends P to Q and maps the multidiagonal $I_{T(\varphi)}(E)$ onto $E^Y = I(Y, E)$ will be denoted by (φ). It is easy to check that (φ) is injective. An X-relation r is said to be *compatible* with φ iff every $P \in r$ (as a mapping of X into E) is compatible with φ. In this case $(\varphi) \cdot r = \{(\varphi) \cdot P;\ P \in r\}$ is a Y-relation. This mapping (φ), which maps the set of X-relations compatible with φ into the set of Y-relations, is called the *contraction* (φ). This mapping is punctual and injective, so it commutes with the infinitary union and intersection, and we have $(\varphi) \cdot \big(I_{T(\varphi)}(E) \cap (\neg r)\big) = (\varphi) \cdot \big(I_{T(\varphi)}(E) \setminus r\big) = \neg\big((\varphi) \cdot r\big)$. Clearly, φ is increasing. If $\varphi\colon X \to Y$ and $\varphi'\colon Y \to Z$ are surjections then $(\varphi') \cdot \big((\varphi) \cdot P\big)$ is defined iff P is compatible with $\varphi'\varphi$, and in this case $(\varphi'\varphi) \cdot P = (\varphi') \cdot \big((\varphi) \cdot P\big)$. The same formula holds for relations.

IIIb. *Dilatations* $[\psi]$. Let $\psi\colon Y \to X$ be a surjection. Then for any X-point $P\colon X \to E$ the mapping $[\psi] \cdot P = P \cdot \psi\colon y \to P \cdot (\psi \cdot y)$ is a Y-point compatible with ψ. The mapping $P \to [\psi] \cdot P$ is injective and maps E^X onto the multidiagonal $I_{T(\psi)}(E)$. For an X-relation r let $[\psi] \cdot r$ stand for $\{[\psi] \cdot P;\ P \in r\}$. Then $[\psi]$, called the *dilatation* $[\psi]$, is a mapping of $P(E^X)$, the set of all X-relations, onto $P\big(I_{T(\psi)}(E)\big)$. Further, this mapping is punctual and injective. Hence it commutes with the infinitary intersection and union, and we have $[\psi] \cdot (\neg r) = I_{T(\psi)}(E) \setminus [\psi] \cdot r$. If $\psi\colon Y \to X$ and $\psi'\colon Z \to Y$ are surjections then $[\psi'\psi] \cdot P = [\psi'] \cdot ([\psi] \cdot P)$ and $[\psi'\psi] \cdot r = [\psi'] \cdot ([\psi] \cdot r)$. Obviously, $(\psi)[\psi] \cdot r = r$ for every X-relation r, and $[\psi](\psi) \cdot r = r$ for every X-relation r compatible with ψ.

Remark 10. Every multidiagonal can be obtained by an appropriate dilatation from some identity.

Note that any multidiagonal can also be obtained as an intersection of (extensions of) simple diagonals. Indeed, $I_C(E) = \bigcap_{x \equiv y(C)} \mathrm{ext}_X \cdot D_{x,y}(E)$ or, up to canonical identification, $I_C(E) = \bigcap_{x \equiv y(C)} D_{x,y}(E)$. The strict multidiagonal $I_C^0(E)$ can be obtained by an intersection of simple diagonals and antidiagonals.

Contractive operations and canonical identification. Let $\varphi\colon X \to Y$ be a surjection and let r be an X-relation compatible with φ. For $x \in X$ the $T(\varphi)$-class of x

is a singleton, provided x is a fictitious argument of r. If $y=\varphi\cdot x$, $\bar{X}=X\setminus\{x\}$, $\bar{Y}=Y\setminus\{y\}$ and $\bar{\varphi}=(\varphi|\bar{X})$, then $\bar{\varphi}$ maps $\bar{X}$ onto $\bar{Y}$, $(r|\bar{X})$ is compatible with $\bar{\varphi}$, and $(\varphi)\cdot r=(\bar{\varphi})\cdot(r|\bar{X})\times E^{\{y\}}$. Thus y is also a fictitious argument of $(\varphi)\cdot r$. More generally, if r is identical outside $\bar{X}\subseteq X$, then φ is injective on $X\setminus\bar{X}$, $\bar{\varphi}=(\varphi|\bar{X})$ maps $\bar{X}$ onto $\bar{Y}=Y\setminus\varphi\cdot(X\setminus\bar{X})$, $(r|\bar{X})$ is compatible with $\bar{\varphi}$, $(\bar{\varphi})\cdot(r|\bar{X})=((\varphi)\cdot r|\bar{Y})$ and $(\varphi)\cdot r$ is identical on $Y\setminus\bar{Y}$. So, $(\bar{\varphi})\cdot(r|\bar{X})\sim(\varphi)\cdot r$.

Two relations, say r and r' with respective argument sets X and X', are equivalent if and only if $(r|X\cap X')=(r'|X\cap X')$ and both are identical outside $X\cap X'$. Indeed, $r\sim r'$ iff $\mathrm{ext}_{X\cup X'}\cdot r=\mathrm{ext}_{X\cup X'}\cdot r'$, and we can use the equalities $(r|X\cap X')=(\mathrm{ext}_{X\cup X'}\cdot r|X\cap X')$ and $(r'|X\cap X')=(\mathrm{ext}_{X\cup X'}\cdot r'|X\cap X')$. Furthermore, if r and r' are equivalent, $r=\mathrm{ext}_X\cdot(r|X\cap X')$.

Let r and r' be relations with respective argument sets X and X', and let $\varphi\colon X\to Y$ and $\varphi'\colon X'\to Y$ be mappings. The pairs (r,φ) and (r',φ') will be said *equivalent* iff $r\sim r'$ and, furthermore, there exists a subset $\bar{X}$ of $X\cap X'$ such that $(\varphi|\bar{X})=(\varphi'|\bar{X})$ and r is identical on $X\setminus\bar{X}$. (Note that in this case $(r|\bar{X})=(r'|\bar{X})$ and r' is identical on $X'\setminus\bar{X}$.) Let $(r,\varphi)\sim(r',\varphi')$ denote that (r,φ) and (r',φ') are equivalent. It is easy to see that this binary relation is in fact an equivalence.

Similarly, let r be an X-relation, r' be an X'-relation, further let $\psi\colon Y\to X$ and $\psi'\colon Y\to X'$ be surjections. Then the pairs (r,ψ) and (r',ψ') are said to be *equivalent* iff $r\sim r'$ and there exists a subset $\bar{X}$ of $X\cap X'$ such that (α) $\psi^{-1}\cdot\bar{X}=\psi'^{-1}\cdot\bar{X}$ (this set will be denoted by $\bar{Y}$) and $(\psi|\bar{Y})=(\psi'|\bar{Y})$, (β) $(\psi|Y\setminus\bar{Y})\colon Y\setminus\bar{Y}\to X\setminus\bar{X}$ and $(\psi'|Y'\setminus\bar{Y})\colon Y'\setminus\bar{Y}\to X'\setminus\bar{X}$ are bijections, and (γ) r and r' are identical outside $\bar{X}$. Note that if (r,ψ) and (r',ψ') are equivalent then $[\psi]\cdot r\sim[\psi']\cdot r'$.

Floatage. Floating equivalences. Free and semi-free intersections. For a bijection $\varphi\colon X\to Y$, every X-relation r is compatible with φ. Then the contraction (φ), which coincides with the dilatation $[\varphi^{-1}]$, is called a *flotage* (of arguments). A subset $\bar{X}$ of X such that $(\varphi|\bar{X})$ is the identity mapping is called an *anchor set* of the floatage (φ), while the maximal anchor set of (φ) will be called its *anchor* and is denoted by $A(\varphi)=\{x\in X;\ \varphi\cdot x=x\}$. The elements of $A(\varphi)$ are referred to as *anchor arguments.* When considering a floatage with an anchor set $\bar{X}$, we say that we *let* the arguments outside $\bar{X}$ *float.*

Two relations, say r and r' with respective argument sets X and X', are called *floatingly equivalent* (in notation $r\underset{f}{\sim}r'$) if there exists a bijection $\varphi\colon X\to Y$ such that $(\varphi)\cdot r\sim r'$. It is easy to verify that this binary relation is really an equivalence, called *floating equivalence.* The existence of a floatage (φ) such that $(\varphi)\cdot r=r'$ is called *restricted floating equivalence* and is denoted by $r\underset{rf}{\sim}r'$. When we allow floatages with a fixed anchor set $\bar{X}$ only then we obtain the analogous notions of *semi-*

floating and *restricted semifloating equivalences of anchor* $\bar{X}$ (in notation $r \underset{\bar{X},f}{\sim} r'$ and $r \underset{\bar{X},r,f}{\sim} r'$, resp.).

Let r be an X-relation and let $\bar{X} \subseteq X$. It is clear that the $\bar{X}$-projection of r does not change when we let the "dumb" arguments $x \in X \setminus \bar{X}$ float. We have also seen that $(r|\bar{X})$ is invariant under canonical equivalence. Therefore $\mathrm{pr}_{\bar{X}} \cdot r = \mathrm{pr}_{\bar{X}} \cdot r'$, provided $r \underset{\bar{X},f}{\sim} r'$. In particular, it is without changing $\mathrm{pr}_{\bar{X}} \cdot r$ that we can let the "dumb" arguments $x \notin \bar{X}$ float so that their images avoid some prescribed set $\hat{X} \supseteq \bar{X}$. If it is so then the image of r by this floatage is said to be regularized for $\hat{X}$.

Let R be a set of relations on E, and let X_r denote the argument set of $r \in R$. For each $r \in R$ take a floatage (φ_r) so that the sets $Y_r = \varphi_r \cdot X_r$ $(r \in R)$ be pairwise disjoint. If Y is a set including $\bigcup_{r \in R} Y_r$ then $\bigcap_{r \in R} \mathrm{ext}_Y (\varphi_r) \cdot r$ does not depend, modulo floating equivalence, on the choice of floatages (φ_r) and of Y. Hence $\bigcap_{r \in R} \mathrm{ext}_Y (\varphi_r) \cdot r$ can be called the *free intersection* of $r \in R$; it is determined up to floating equivalence. When we take $Y = \bigcup_{r \in R} Y_r$ then $\bigcap_{r \in R} \mathrm{ext}_Y (\varphi_r) \cdot r$ is clearly the cartesian product $\prod_{r \in R} (\varphi_r) \cdot r$, which is equivalent to $\prod_{r \in R} r$. So the free intersection is, up to floating equivalence, the (complete) cartesian product. The free intersection of all $r \in R$ will be denoted by $\bigcap_f \cdot R$.

Given a set $\bar{X}$ and a set R of relations r on E and with argument sets X_r, the *semi-free intersection of anchor* $\bar{X}$ of R is defined as follows. Put $\bar{X}_r = \bar{X} \cap X_r$ and choose floatages (φ_r) with anchor sets $\bar{X}_r$ so that $\bar{X} \cap \varphi_r \cdot (X_r \setminus \bar{X}_r) = \emptyset$ and the sets $\varphi_r \cdot (X_r \setminus \bar{X}_r)$, $r \in R$, be pairwise disjoint. Further, take a set Y including all $\varphi_r \cdot X_r$. Then $\bigcap_{r \in R} \mathrm{ext}_Y (\varphi_r) \cdot r$, called the semi-free intersection of anchor $\bar{X}$ of R and denoted by $\bigcap_f^{(\bar{X})} \cdot R$, does not depend, up to semi-floating equivalence of anchor $\bar{X}$, on the choice of Y and that of φ_r $(r \in R)$.

Lemma 1. *Let R be a set of relations r with argument sets X_r, let $\bar{X}_r \subseteq X_r$, and put $\bar{X} = \bigcup_{r \in R} \bar{X}_r$. Then*

$$\bigcap_{r \in R} \mathrm{ext}_{\bar{X}} \, \mathrm{pr}_{\bar{X}_r} \cdot r = \mathrm{pr}_{\bar{X}} \cdot (\bigcap_f^{(\bar{X})} \cdot R).$$

Proof. Put $\varrho = \bigcap_{r \in R} \mathrm{ext}_{\bar{X}} \, \mathrm{pr}_{\bar{X}_r} \cdot r$ and $\varrho^* = \mathrm{pr}_{\bar{X}} \cdot (\bigcap_f^{(\bar{X})} \cdot R)$. Let $\bigcap_f^{(\bar{X})}$ be represented by $\bigcap_{r \in R} \mathrm{ext}_{\bar{X} \cup Y'} (\varphi_r) \cdot r$ where $\varphi_r \colon X_r \to \bar{X}_r \cup Y_r$ are bijections subject to the previous conditions. I.e., the Y_r are pairwise disjoint and $Y' = \bigcup_{r \in R} Y_r$ is disjoint from $\bar{X}$. An $\bar{X}$-point $\bar{P} \colon \bar{X} \to E$ is in ϱ iff for every $r \in R$ $(\bar{P}|\bar{X}_r)$ is a point such that there exists an $(X_r \setminus \bar{X}_r)$-point P_r' with $((\bar{P}|\bar{X}_r), P_r')$ belonging to r. But this is equivalent to $(\varphi_r) \cdot ((\bar{P}|\bar{X}_r), P_r') \in (\varphi_r) \cdot r$ and, as $(\varphi_r|\bar{X}_r)$ is the identity map, also to the existence of a Y_r-point $P_r''=(\varphi_r|X_r\setminus\bar{X}_r)\cdot P_r'$ such that $(\bar{P}, P_r'')\in\mathrm{ext}_{X\cup Y_r}(\varphi_r)\cdot r$. Since the sets Y_r are pairwise disjoint, for any set $\{P_r'': Y_r\to E;\ r\in R\}$ of points there exists exactly one point $P'': Y'\to E$ such that $(P''|Y_r)=P_r''$ holds for each $r\in R$. Clearly, $(\bar{P}, P'')\in\mathrm{ext}_{X\cup Y_r}(\varphi_r)\cdot r$ is equivalent to

$$(\bar{P}, P'')\in\mathrm{ext}_{X\cup Y'}\,\mathrm{ext}_{X\cup Y_r}(\varphi_r)\cdot r = \mathrm{ext}_{X\cup Y'}(\varphi_r)\cdot r.$$

Thus the simultaneous existence of all $P_r'': Y_r\to E$ with $(\bar{P}, P_r'')$ belonging to $\mathrm{ext}_{X\cup Y_r}(\varphi_r)\cdot r$ is equivalent to the existence of a single $P'': Y'\to E$ such that $(\bar{P}, P'')\in\mathrm{ext}_{X\cup Y'}(\varphi_r)\cdot r$ for every $r\in R$, i.e., $(\bar{P}, P'')$ belongs to $\bigcap_{r\in R}\mathrm{ext}_{X\cup Y'}(\varphi_r)\cdot r= =\bigcap_{r\in R}\mathrm{ext}_Y(\varphi_r)\cdot r$, which is equivalent to $\bar{P}\in\varrho^*$. I.e., $\bar{P}\in\varrho$ is equivalent to $\bar{P}\in\varrho^*$, which completes the proof.

The operations Ia, Ib, Ic $(\cup, \cap, \neg)$, IIa, IIb $(\mathrm{pr}_X, \mathrm{ext}_{X'})$, IIIa and IIIb $((\varphi), [\psi])$ are called *fundamental operations*. The increasing fundamental operations, i.e. all but the negation $\neg$, are called *direct fundamental operations*. Two nullary operations, namely IVa: (adding to any set of relation) the empty relation $\emptyset$ and IVb: (adding) the $\emptyset$-identity $I(\emptyset, E)=\{P_\emptyset\}$, are also considered as direct fundamental operations. These two nullary operations are combinations of the rest of the fundamental operations when we start from a nonempty set R of relations. Indeed, take an $r\in R$, then $\emptyset=r\cap(\neg r)$ and $I(\emptyset, E)=\mathrm{pr}_\emptyset\cdot(r\cup(\neg r))$. Yet, they are not combinations of direct fundamental operations in general.

If $r\sim r'$ or $r\underset{f}{\sim}r'$ (or, in particular, $r\underset{rf}{\sim}r'$, $r\underset{X,rf}{\sim}r'$ or $r\underset{X,f}{\sim}r'$) then each of r and r' can be obtained from the other by a suitable combination of direct fundamental operations. On the other hand if we identify the canonically equivalent relations, we can drop all extensions from (direct) fundamental operations. When passing from relations to floatingly (and even restricted floatingly) equivalent ones is permitted, we may fix a representative set $X(c)$ of cardinality c for each cardinal c, e.g., we may put $X(c)=\{\alpha;\ \alpha$ is an ordinal and $\alpha<\omega(c)\}$ where $\omega(c)$ denotes the smallest ordinal with cardinality c. (I follow Cantor's point of view rather than that of von Neumann. In fact, the second point of view has been adopted in my first paper [1] on abstract Galois theory, while the first one in all of my other papers.)

When the axiom of choice is admitted, contractions become combinations of projections and floatages, while dilatations become combinations of extensions, floatages and intersections with simple diagonals. Indeed, if $\varphi: X\to Y$ is a surjection, for each $y\in Y$ we can choose an $x(y)\in X$ such that $\varphi\cdot x(y)=y$. Put $\bar{X}=\{x(y);\ y\in Y\}$. As $(\varphi|\bar{X}): \bar{X}\to Y$ is a bijection, $((\varphi|\bar{X}))$ is a floatage, and $(\varphi)\cdot r=(\varphi|\bar{X})\,\mathrm{pr}_{\bar{X}}\cdot r$, provided r is compatible with φ. Similarly, if $\psi: Y\to X$ is a surjection, $x\to y(x)$ is a mapping of X into Y such that $\psi\cdot y(x)=x$, and $\bar{Y}=\{y(x);\ x\in X\}$ then $\bar{\psi}=(\psi|\bar{Y}): y(x)\to x$ is a bijection of $\bar{Y}$ onto X. Hence $[\bar{\psi}]=(\bar{\psi}^{-1})$ is a floatage, and for any X-relation r we have

$$[\psi]\cdot r = \mathrm{ext}_Y[\bar{\psi}]\cdot r \cap \Big(\bigcap_{\bar{y}\in \bar{Y}}\ \bigcap_{y=\bar{y}(T(\psi))} D_{\bar{y},y}\Big).$$

When the image of φ or ψ is finite, the axiom of choice is not necessary for the above results.

We say that fundamental or direct fundamental operations are used below X^0, if these operations are used only for relations with argument sets included in X^0 and only when these operations result in relations whose argument sets are also included in X^0. I.e., in case of $\mathrm{pr}_{\bar{X}}$, $\mathrm{ext}_{X'}$, $(\varphi\colon X\to Y)$ and $[\psi\colon Y\to X]$ the inclusions $\bar{X}\subseteq X^0$, $X'\subseteq X^0$ and $Y\subseteq X^0$ are also required. In particular, if E is finite and these operations are used below some finite X^0 then they are equivalent to the realizations of operations of the predicate calculus with equality on the finite model E, the set of object variables being X^0. Indeed, any X-relation r on E (where $X\subseteq X^0$) can be considered as the realization of some predicate $P_r=P_r(X)$ on E. Further, $P_{r\cup r'}=P_r\vee P_{r'}$, $P_{r\cap r'}=P_r \,\&\, P_{r'}$, $P_{\neg r}=\neg P_r$, $P_{\mathrm{pr}_{\bar{X}}\cdot r}=(\exists x_1)\dots(\exists x_s)P_r$ where $\{x_1,\dots,x_s\}=X\setminus\bar{X}$, $P_{\mathrm{ext}_{X'}\cdot r}=P_r(X')$ where $P_r(X')$ is the predicate obtained from $P_r=P_r(X)$ by adding the set $X'\setminus X$ of fictitious variables, if $\varphi\colon X\to Y$ is a bijection and $X=\{x_1,\dots,x_n\}$ then $P_{(\varphi)\cdot r}=P_r^{(\varphi)}$ is a predicate such that $P_r^{(\varphi)}(\varphi\cdot x_1,\dots,\varphi\cdot x_n)=$ $=P_r(x_1,\dots,x_n)$, and we have $P_{D_{x,y}}=(x=y)$. The direct fundamental operations are equivalent to the part of predicate calculus generated by $\vee$, $\&$, existential quantifiers, addition of fictitious variables, substitutions of object variables, the inequality $x_i\neq x_i$ and equalities $x_i=x_j$ (in particular, $x_i=x_i$). In the general case we may consider the fundamental operations as realizations on models of an (unlimited) infinitary generalization of predicate calculus, and direct fundamental operations as that of certain "positive" part of it.

Lemma 2. *For any relation r there exists a set R_r of relations with the same argument set such that*

(1) *every relation in R_r can be obtained from r by a combination of direct fundamental operations;*

(2) *all the relations in R_r are semi-regular, and for each point P of an arbitrary relation $s\in R_r$ there exists a relation $\bar{s}\in R_r$ such that $\bar{s}\subseteq s$ and $P\in t(\bar{s})$; and*

(3) $r=\bigcup\cdot R_r$.

Proof. Firstly, every multidiagonal is obtained by a successive use of direct fundamental operations (starting from the empty set!). Indeed, it is obtained by dilatation from some identity $I(X,E)=\mathrm{ext}_X\cdot I(\emptyset,E)$. Let P be a point of r with type $T(P)$ and let $r_P=r\cap I_{T(P)}(E)$. Put $R_r=\{r_P;\ P\in r\}$. Then (1) is clearly satisfied. It is easy to see that r_P is semiregular and of type $T(P)$, and $P\in t(r_P)$. For $P\in s\in R_r$ we have $s=r_Q\subseteq r$ where Q is a point of r such that P is compatible with

$T(Q)$. Then $T(P)$ is thicker than $T(Q)$, so $I_{T(P)}(E) \subseteqq I_{T(Q)}(E)$ and $r_P \subseteqq r_Q = s$. Put $\bar{s} = r_P$, and (2) is clearly satisfied. Finally, $P \in r_P \subseteqq r$ implies

$$r = \{P;\ P \in r\} = \bigcup_{P \in r} \{P\} \subseteqq \bigcup_{P \in r} r_P \subseteqq r,$$

which yields $\bigcup \cdot R_r = \bigcup_{P \in r} r_P = r$, i.e. (3) holds.

The set R_r constructed in the previous proof is called the *semi-regular decomposition* of r.

Formalism of fundamental operations. If we apply a (generally infinite) combination of fundamental operations to relations, we obtain an operation, which can be represented by a (generally infinite) formula of the "fundamental operation calculus". The best way of denoting these formulas is to use (generally infinite) trees with finite branches. By a tree we mean an unoriented, connected graph without loops, without circles (i.e. closed paths), and with a distinguished vertex, called its root. Let T be a tree with root r. Then for any vertex v in T (in notation, $v \in T$) there is exactly one path in T that connects v and r, provided $v \neq r$. Let w be the vertex next to v on this path. Now w is called the *father* of v, while v is called the *son* of w. A vertex $v \neq r$ has one and only one father, while the set $S(v)$ of sons of v can be of arbitrary cardinality. Vertices without sons are called extremities of T. We shall write $v < v'$ if $v \neq v'$ and v is on the path connecting r and v'. For a vertex v the set $\{v';\ v \leqq v'\}$ of vertices spans a subgraph, called the *subtree of T of root v*. The number of edges in the path connecting v and r is denoted by $h(v)$ and is called the *height* of v. In particular, $h(r) = 0$. Let $h(T) = \sup_{v \in T} h(v)$ be called the *height* of T, which is a non-negative integer or ∞. T is called of *finite* or *infinite height* according to $h(T) \neq \infty$ or $h(T) = \infty$.

A *branch* of T is a maximal linearly ordered set of vertices together with the edges connecting them. We shall deal only with trees without infinite branches. I.e., we always assume that our trees have no infinite, linearly ordered sequence of vertices $v_1 < v_2 < v_3 < \dots$. For such trees there is another invariant, the so-called depth, which is more important than the height. Given a tree T, a mapping ν from its vertex set into the class of ordinals is called a *depth function* of T if for any vertex $v \in T$ we have $\nu(v) = \sup_{u \in S(v)} (\nu(u) + 1)$ (in particular, $\nu(v) = 0$ for any extremity of T). If a tree has a depth function then it cannot have infinite branches. Indeed, if $r = v_0 < v_1 < v_2 < v_3 < \dots$ were an infinite branch then $\nu(v_0) > \nu(v_1) > \nu(v_2) > \nu(v_3) > \dots$ would be an infinite decreasing sequence of ordinals, which is impossible. As to the converse, admitting the denumerable axiom of choice, we can prove the following

Lemma 3. *Any tree without infinite branches has one and only one depth function.*

Proof. Assume that a vertex $v \in T$ is irregular in the sense that the lemma is not true for the subtree T_v. I.e., T_v has no depth function or has more than one depth functions. Then v must have at least one irregular son u. Really, if for all $u \in S(v)$ the subtree T_u has a unique depth function ν_u, then the mapping ν_v defined by $\nu_v(w) = \nu_u(w)$ if $w \in T_u$ and $u \in S(v)$ and, further, $\nu_v(v) = \sup_{u \in S(v)} (\nu_u(u) + 1)$ is a depth function of T_v. As the restiction of this ν_v to any T_u, $u \in S(v)$, is unique by the assumption, ν_v is the only depth function of T_v, which is a contradiction. Thus we have seen that any irregular vertex has an irregular son. Now, if the lemma is not true for a tree T, then its root r is irregular as $T = T_r$. Hence an irregular son r_1 of r, then an irregular son r_2 of r_1, etc. can be chosen. I.e., the denumerable axiom of choice yields the existence of a denumerable sequence $r = r_0, r_1, r_2, \ldots$ of irregular vertices such that each r_i, $i > 0$, is a son of r_{i-1}. But then $r_0 < r_1 < r_2 < \ldots$ contradicts the fact that T has no infinite branch.

When T is a tree without infinite branches and ν is its unique depth function, $d(T) = \nu(r)$ is called the *depth* of T. Any ordinal can be the depth of some tree. The depth of T is finite iff $h(T)$ is finite; in this case $d(T) = h(T)$.

A *formula* is a mapping F from the vertex set of a tree T without infinite branches such that

(1) $F(v)$ is a fundamental operation provided v is not an extremity, and $F(v)$ is either $\cup$ or $\cap$ if $S(v)$ is not a singleton;

(2) for any extremity v with father w, $F(v)$ is a *relation set variable* denoted by $X(v)$ (with capital X) provided $S(w) = \{v\}$ and $F(w)$ is $\cup$ or $\cap$, and $F(v)$ is a *relation variable* $x(v)$ in all other cases.

Note that $F(u)$ and $F(v)$ may coincide even for distinct extremities u and v.

Let E be a base set. A map F' from T is called an *E-formula* if it is obtained from some formula F via replacing certain relation set variables $X(v)$ and certain relation variables $x(v)$ at all of their occurrences by some relation sets $R(v)$ and some relations $r(v)$, resp., on E. Clearly, $X(u) = X(v)$ or $x(u) = x(v)$ must imply $R(u) = R(v)$ or $r(u) = r(v)$, respectively.

Given a base set E and a formula F, let $\Phi(F) = \{F(v);\ v \text{ is an extremity of } T\}$. A mapping ϱ of $\Phi(F)$ is called the *system of values* of variables of F if $\varrho \cdot F(v)$ is a set of relations on E with the same argument set when $F(v) = X(v)$ is a relation set variable while $\varrho \cdot F(v)$ is a single relation on E when $F(v) = x(v)$ is a relation variable. A mapping $t(\varrho)$ from the vertex set of T, $t(\varrho)$: $v \to t(\varrho; v)$, will be called a *coherent valuation* of F for ϱ if:

(1) $t(\varrho; v) = \varrho \cdot F(v)$ for every extremity v of T;

(2) if v is not an extremity then $t(\varrho; v)$ is a relation on E;

(3) if $F(v)$ is $\cup$ or $\cap$, $S(v) = \{v'\}$, v' is an extremity, and $F(v') = X(v')$ then $\varrho \cdot F(v) = F(v) \cdot (\varrho \cdot F(v'))$;

(4) in any other case when $F(v)$ is $\cup$ or $\cap$, all the $\varrho \cdot F(v')$, $v' \in S(v)$, have the same argument set and $\varrho \cdot F(v) = \bigcup_{v' \in S(v)} (\varrho \cdot F(v'))$ or $\varrho \cdot F(v) = \bigcap_{v' \in S(v)} (\varrho \cdot F(v'))$, respectively;

(5) if $F(v)$ is $\neg$, $\mathrm{pr}_X^{\bar{X}}$, $\mathrm{ext}_{X'}^{X}$, $(\varphi\colon X \to Y)$ or $[\psi\colon Y \to X]$ then $S(v)$ is a singleton $\{u\}$ and $\varrho \cdot F(u)$ is an X-relation such that, in case $F(v) = (\varphi)$, $\varrho \cdot F(u)$ is compatible with φ, and, in all cases, $\varrho \cdot F(v) = F(v) \cdot (\varrho \cdot F(u))$.

Given ϱ, an easy induction on $\nu(v)$, $v \in T$, shows that there is at most one such coherent valuation $t(\varrho)$.

It is possible to define the fundamental operations for formulas. Let U be a set of formulas (or E-formulas), and let r_F denote the root of the formula $F \in U$. We construct a new formula $F^0 = \bigcup U$ or $F^0 = \bigcap U$, resp., via taking a new root r^0, adding a new edge (r^0, r_F) to every $F \in U$, and putting $F^0(r^0) = \cup$ or $F^0(r^0) = \cap$, respectively. Note that $S(r^0) = \{r_F;\ F \in U\}$ and each F becomes $F^0_{r_F}$. If F is a formula or E-formula and ω is one of the operations $\neg$, $\mathrm{pr}_X^{\bar{X}}$, $\mathrm{ext}_{X'}^{X}$, $(\varphi\colon X \to Y)$, and $[\psi\colon Y \to X]$ then the formula (or E-formula) $\omega \cdot F$ is constructed so that we join a new root r^0 with the root r of F by a new edge (then r becomes the only son of r^0) and we put $(\omega \cdot F)_r = F$ and $(\omega \cdot F)(r^0) = \omega$. It is easy to verify that if ϱ_F is the value of $\Phi(F)$, $F \in U$, and ϱ is the value of $\Phi(\bigcup U)$ or $\Phi(\bigcap U)$, respectively, such that we have $(\varrho | \Phi(F)) = \varrho_F$ for every $F \in U$, then $(\bigcup U)(\varrho)$ resp. $(\bigcap U)(\varrho)$ is defined iff all the $F(\varrho_F)$, $F \in U$, are defined and $\cup$ resp. $\cap$ is applicable to $\{F(\varrho_F);\ F \in U\}$. If this is so then we have $(\bigcup U)(\varrho) = \bigcup_{F \in U} F(\varrho_F)$ and $(\bigcap U)(\varrho) = \bigcap_{F \in U} F(\varrho_F)$. If ω is one of the operations $\neg$, $\mathrm{pr}_X^{\bar{X}}$, $\mathrm{ext}_{X'}^{X}$, (φ), and $[\psi]$ and ϱ is a value of $\Phi(F)$ then $(\omega \cdot F)(\varrho)$ is defined iff $F(\varrho)$ is defined and ω is applicable to it. In this case we have $(\omega \cdot F)(\varrho) = \omega \cdot F(\varrho)$.

The formalism can be defined modulo canonical identification, too. Then ext disappears and the results of the rest of fundamental operations are always defined for arbitrary relations and, for $\cup$ and $\cap$, for arbitrary sets of relations. Indeed, we only have to consider relations and operations modulo canonical identification and then to replace $(\varphi) \cdot r$, where $\varphi\colon X \to Y$ is a surjection, by $(\varphi)(\mathrm{pr}_X^{X'}\, \mathrm{ext}_{X_r}^{X'} \cdot r \cap I_{T(\varphi)}(E))$ where X_r is the argument set of r and X' includes $X_r \cup X$.

3. Fundamental operations and mappings

Let $\omega(\ldots)$ be one of the considered fundamental operations. We denote by ξ an arbitrary value of its argument, which may be a set of relations (for Ia, Ib) or a relation (for I3, IIa, IIb, IIIa, IIIb) or nothing (for IVa, IVb). Let $d\colon E \to E'$ be a mapping from the base set E into another set E'. We say that ω *commutes* with d if for any ξ (with base set E) ω is defined for $d \cdot \xi$ provided it is defined for ξ, and $d \cdot \omega(\xi) = \omega(d \cdot \xi)$. We say that ω *semi-commutes* with d if $\omega(d \cdot \xi)$ is defined when $\omega(\xi)$ is, and $d \cdot \omega(\xi) \subseteqq \omega(d \cdot \xi)$.

Proposition 1. (1) *Every fundamental operation commutes with any bijection.*

(2) *Every direct fundamental operation semi-commutes with any mapping.*

(3) *More precisely, the infinitary union, projections, contractions, dilatations, and the addition of $\emptyset$ and $I_0(E)$ commute with all mappings, the infinitary intersection commutes only with injections, and extensions commute only with surjections.*

Proof. As every mapping d of the base set preserves the argument sets of relations, it is clear that if any of the operations Ia, Ib, Ic, IIa, IIb, IIIb, IVa, and IVb is defined for some value ξ of its argument then it is also defined for $d \cdot \xi$. If $\varphi: X \to Y$ is a surjection and $P: X \to E$ is compatible with φ then $d \cdot P$ is also compatible with φ, where $d: E \to E'$ is an arbitrary mapping from E. Indeed, for $x \in X$, $(d \cdot P) \cdot x = d \cdot (P \cdot x)$ depends only on $P \cdot x$, which depends only on $\varphi \cdot x$. Therefore, if an X-relation r is compatible with φ then so is $d \cdot r$, i.e., $(\varphi) \cdot r$ being defined implies that $(\varphi) \cdot (d \cdot r)$ is also defined. So the preliminary condition on commutation and semi-commutation is always fulfilled.

Let us compute:

$$d \cdot (\bigcup R) = d \cdot \{P; (\exists r \in R)(P \in r)\} = \{d \cdot P; (\exists r \in R)(P \in r)\} =$$
$$= \{Q; (\exists s \in d \cdot R)(Q \in s)\} = \bigcup \cdot (d \cdot R).$$

For $\bar{X} \subseteqq X$ and an X-relation r we have

$$d \cdot (r | \bar{X}) = d \cdot \{(P | \bar{X}); P \in r\} = \{d \cdot (P | \bar{X}); P \in r\} = \{(d \cdot P | \bar{X}); P \in r\} =$$
$$= \{(Q | \bar{X}); Q \in d \cdot r\} = (d \cdot r | \bar{X}), \quad \text{i.e.,} \quad d \cdot \mathrm{pr}_{\bar{X}}\, r = \mathrm{pr}_{\bar{X}}\, (d \cdot r).$$

If $P: X \to E$ is an X-point compatible with the surjection $\varphi: X \to Y$ then $(\varphi) \cdot P$ is the mapping $Y \to E$, $y \to P \cdot x$ where $\varphi \cdot x = y$. So, $d \cdot ((\varphi) \cdot P)$ is the mapping $y \to d \cdot (((\varphi) \cdot P) \cdot y) = d \cdot (P \cdot x) = (d \cdot P) \cdot x$, where $\varphi \cdot x = y$. Thus $d \cdot ((\varphi) \cdot P) = (\varphi) \cdot (d \cdot P)$, and, if r is an X-relation compatible with φ, we have

$$d \cdot ((\varphi) \cdot r) = d \cdot \{(\varphi) \cdot P; P \in r\} = \{(\varphi) \cdot (d \cdot P); P \in r\} =$$
$$= \{(\varphi) \cdot Q; Q \in d \cdot r\} = (\varphi) \cdot (d \cdot r).$$

When $\psi: Y \to X$ is a surjection and r is an X-relation,

$$d \cdot ([\psi] \cdot r) = d \cdot \{[\psi] \cdot P; P \in r\} = \{d \circ (P \circ \psi); P \in r\} = \{(d \circ P) \circ \psi; P \in r\} =$$
$$= \{Q \circ \psi; Q \in d \cdot r\} = [\psi] \cdot (d \cdot r].$$

It is clear that $\emptyset$ and $I(\emptyset, E)$ depend on no argument, $d \cdot \emptyset = \emptyset$, and $d \cdot I(\emptyset, E) = I(\emptyset, E)$.

If R is a set of X-relations, we have

$$d\cdot(\bigcap R)=d\cdot\{P;\ (\forall r\in R)(P\in r)\}=\{d\cdot P;\ (\forall r\in R)(P\in r)\}.$$

Since $P\in r$ implies $d\cdot P\in d\cdot r$, $Q\in d\cdot(\bigcap R)$ implies $Q\in d\cdot r$, for each $r\in R$, i.e., $d\cdot(\bigcap R)\subseteqq\bigcap\cdot(d\cdot R)$. The converse implication $d\cdot P\in d\cdot r\Rightarrow P\in r$ holds for all $r\subseteqq E^X$ iff d is injective. Therefore the equality $d\cdot(\bigcap R)=\bigcap\cdot(d\cdot R)$ holds for any set R of X-relations only if d is injective.

Let r be an X-relation and let $X'\supset X$, i.e., $X'\setminus X\neq\emptyset$. Then $d\cdot \mathrm{ext}_{X'}r=$ $=d\cdot(r\times E^{X'\setminus X})=(d\cdot r)\times(d\cdot E)^{X'\setminus X}\subseteqq(d\cdot r)\times(E')^{X'\setminus X}=\mathrm{ext}_{X'}(d\cdot r)$ and we have the equality $d\cdot\mathrm{ext}_{X'}r=\mathrm{ext}_{X'}(d\cdot r)$ (even for only one arbitrary $r\neq\emptyset$) iff d is surjective. This proves (3). Now (1) and (2), except the case of $\neg$, are consequences of (3). But if $s\colon E\to E'$ is a bijection then it commutes with all the Boolean operations, so, in particular, with the negation $\neg\colon r\to E^X\setminus r$. The proof of Proposition 1 is complete.

Applying Proposition 1 to the particular case $E=E'$ we obtain

Corollary 1. (1) *Every fundamental operation commutes with any permutation of the base set.*

(2) *Every direct fundamental operation semi-commutes with any self-mapping of E.*

(3) *The infinitary union, projections, contractions, dilatations, and the addition of $\emptyset$ and $I_\emptyset(E)$ commute with all self-mappings of E, the infinitary intersection commutes only with its self-injections, while the extensions commute only with its self-surjections.*

Proposition 2. *Let σ be a permutation of E, let R be a set of relations on E, and assume that a fundamental operation ω is applied to a subset or element ξ of R. (It is a subset when $\omega=\bigcup$ or $\omega=\bigcap$, and it is an element otherwise.) If σ is preserving on R then σ preserves $\omega(\xi)$.*

Proof. As $\sigma\cdot\xi=\xi$ and ω commutes with σ, we have $\sigma\cdot\omega(\xi)=\omega(\sigma\cdot\xi)=$ $=\omega(\xi)$, indeed.

Proposition 3. *If δ is a self-mapping of E stabilizing on a set R of relations and if ω is an increasing fundamental operation semi-commuting with δ which is applicable to a subset or element ξ of R then δ stabilizes $\omega(\xi)$.*

Proof. Indeed, we have $\delta\cdot\omega(\xi)\subseteqq\omega(\delta\cdot\xi)$. Further, if ξ is a set of relations, $\varphi\colon r\to\delta\cdot r$ $(r\in\xi)$ is a surjection of ξ onto $\delta\cdot\xi$ such that $\varphi\cdot r=\delta\cdot r\subseteqq r$ for all $r\in\xi$. Hence $\delta\cdot\xi\leqq\xi$. When ξ is a single relation, $\delta\cdot\xi\subseteqq\xi$. Therefore, as ω is increasing, we have $\omega(\delta\cdot\xi)\subseteqq\omega(\xi)$ and $\delta\cdot\omega(\xi)\subseteqq\omega(\delta\cdot\xi)$, whence $\delta\cdot\omega(\xi)\subseteqq\omega(\xi)$.

Corollary 2. *Let ω be a fundamental operation which is applicable to a subset or element ξ of a set R of relations on E. If a self-mapping δ of E is stabilizing on R then it stabilizes $\omega(\xi)$.*

It follows from the preceding results that for any set $\Delta \subseteqq D(E)$ of self-mappings of E, s-Inv Δ is closed with respect to all direct fundamental operations. I.e., if a direct fundamental operation ω is applied to an element or a subset ξ of s-Inv Δ then $\omega(\xi)$ belongs to s-Inv Δ. Similarly, s-$\mathrm{Inv}^{(X^0)}\Delta$ is closed with respect to these operations below X^0. In particular, the same closedness is true for $\bar{R}$ and $\bar{R}^{(X^0)}$, where R is a set of relations on E. If $\Delta \subseteqq S(E)$ is a set of permutations of E then p-Inv Δ is closed with respect to all fundamental operations, and so is the preservation closure $\bar{R}$ of a set R of relations on E. Similarly, p-$\mathrm{Inv}^{(X^0)}\Delta$ and $\bar{R}^{(X^0)}$ are closed with respect to all fundamental operations below X^0.

4. Equivalence and existence theorems of abstract Galois theory and endotheory

Let X^0 be a set and let R be a set of relations under X^0. I.e., the argument sets of relations in R are subsets of X^0. The set R is said to be *logically* resp. *directly closed below* X^0 if it is closed with respect to all fundamental resp. all direct fundamental operations below X^0. If F is a logically or directly closed family of sets of relations on E then the intersection $\bigcap_{R \in F} R$ of this family is also logically or directly closed, respectively. If R is a non-empty set of relations on E then the family of all relation sets that include R, are under X^0 and are logically resp. directly closed is not empty as it contains $R^{(X^0)}$, the set of all relations on E under X^0. The intersection $R_f^{(X^0)}$ resp. $R_{df}^{(X^0)}$ of this family is called the *logical* resp. *direct logical* closure of R below X^0. $R_f^{(X^0)}$ and $R_{df}^{(X^0)}$ are the smallest relation sets (on E) under X^0 that are logically and directly closed, respectively. Let $S=(E, R)$ and $S'=(E, R')$ be two structures on E so that both R and R' be under X^0. (In this case S and S' are said to be structures under X^0.) We say that S and S' are *equivalent* resp. *directly equivalent below* X^0 if $R_f^{(X^0)}=R_f'^{(X^0)}$ resp. $R_{df}^{(X^0)}=R_{df}'^{(X^0)}$. Generally, these equivalences depend on X^0. Yet, as it will be shown, they do not depend on X^0 when card $X^0 \geqq$ card E is assumed. Indeed, our main purpose in this paragraph is to prove the following four theorems, in which card $X^0 \geqq$ card E is always supposed.

Equivalence theorem of abstract Galois endotheory. *Let S and S' be structures under X^0 and assume that* card $X^0 \geqq$ card E, *where E is the common base set of these structures. Then S and S' are directly equivalent iff $D_{E/S}=D_{E/S'}$.*

Equivalence theorem of abstract Galois theory. *LetS and S' be two structures under X^0 on E where* card $X^0 \geqq$ card E. *Then S and S' are equivalent iff $G_{E/S}=G_{E/S'}$.*

Existence theorem of abstract Galois endotheory. *For any semigroup D of self-mappings of E, if D contains the identical mapping 1_E and X^0 is a set with* $\operatorname{card} X^0 \geqq \operatorname{card} E$ *then there exists a structure S under X^0 on E such that $D = D_{E/S}$.*

Existence theory of abstract Galois theory. *Let G be an arbitrary permutation group on E and let X^0 be a set with* $\operatorname{card} X^0 \geqq \operatorname{card} E$. *Then there exists a structure S under X^0 on E such that $=G_{S/E}$.*

Proof of equivalence and existence theorems of abstract Galois endotheory. (a) Consider $\bar{R}^{(X^0)} = \text{s-Inv}^{(X^0)} D_{E/S}$. This set is directly closed below X^0, so it contains $R_{df}^{(X^0)}$. Hence $D_{E/Q} \supseteqq D_{E/S}$ where Q stands for $R_{df}^{(X^0)}$. As $Q \supseteqq R$, we also have $D_{E/S} = D_{E/R} \supseteqq D_{E/Q}$, i.e. $D_{E/Q} = D_{E/S}$. Therefore if S and S' are directly equivalent below X^0, i.e. $R_{df}^{(X^0)} = R_{df}'^{(X^0)}$, then $D_{E/S} = D_{E/S'}$.

(b) Let D be a submonoid of $D(E)$. For an X-point P on E the set $D \cdot P = \{\delta \cdot P;\ \delta \in D\}$ is called the *D-orbit* of P. Every D-orbit is stabilized by all $\delta \in D$, as $\delta \cdot (D \cdot P) = \delta D \cdot P \subseteqq D \cdot P$. It is also clear that any $\delta \in D$ stabilizes every union of D-orbits. Conversely, assume that each $\delta \in D$ stabilizes a relation r. Then, for any $P \in r$, we have

$$\{P\} = \{1_E \cdot P\} \subseteqq D \cdot P = \{\delta \cdot P;\ \delta \in D\} = \bigcup_{\delta \in D} \{\delta \cdot P\} \subseteqq \bigcup_{\delta \in D} \delta \cdot r \subseteqq \bigcup_{\delta \in D} r = r,$$

i.e., $\{P\} \subseteqq D \cdot P \subseteqq r$. By forming unions we infer that

$$r = \bigcup_{P \in r} \{P\} \subseteqq \bigcup_{P \in r} D \cdot P \subseteqq \bigcup_{P \in r} r = r,$$

i.e., $r = \bigcup_{P \in r} D \cdot P$. Hence every relation stabilized by D is a union of certain D-orbits.

The set of all relations under X^0 that are stabilized by D will be denoted by $R_D^{(X^0)}$. It is clear that the endomorphism monoid of $E/R_D^{(X^0)}$ includes D.

If $P\colon X \to E$ is a surjective point then the mapping $D(E) \to D(E)$, $\delta \to \delta \cdot P$ is injective. If $\operatorname{card} X^0 \geqq \operatorname{card} E$ then there exist surjective $\tilde{X}$-points $\tilde{P}$ with $\tilde{X} \subseteqq X^0$. If δ stabilizes the D-orbit of such a point $\tilde{P}$ then δ must belong to D. Indeed, $\delta \cdot (D \cdot P) = \delta D \cdot P$, $\delta \cdot P = \delta \cdot (1_E \cdot P) \in \delta \cdot (D \cdot P)$, so $\delta \notin D$ would imply $\delta \cdot P \notin D \cdot P$, i.e., δ would not stabilize $D \cdot P$. This means that, denoting $R_D^{(X^0)}$ by Q, $\delta \notin D_{E/Q}$, i.e. $D_{E/Q} = D$, which proves the existence theorem of abstract Galois endotheory.

(c) As $\operatorname{card} X^0 \geqq \operatorname{card} E$, there is a bijective point $\tilde{P}\colon \tilde{X} \to E$ under X^0, i.e. $\tilde{X} \subseteqq X^0$. Let us fix such a point $\tilde{P}$ arbitrarily. Let $P\colon X \to E$ be another arbitrary point under X^0, and put $E_P = P \cdot X$ and $\tilde{X}_P = \tilde{P}^{-1} \cdot E_P$. Then $\tilde{P}^{-1}P\colon X \to \tilde{X}$ is a mapping, which induces a surjection $\varepsilon_{P,\tilde{P}}\colon X \to \tilde{X}_P$. Since $\tilde{P}$ is bijective, the type $T(\varepsilon_{P,\tilde{P}})$ of this mapping is equal to that of P. Hence P is compatible with $\varepsilon_{P,\tilde{P}}$. For any $x \in X$ and $\tilde{x} = \varepsilon_{P,\tilde{P}} \cdot x \in \tilde{X}_P$ we have

$$\big((\varepsilon_{P,\tilde{P}}) \cdot P\big) \cdot \tilde{x} = P \cdot x = (\tilde{P}\tilde{P}^{-1})P \cdot x = \tilde{P} \cdot (\tilde{P}^{-1}P \cdot x) = \tilde{P} \cdot (\varepsilon_{P,\tilde{P}} \cdot x) = \tilde{P} \cdot \tilde{x}.$$

Note that $(\varepsilon_{P,\tilde{P}})\cdot P$ denotes the image of P by the contraction $(\varepsilon_{P,\tilde{P}})$ induced by the surjection $\varepsilon_{P,\tilde{P}}: X\to\tilde{X}_P$, not the composite $\varepsilon_{P,\tilde{P}}\circ P$, which even does not exist in general. So, we have $(\varepsilon_{P,\tilde{P}})\cdot P=(\tilde{P}|\tilde{X}_P)$ and, conversely, $P=[\varepsilon_{P,\tilde{P}}]\cdot(\tilde{P}|\tilde{X}_P)$. As every self-mapping δ of E commutes with projections, contractions and dilatations, we also have $\delta\cdot(\tilde{P}|\tilde{X}_P)=(\varepsilon_{P,\tilde{P}})\cdot(\delta\cdot P)$ and $\delta\cdot P=[\varepsilon_{P,\tilde{P}}]\cdot(\delta\cdot\tilde{P}|\tilde{X}_P)$. Further, if P is compatible with some surjection $\varphi: X\to Y$ then, clearly, so is $\delta\cdot P$. Finally, if D is a semigroup of self-mappings of E, we have $D\cdot(\tilde{P}|\tilde{X}_P)=(\varepsilon_{P,\tilde{P}})\cdot(D\cdot P)$ and $D\cdot P=[\varepsilon_{P,\tilde{P}}]\cdot(D\cdot\tilde{P}|\tilde{X}_P)$. If, in particular, D is a monoid containing 1_E, then the D-orbit $D\cdot P$ of an arbitrary point $P: X\to E$ can be obtained from the D-orbit of the fixed bijective point $\tilde{P}$ by a combination of direct fundamental operations. If P is under X^0 then these operations are below X^0. Therefore $R_D^{(X^0)}\subseteqq\{D\cdot\tilde{P}\}_{df}^{(X^0)}$. Indeed, every $r\in R_D^{(X^0)}$, which is a union of D-orbits by (b), is obtainable from $D\cdot\tilde{P}$ by means of direct fundamental operations (more precisely, by infinitary union, projections, and dilatations) below X^0. Suppose $D=D_{E/S}$. Then, if $S=(E,R)$, we have $R\subseteqq R_D^{(X^0)}$, whence $R_{df}^{(X^0)}\subseteqq(R_D^{(X^0)})_{df}^{(X^0)}=R_D^{(X^0)}$. On the other hand, $\{D\cdot\tilde{P}\}_{df}^{(X^0)}\subseteqq R_D^{(X^0)}$ is trivial and $\{D\cdot\tilde{P}\}_{df}^{(X^0)}\supseteqq R_D^{(X^0)}$ has already been proved, whence $\{D\cdot\tilde{P}\}_{df}^{(X^0)}=R_D^{(X^0)}$. Therefore if we prove $D\cdot\tilde{P}\subseteqq R_{df}^{(X^0)}$ then we also have $R_D^{(X^0)}=\{D\cdot\tilde{P}\}_{df}^{(X^0)}\subseteqq R_{df}^{(X^0)}$ and $R_{df}^{(X^0)}=R_D^{(X^0)}$, from which the equivalence theorem follows. Indeed, if $S=(E,R)$ and $S'=(E,R')$ are two structures under X^0 with the same stability monoid $D=D_{E/S}=D_{E/S'}$ then $R_{df}^{(X^0)}=R_D^{(X^0)}=R_{df}'^{(X^0)}$ would mean the equivalence of S and S' below X^0.

(d) Now we prove $D\cdot\tilde{P}\in R_{df}^{(X^0)}$ via obtaining this orbit explicitly from R by direct fundamental operations. Firstly, we replace every $r\in R$ by the set R_r of semi-regular relations having the same argument sets as r, which has been defined in Lemma 2, Section 2. Then R is replaced by the set of relations $\hat{R}=\bigcup_{r\in R} R_r$, which is under X^0 provided so is R, and which has the following properties implied by the quoted lemma:

(1) every $\hat{r}\in\hat{R}$ can be derived from some $r\in R$ by direct fundamental operations;

(2) for any $P\in\hat{r}\in\hat{R}$ there exists an $\hat{r}'\in\hat{R}$ such that $\hat{r}'\subseteqq\hat{r}$ and $P\in t(\hat{r}')$; and

(3) every $r\in R$ is the union $\bigcup\cdot\hat{R}'$ of some subset $\hat{R}'$ of $\hat{R}$.

These three properties show that $\hat{R}\subseteqq R_{df}^{(X^0)}$ and $R\subseteqq\hat{R}_{df}^{(X^0)}$, whence $R_{df}^{(X^0)}=\hat{R}_{df}^{(X^0)}$ and it is sufficient to prove $D\cdot\tilde{P}\in\hat{R}_{df}^{(X^0)}$. Therefore it suffices to prove $D\cdot\tilde{P}\in R_{df}^{(X^0)}$ only for sets R of *semi-regular* relations under X^0 that have property (2).

Let R be such a set of semi-regular relations and consider the relation

$$r^*=\bigcap_{r\in R}\bigcap_{P\in t(r)}\operatorname{ext}_{\tilde{X}}(\varepsilon_{P,\tilde{P}})\cdot r.$$

Clearly, r^* is obtained from R by direct fundamental operations, whence it belongs to $R_{df}^{(X^0)}$. We shall prove that r^* is precisely $D\cdot\tilde{P}$ where $D=D_{E/S}$.

First, as $P\in t(r)$, $(\varepsilon_{P,\mathfrak{p}})\cdot r$ is defined and $(\tilde{P}|\tilde{X}_P)=(\varepsilon_{P,\mathfrak{p}})\cdot P\in(\varepsilon_{P,\mathfrak{p}})\cdot r$. Thus $\tilde{P}\in\mathrm{ext}_{\tilde{X}}\cdot((\varepsilon_{P,\mathfrak{p}})\cdot r)=\mathrm{ext}_{\tilde{X}}(\varepsilon_{P,\mathfrak{p}})\cdot r$ and $\tilde{P}\in r^*$. But, as r^* is obtained from R by a combination of direct fundamental operations and all $\delta\in D$ are stabilizing on R, every $\delta\in D$ stabilizes r^* and $D\cdot\tilde{P}\subseteq r^*$.

For an arbitrary $\tilde{X}$-point $\tilde{Q}$ we have $\tilde{Q}=\tilde{Q}\circ 1_{\tilde{X}}=\tilde{Q}\circ(\tilde{P}^{-1}\circ\tilde{P})=(\tilde{Q}\circ\tilde{P}^{-1})\circ\tilde{P}$, for $\tilde{P}$ is injective. Hence $\tilde{Q}=\delta\cdot\tilde{P}$ where $\delta=\tilde{Q}\circ\tilde{P}^{-1}$ is a self-mapping of E. Therefore every $\tilde{X}$-point of E is the transform of $\tilde{P}$ by some self-mapping δ of E.

Now assume that $\delta\notin D$, and let us prove that $\delta\cdot P\notin r^*$. Since $\delta\notin D=D_{E/R}$, there exists some $r\in R$ not stabilized by δ, i.e. $\delta\cdot r\nsubseteq r$. Therefore there is a point $P\in r$ such that $\delta\cdot P\notin r$. Since (2) holds for R, there exists an $r'\in R$ such that $P\in t(r')$ and $r'\subseteq r$. Then $\delta\cdot\tilde{P}\notin r'$. As the contraction $(\varepsilon_{P,\mathfrak{p}})$, which is defined also for $\delta\cdot P$, is injective (for points), we have

$$(\delta\cdot\tilde{P}|\tilde{X}_P)=\delta\cdot(\tilde{P}|\tilde{X}_P)=\delta\cdot\big((\varepsilon_{P,\mathfrak{p}})\cdot P\big)=(\varepsilon_{P,\mathfrak{p}})\cdot(\delta\cdot P)\notin(\varepsilon_{P,\mathfrak{p}})\cdot r'$$

and that $\{\delta\cdot\tilde{P}|\tilde{X}_P\}\times E^{\tilde{X}\setminus\tilde{X}_P}$ is disjoint from $\big((\varepsilon_{P,\mathfrak{p}})\cdot r'\big)\times E^{\tilde{X}\setminus\tilde{X}_P}=\mathrm{ext}_{\tilde{X}}(\varepsilon_{P,\mathfrak{p}})\cdot r'$. Thus $\delta\cdot\tilde{P}\in(\delta\cdot\tilde{P}|\tilde{X}_P)\times E^{\tilde{X}\setminus\tilde{X}_P}$ does not belong to $\mathrm{ext}_{\tilde{X}}(\varepsilon_{P,\mathfrak{p}})\cdot r'\supseteq r^*$ and $\delta\cdot\tilde{P}\notin r^*$. Therefore, $\delta\cdot\tilde{P}\in r^*$ iff $\delta\in D$. Thus the equivalence theorem of of abstract Galois endotheory is proved.

Proof of the equivalence and existence theorems of abstract Galois theory. Since $\bar{R}^{(X^0)}$ is closed with respect to all fundamental operations below X^0, an argument analogous to (a) shows that if $S=(E,R)$ and $S'=(E,R')$ are equivalent below X^0 then $G_{E/S}=G_{E/S'}$. We have already seen (cf. Remark 1 in Section 1) that if σ is a permutation and both σ and σ^{-1} stabilize a relation r then σ preserves r. Consequently, if a monoid G consisting of some self-mappings of E happens to be a group, i.e., a permutation group on E, then every $\sigma\in G$ even preserves and not only stabilizes all $r\in R_G^{(X^0)}$. Therefore $R_G^{(X^0)}=s\text{-}\mathrm{Inv}^{(X^0)}G=p\text{-}\mathrm{Inv}^{(X^0)}G$ and, if card $X^0\geqq\mathrm{card}\,E$, G is the stability monoid and also the preservation monoid of $E/R_G^{(X^0)}$. Hence for any permutation group G on E there exists a structure $S=(E,R)$ such that $G=G_{E/S}$, which proves the existence theorem of abstract Galois theory.

Considering the particular case $D=G$ and keeping the notations of (c) of the preceding proof we have $G\cdot(\tilde{P}|\tilde{X}_P)=(\varepsilon_{P,\mathfrak{p}})\cdot(G\cdot\tilde{P})$ and $G\cdot P=[\varepsilon_{P,\mathfrak{p}}]\cdot(G\cdot\tilde{P}|\tilde{X}_P)$. If $G=G_{E/S}$ then $R\subseteq R_G^{(X^0)}$ and, as $R_G^{(X^0)}$ is closed with respect to all fundamental operations, $R_f^{(X^0)}\subseteq R_G^{(X^0)}$. Since $G\cdot\tilde{P}$ and $R_G^{(X^0)}$ are equivalent (and even directly equivalent), to prove $R_f^{(X^0)}=R_G^{(X^0)}$ it is sufficient to show $G\cdot\tilde{P}\in R_f^{(X^0)}$.

Let $S=(E,R)$ be a structure under X^0 with card $X^0\geqq\mathrm{card}\,E$ and let $G=G_{E/S}$. Consider $S^*=(E,R\cup\neg R)=(E,R^*)$ where $\neg R=\{\neg r; r\in R\}$. Then S and S^* are equivalent below X^0 (really, $R\subseteq R^*$ and $R^*\subseteq R_f^{(X^0)}$) and $G_{E/S^*}=G_{E/S}$. Thus it suffices to prove $G\cdot\tilde{P}\in R_f^{*(X^0)}$, i.e., to prove $G\cdot\tilde{P}\in R_f^{(X^0)}$ under the hypothesis $R=\neg R$. In this case, by Remark 2 of Section 1, we have $G_{E/S}=D_{E/S}\cap S(E)$. As $\tilde{P}$ is bijective, $\delta\to\delta\cdot\tilde{P}$ is injective, implying $G\cdot\tilde{P}=D\cdot\tilde{P}\cap S(E)\cdot\tilde{P}$, where $D=D_{E/S}$. If δ is an injective, surjective or bijective self-mapping of E then $\delta\cdot\tilde{P}$ is injective, surjective or bijective as well, respectively. I. e., $S(E)\cdot\tilde{P}$ is the set of all bijective $\tilde{X}$-points while $G\cdot\tilde{P}$ is the set of all bijective points of $D\cdot\tilde{P}$. On the other hand, $r^*=D\cdot\tilde{P}\in R_{df}^{(X^0)}\subseteq R_f^{(X^0)}$ has already been proved. Hence it is sufficient to show that the set of all bijective points of $r^*=D\cdot\tilde{P}$ can be obtained from this relation via a combination of fundamental operations.

First, an $\tilde{X}$-point $\tilde{Q}$ is not injective iff there exist $x,y\in\tilde{X}$, $x\neq y$, such that $\tilde{Q}\cdot x=\tilde{Q}\cdot y$, i.e., iff $\tilde{Q}\in\mathrm{ext}_{\tilde{X}}\cdot D_{x,y}$. Therefore the set of injective points of r is

$$r^{**}=r^*\cap(\neg\cdot\bigcup_{\substack{x,y\in\tilde{X}\\ x\neq y}}D_{x,y})=r^*\cap(\bigcap_{\substack{x,y\in\tilde{X}\\ x\neq y}}(\neg\cdot D_{x,y})).$$

As we do not want to use the axiom of choice, two cases have to be handled even if E is infinite.

(1) There exists no bijection from E (and also of $\tilde{X}$) onto any of its proper subsets. Then every injective $\tilde{X}$-point of E is surjective and r^{**} is the set of all bijective points of r^*. Now r^{**} is obtained from r^* and from simple diagonals via infinitary boolean operations, whence (cf. Remark 10 of Section 2 and the discussion of operations IV. 1-2 in the same section) r^{**} can be obtained from r^* via a combination of fundamental operations; which was to be proved.[1]

(2) There exist bijections from E onto some of its proper subsets. Then a set $\tilde{X}$ ($\tilde{X}\subseteq X^0$) and a mapping $\tilde{P}$ can be chosen so that $\tilde{X}\neq X^0$. Let y be an element of $X^0\setminus\tilde{X}$ and put $X'=\tilde{X}\cup\{y\}$. Let $\tilde{Q}\colon\tilde{X}\to E$ be an injective point and consider an arbitrary $\tilde{Q}'\in\{\tilde{Q}\}\times E^{\{y\}}$. Now, if $\tilde{Q}$ is bijective (i.e., surjective) then $\tilde{Q}'\cdot y$ belongs to $E=\tilde{Q}\cdot\tilde{X}=(\tilde{Q}'|\tilde{X})\cdot\tilde{X}$. Hence there exists an $x\in\tilde{X}$ such that $\tilde{Q}'\cdot x=\tilde{Q}'\cdot y$. I.e., $\tilde{Q}'$ cannot be injective. Conversely, if $\tilde{Q}$ is not surjective then there are an $e\in E$ and a $\tilde{Q}'$ such that $e\notin\tilde{Q}\cdot\tilde{X}$, $\tilde{Q}'\cdot y=e$ and $\tilde{Q}'$ is injective. So when $\tilde{Q}'$ ranges over the set of all injective points of $\mathrm{ext}_{X'}\cdot r^{**}$ then $(\tilde{Q}'|\tilde{X})$ ranges over the set of all non-bijective points of r^{**}. The set of injective points of $\mathrm{ext}_{X'}\cdot r^{**}$ is, visibly,

$$\mathrm{ext}_{X'}\cdot r^{**}\cap(\neg\cdot\bigcup_{x\in\tilde{X}}\mathrm{ext}_{X'}\cdot D_{x,y}).$$

[1]) Originally I proved the equivalence theorem of abstract Galois theory without using the axiom of choice under the assumption card $X^0\geqq$ card $E+1$. It was B. Poizat who found the present proof with card E instead of card $E+1$ for the case (1). P. Jurie proved that card E can be replaced even by card $E-1$ when E is finite.

Therefore the set of bijective points of r^{**} is

$$G\cdot\bar{P} = r^{***} = r^{**}\cap(\neg\cdot \mathrm{pr}_{\mathfrak{X}}\cdot(\mathrm{ext}_{X'}\cdot r^{**}\cap(\neg\cdot\bigcup_{x\in\mathfrak{X}}\mathrm{ext}_{X'}\cdot D_{x,y}))),$$

which is obtained from r^{**} and also from $r^{*}=D\cdot\bar{P}$ via a combination of fundamental operations. This completes the proof.

Remark 1. If $\mathrm{card}\,X^0\geqq\mathrm{card}\,E$ then we have $\bar{R}^{(X^0)}=R_f^{(X^0)}$ and $\bar{\bar{R}}^{(X^0)}=R_{df}^{(X^0)}$.

Indeed, we have seen that $D_{E/\bar{\bar{R}}^{(X^0)}}=D_{E/R}$ and $G_{E/\bar{R}^{(X^0)}}=G_{E/R}$. Thus the equivalence theorems together with the fact that $\bar{\bar{R}}^{(X^0)}$ resp. $\bar{R}^{(X^0)}$ is closed with respect to direct resp. to all fundamental operations yield

$$R_{df}^{(X^0)} = (\bar{\bar{R}}^{(X^0)})_{df}^{(X^0)} = \bar{\bar{R}}^{(X^0)} \quad\text{and}\quad R_f^{(X^0)} = (\bar{R}^{(X^0)})_f^{(X^0)} = \bar{R}^{(X^0)}.$$

This means that a relation under X^0 belongs to $R_{df}^{(X^0)}$ iff it is stabilized by all selfmappings of E that stabilize every $r\in R$, and, analogously, it is in $R_f^{(X^0)}$ iff it is preserved by all permutations of E that preserve every $r\in R$.

Remark 2. Let S and S' be structures under X^0, where $\mathrm{card}\,X^0\geqq\mathrm{card}\,E$. It follows from the equivalence theorems that it does not depend on the particular choice of X^0 whether S and S' are (directly) equivalent below X^0 or not. Therefore the notion of equivalence and that of direct equivalence can be defined without any reference to a particular X^0 in the following way: Two structures, S and S', are said to be equivalent resp. directly equivalent (in notation $S\sim S'$ resp. $S\underset{d}{\sim}S'$) if there exists a set X^0 such that $\mathrm{card}\,X^0\geqq\mathrm{card}\,E$, S and S' are under X^0, and S and S' are equivalent resp. directly equivalent below X^0.

In particular, if R and R' are under X^0 and $X^{0\prime}\supseteqq X^0$ then we have

$$R_{df}^{(X^{0\prime})}\cap R_E^{(X^0)} = R_{df}^{(X^0)},\quad R_f^{(X^{0\prime})}\cap R_E^{(X^0)} = R_f^{(X^0)},$$
$$R_{df}^{(X^{0\prime})} = (R_{df}^{(X^0)})_{df}^{(X^{0\prime})},\quad\text{and}\quad R_f^{(X^{0\prime})} = (R_f^{(X^0)})_{df}^{(X^{0\prime})}.$$

Thus a set of relations under $X^{0\prime}$, which is closed with respect to direct resp. all fundamental operations and its part below X^0, which is also closed with respect the same operations below X^0, mutually determine each other. More generally, if $\mathrm{card}\,X^0\geqq\mathrm{card}\,E$ and $\mathrm{card}\,X^{0\prime}\geqq\mathrm{card}\,E$ and R is under $X^0\cap X^{0\prime}$ then $R_{df}^{(X^0)}$ and $R_{df}^{(X^{0\prime})}$ mutually determine each other (because any of them is characterized by $R_{df}^{(X^0\cup X^{0\prime})}$), and so do $R_f^{(X^0)}$ and $R_f^{(X^{0\prime})}$.

Remark 3. We are going to define two preorders, the thin (alias direct) Galois preorder $\underset{d}{\leqq}$ and the thick Galois preorder $\leqq$. For structures $S=(E,R)$ and $S'=(E,R')$ we write $S\underset{d}{\leqq}S'$ resp. $S\geqq S'$ if there is a set X^0 such that $\mathrm{card}\,X^0\geqq\mathrm{card}\,E$, S and S' are under X^0 and $R_{df}^{(X^0)}\subseteqq R_{df}'^{(X^0)}$ resp. $R_f^{(X^0)}\subseteqq R_f'^{(X^0)}$. Note that $\underset{d}{\sim}$ and $\sim$ are the equivalence hulls of $\underset{d}{\leqq}$ and $\leqq$, respectively. For a structure S under

X^0 let $C_{de}^{(X^0)}(S)$ and $C_e^{(X^0)}(S)$ denote the $\underset{d}{\sim}$-class and $\sim$-class of S, respectively. Then, by the equivalence theorems, the mappings $C_{de}^{(X^0)}(S) \to D_{E/S}$ and $C_e^{(X^0)}(S) \to \to G_{E/S}$ are injective, are decreasing with respect to the orders $\underset{d}{\leqq}$ and $\leqq$, and do not depend on the choice of X^0. (Here the orders are induced by the similarly denoted preorders.) These mappings map $R_E^{(X^0)}/\underset{d}{\sim}$ and $R_E^{(X^0)}/\sim$, which do not depend on X^0, onto the set of semigroups of self-mappings of E that contain 1_E and onto the set of permutation groups on E, respectively. (This is an easy consequence of the existence theorems.)

Remark 4. Let $S=(E, R)$ be a structure under X^0, where card $X^0 \geqq$ card E, put $D=D_{E/S}$, let $\tilde{X}$ be a subset of X^0 with card $\tilde{X}$=card E, and let $\tilde{P}$: $\tilde{X} \to E$ be a bijective point. We have seen that any relation in $R_{df}^{(X^0)}=R_D^{(X^0)}=\bar{R}^{(X^0)}$ can be obtained from $D \cdot \tilde{P}$ via a combination of direct fundamental operations. (More precisely, first projections, then dilatations and finally an infinitary union have to be applied.)

Case of finite base set. In case E has only a finite number of elements, say m elements, it suffices to take a finite set $X^0=\{x_1, \dots, x_n\}$ with $n \geqq m$ in the equivalence and existence theorems. If $S=(E, R)$ is a structure under this X^0 then R is a finite set of relations. Further, the infinitary boolean operations are, in fact, the ordinary ones. So every structure can be considered as a model (with base set E) of some finite system $P_1(X_1), \dots, P_s(X_s)$ of predicates (with no axioms). (Here each $P_i(X_i)$ depends on a set $X_i \subseteqq X^0$ of object variables.) By a *model* (with base set E) of the previous system of predicates we mean a mapping r: $P_i(X_i) \to r(P_i)$ $(i=1, \dots, s)$ where $r(P_i)$ is an X_i-relation on E. This mapping will be extended, in the following way, to a mapping $F \to r(F)$ from the set of all formulas $F=F(P_1, \dots, P_s)$ obtained from $P_1, \dots, P_s$ via the operations of the predicate calculus with equality, used below X^0, into the set of relations under X^0. Firstly, these operations are generated by the following ones via superposition:

(1) *disjunction*, i.e., $(P, Q) \to P \vee Q$;

(2) *conjunction*, i.e., $(P, Q) \to P \& Q$;

(3) *negation*, i.e., $P \to \neg P$;

(4) *existential quantification*, i.e., $P(X) \to (\exists x) P(X)$ where $x \in X \subseteqq X^0$;

(5) *adjunction of a set of fictitious variables*, i.e., $P(X) \to P^{X'}(X')$ where $X \subseteqq \subseteqq X' \subseteqq X^0$ and $X' \setminus X$ is the set of fictitious variables;

(6) *floatages*, i.e., $P(X) \to P^{\lambda}(\lambda \cdot X)$ where λ is a bijection of $X=\{x_{i(1)}, x_{i(2)}, \dots, x_{i(t)}\}$ $(1 \leqq i(1) < i(2) < \dots < i(t) \leqq n)$ onto a subset $\lambda \cdot X$ of X^0 and
$P^{\lambda}(\lambda \cdot x_{i(1)}, \dots, \lambda \cdot x_{i(t)}) = P(x_{i(1)}, \dots, x_{i(t)})$;

(7) *adjunction of equality predicates* $x=y$ $(x, y \in X^0)$, which may be proper equality predicates if x and y are distinct or the *x-identity* predicates $x=x$.

It is not hard to see that any fundamental operation is a superposition of some of these seven kinds of operations. Really, $\cup$ and $\cap$ are iterations of disjunctions and conjunctions, pr_Y is a suitable iteration of (4), contractions can be composed from projections and (6), and any dilatation $[\psi]$ is a superposition of a floatage, of an extension, and of an intersection with some simple diagonals (see the discussion on the axiom of choice after the definition of direct fundamental operations). The above considerations allow us to extend r to all formulas $F(P_1, \ldots, P_s)$ below X^0 in the following obvious way, via induction: put

(1) $r(P \vee Q) = r(P) \cup r(Q)$,

(2) $r(P \& Q) = r(P) \cap r(Q)$,

(3) $r(\neg P) = \neg r(P)$,

(4) $r((\exists X) P(X)) = \mathrm{pr}_{X \setminus \{x\}} r(P(X))$,

(5) $r(P^{X'}) = \mathrm{ext}_{X'} r(P)$,

(6) $r(P^\lambda) = (\lambda) \cdot r(P)$,

(7) $r(x=y) = D_{x,y}$ if x and y are distinct while $r(x=x) = I(\{x\}; E) = E^{\{x\}}$.

Now it is clear that the set of all $r(F(P_1(X_1), \ldots, P_s(X_s)))$, where $F = F(T_1(X_1), \ldots, T_s(X_s))$ ranges over all formulas of the predicate calculus with equality sign that depend on the predicate variables $T_1(X_1), \ldots, T_s(X_s)$, coincides with the logical closure $R_f^{(X^0)}$ of $R = \{r(P_1), \ldots, r(P_s)\}$ below X^0. On the other hand, it is easy to see that the realizations (i.e., r-images) of the operations $T \vee T'$, $T \& T'$, $(\exists x) T(X)$ for $x \in X$, $T(X) \to T^{X'}(X')$ for $X \subseteq X'$, $T \to T^\lambda$, the adjunction of $x=y$ and also of $\neg(x=x)$ are direct fundamental operations. Conversely, every direct fundamental operation is the realization of an appropriate superposition of these operations. Let us call the part of predicate calculus (below X^0) generated by these operations *strictly positive predicate calculus* (below X^0). Then $R_{df}^{(X^0)}$ is the set of $r(F(P_1, P_2, \ldots, P_s))$ where $F(T_1, \ldots, T_s)$ ranges over the formulas of strictly positive predicate calculus (below X^0) that depend on the predicate variables $T_i = T_i(X_i)$ $(i = 1, 2, \ldots, s)$. So we have

Equivalence theorems for a finite base set E. *Let* $M = (E; P_i(X_i) \to r_i \subseteq E^{X_i}$ $(i=1, \ldots, s))$ *be a model of a system of predicates* $\{P_i(X_i); i = 1, 2, \ldots, s\}$. *Then a relation* r *on* E *is of the form* $r(F(P_1, \ldots, P_s))$ *for some formula*

$F(T_1(X_1), \ldots, T_s(X_s))$ of the predicative resp. strictly predicative calculus below X^0 if and only if r is preserved resp. stabilized by all $\sigma \in S(E)$ resp. $\delta \in D(E)$ that preserve resp. stabilize all r_i $(i=1, \ldots, s)$. (The set X^0 is supposed to contain all X_i and to have at least as many elements as E.)

Examples of some classical structures

1. *The structure of the classical Galois theory.* Let E/k be a commutative field extension which is normal algebraic or algebraically closed. Consider two $\{x, y, z\}$-relations on E, $+(x, y, z)$ and $\times(x, y, z)$ such that $P \in +(x, y, z)$ iff $P \cdot x + P \cdot y = P \cdot z$ and $P \in \times(x, y, z)$ iff $(P \cdot x)(P \cdot y) = P \cdot z$. For $e \in E$ let $(x; e)$ denote the $\{x\}$-relation on E with the property $P \in (x; e)$ iff $P \cdot x = e$. Put $R_0 = \{+(x, y, z), \times(x, y, z)\} \cup \{(x; \alpha);\ \alpha \in k\}$, and let A be a subset of E. We can consider the structure $S = S_0(A) = (E, R_0 \cup \{(x; a);\ a \in A\})$. Then $G_{E/S}$ coincides with the ordinary Galois group of the field extension $E/k(A)$ while $D_{E/S}$ is the monoid of all isomorphisms of $E/k(A)$ into E. Note that $G_{E/S}$ and $D_{E/S}$ are the same when $E/k(A)$ is algebraic.

For $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ let $(f=0)$ denote the $\{x_1, \ldots, x_n\}$-relation on E such that an $\{x_1, \ldots, x_n\}$-point P belongs to $(f=0)$ iff $f(P \cdot x_1, \ldots, P \cdot x_n) = 0$. Then

$$+(x, y, z) = (x+y-z=0), \quad \times(x, y, z) = (xy-z=0) \quad \text{and} \quad (x; e) = (x-e=0).$$

Let

$$R_0' = \{(f=0);\ f \in k[x_1, x_2, \ldots] = k[\{x_n;\ n \in \mathbf{N}^*\}]\}$$

(here $\mathbf{N}^*$ stands for the set of positive natural numbers).

We claim that R_0 *and* R_0' *are deducible from one another* by means of direct fundamental operations. Really, a standard argument shows that the same self-mappings of E stabilize R_0 as R_0', whence the equivalence theorem of abstract Galois endotheory yields this assertion.

The aim of the classical Galois theory, as we have seen it in the introduction, is to determine the set $\bar{A}$ of all $\bar{a} \in E$ that are preserved by each $\sigma \in G_{E/k(A)}$. (Note that $\bar{A}$ coincides with the set $\bar{A}$ of all elements in E that are preserved by each $\delta \in D_{E/k(A)}$.) It is clear that $\sigma \cdot \bar{a} = \bar{a}$ is equivalent to $\sigma \cdot (x; \bar{a}) = (x; \bar{a})$. The abstract Galois theory answers this problem by describing $\bar{A}$ as follows:

$$\bar{a} \in \bar{A} \quad \text{iff} \quad (x; \bar{a}) \in (R_0 \cup \{(x; a);\ a \in A\})_f = (R_0' \cup \{(x; a);\ a \in A\})_f.$$

On the other hand, the classical Galois theory says that $\bar{A}$ is the closure of $k \cup A$ with respect to addition $x+y$, multiplication xy (both defined on $E \times E$), inversion x^{-1} (defined on $E^* = E \setminus \{0\}$) and, when the characteristic p of k is not 0, forming of

pth roots $\sqrt[p]{x}$ (defined on $E^p=\{x^p;\ x\in E\}$). The second result can be deduced from the first by means of "abstract Galois set theory", to be exposed in Section 6, and of the theory of "eliminative structures", to be exposed elsewhere. Although this deduction is quite complicated, it reveals deep reasons why the operations $x+y$, xy, x^{-1} and $\sqrt[p]{x}$, and only these operations, occur in the above-mentioned result of the classical Galois theory. Moreover, it can be shown that $\{G_{E/k(A)};\ A\subseteqq E\}$ is the set of all subgroups of $G_{E/k}$ that are closed with respect to the finite topology ("Krull topology") on $D(E)$, provided E/k is algebraic.

2. *A slightly different structure* is obtained if we replace $(x;e)=(x-e=0)$ by $(x,y;e)=(y-ex=0)$. I.e., R_0 is replaced by

$$R_0^* = \{+(x,y,z),\ \times(x,y,z)\}\cup\{(x,y;\alpha);\ \alpha\in k\}$$

and $R_0(A)$ by

$$R_0^*(A) = \{(x,y;a);\ a\in A\}\cup R_0^*.$$

Let $S_0^*(A)$ stand for $(E, R_0^*(A))$. Then we have $G_{E/S_0^*(A)}=G_{E/S_0(A)}$, i.e., $S_0^*(A)\sim\sim S_0(A)$. Indeed,

$$(y-ex=0) = \mathrm{pr}_{\{x,y\}}\cdot((y-zx=0)\cap(z-e=0))$$

and

$$(x-e=0) = \mathrm{pr}_{\{x\}}\cdot((x-ey=0)\cap\mathrm{pr}_{\{x,y\}}\,\mathrm{ext}_{\{x,y,z,t\}}\cdot$$
$$\cdot((yz-t=0)\cap\neg(y+z-t=0)\cap D_{\{y,z,t\}}(E))).$$

Similarly, $D_{E/S_0^*(A)}=D_{E/S_0(A)}\cup\{0\}$, where 0 denotes $E\to\{0\}$, the zero homomorphism of E.

3. *Linear Galois theory*. Let k be a not necessarily commutative field, and let E/k be a field extension. We consider

$$R_0^{(L)} = \{+(x,y,z)\}\cup\{(x,y;\ \alpha);\ \alpha\in k\}$$

and

$$S_0^{(L)}(A) = (E, R_0^{(L)}\cup\{(x,y;\ a);\ a\in A\}).$$

The stability monoid $D_{E/S_0^{(L)}(A)}$ of $E/S_0^{(L)}(A)$ is the semigroup $\Lambda_{E/k(A)}$ of all linear transformations $\lambda\colon E\to E$ of the left vector space E over the field $k(A)$ (the field generated by $k\cup A$), while the Galois group $G_{E/S_0^{(L)}(A)}$ of $E/S_0^{(L)}(A)$ is the group of bijective linear transformations of the same vector space, i.e., it is the general linear group $GL_{k(A)}(E)$ of E over $k(A)$. The two main questions of this theory in classical algebra are the following: how to determine the set $\bar{A}$ of all $\bar{a}\in E$ such that every $\delta\in D_{E/S_0^{(L)}(A)}$ stabilizes $(x,y;\bar{a})$; and which submonoids of $D_{E/S_0^{(L)}}=\Lambda_{E/k}$ are of the form $D_{E/S_0^{(L)}(A)}$ for some $A\subseteqq E$. It can be shown, in an elementary, way, that $\bar{A}=k(A)$. As regards the second question, Jacobson's density theorem yields the following answer. For a given $e \in E$ let (e) denote the linear transformation $x \to xe$ of the left vector space E/k, and put $(E) = \{(e);\ e \in E\}$. Then (E) is a field with respect to the addition and multiplication in $\Lambda_{E/k}$, and (E) is anti-isomorphic to E. Now, a submonoid Λ of $\Lambda_{E/k}$ is of the form $D_{E/S_0^{(L)}}$ for some $A \subseteqq E$ if and only if Λ is a subring of $\Lambda_{E/k}$ containing (E) and closed with respect to the finite topology on $D(E)$, the set of self-mappings of E.

4. *Homogeneous Galois theory*. Let E/k be the same as in the first example; we put

$$R_0^{(h)} = \{+(x, y, z),\ \pi(x, y, z, t) = (xy - zt = 0)\} \cup \{(x; \alpha);\ \alpha \in k\}$$

and

$$R_0^{(h)}(A) = R_0^{(h)} \cup \{(x; a);\ a \in A\}.$$

It is easy to show that $G_{E/R_0^{(h)}(A)}$ and $D_{E/R_0^{(h)}(A)}$ are the group generated by the ordinary Galois group $G_{E/k(A)}$ together with the group

$$(E^*) = \{(e)\colon x \to xe;\ e \in E^* = E \setminus \{0\}\}$$

of multiplications by the non-zero elements of E, and the semigroup generated by the ordinary stability monoid $D_{E/k(A)}$ together with (E^*). In order to describe the set $\bar{A}$ of all elements $\bar{a} \in E$ that are preserved by every $\sigma \in G_{E/R_0^{(h)}(A)}$, which is the same as the set of elements preserved by all $\delta \in D_{E/R_0^{(h)}(A)}$, let $\hat{k}(B)$ denote the perfect closure (in E) of the field $k(B)$ generated by B (where $B \subseteqq E$). Then $\bar{A} = a\hat{k}(a^{-1}A) = a\hat{k}(\{a^{-1}b;\ b \in A\})$ for some (moreover, for any) non-zero element a in A, and $\overline{\{0\}} = \{0\}$. Finally, note that $R_0^{(h)}$ can be replaced, up to direct equivalence, by the set

$$\{(f = 0);\ f \in k[x_1, x_2, \ldots] \text{ and } f \text{ is homogeneous}\}.$$

References

[1] M. Krasner, Une generalisation de la notion de corps, *J. Math. Pures Appl.*, **17** (1938), 367—385.

[2] M. Krasner, Generalisation abstraite de la théorie de Galois, in: *Algebra and Number Theory* (24th International Colloquium of CNRS, Paris, 1949), 1950; pp. 163—168.

[3] M. Krasner, Endothéorie de Galois abstraite, in: *Proceedings of the International Math. Congress* (Moscow, 1966), Abstracts 2 (Algebra), p. 61.

[4] M. Krasner, Endothéorie de Galois abstraite, *P. Dubreil Seminar* (Algebra and Number Theory), 22/1 (1968—1969), no. 6.

[5] M. Krasner, Endothéorie de Galois abstraite et son théoreme d'homomorphie; *C. R. Acad. Sci. Paris*, **232** (1976), 683—686.

[6] B. Poizat, Third cycle thesis, 1967.

[7] P. Lecomte, Doctoral thesis.

Acta Sci. Math., 50 (1986), 287—298

Rédei-Funktionen und ihre Anwendung in der Kryptographie

RUPERT NÖBAUER[1])

1. Einleitung. In [8] hat L. Rédei eine Klasse von rationalen Funktionen über einem endlichen Körper K ungerader Ordnung untersucht, die Permutationen von K induzieren.

In der vorliegenden Arbeit erfolgt nun u.a. eine Übertragung der von L. Rédei gefundenen Ergebnisse von endlichen Körpern K auf Restklassenringe $Z/(m)$ des Rings der ganzen rationalen Zahlen modulo ungerader natürlicher Zahlen m. In Abschnitt 2 werden rationale Funktionen über $Z/(m)$ definiert, die den von L. Rédei untersuchten Funktionen entsprechen und die daher als Rédei-Funktionen bezeichnet werden. Es wird gezeigt, daß bestimmte Mengen von Permutationen von $Z/(m)$, die durch solche Rédei-Funktionen induziert werden, bezüglich der Komposition Gruppen bilden. In Abschnitt 3 wird die Anzahl der Fixpunkte der durch Rédei-Funktionen induzierten Permutationen von $Z/(m)$ berechnet. In Abschnitt 4 wird die Struktur von durch Rédei-Funktionen induzierten Permutationsgruppen von $Z/(m)$ ermittelt, und es werden alle ungeraden m bestimmt, für die diese Gruppen zyklisch sind. In Abschnitt 5 wird u.a. gezeigt, daß es für jedes ungerade $m \geqq 3$ Permutationen von $Z/(m)$ gibt, die durch Rédei-Funktionen induziert werden und die nur *einen* Fixpunkt aufweisen, und es wird eine Aussage über die Anzahl derartiger Permutationen hergeleitet.

In Abschnitt 6 erfolgt die Beschreibung eines Public-Key Kryptosystems — also eines Verschlüsselungssystems mit öffentlich bekanntem Schlüssel (vgl. [1]) — auf der Basis von Rédei-Funktionen. Das Verfahren kann als Variante des RSA-Schemas (siehe etwa [9]) angesehen werden: Beim RSA-Schema erfolgt die Verschlüsselung der Nachrichten mit Hilfe solcher Permutationen von $Z/(m)$, die durch Potenzen x^n induziert werden, beim vorliegenden System erfolgt sie mit Hilfe von durch

Received March 21, 1984 and in revised form July 17, 1984.

[1]) Der Autor dankt dem Institut für Mathematik der Universität Klagenfurt für die Ermöglichung dieser Arbeit. Weiters dankt der Autor dem Referenten für wertvolle Verbesserungsvorschläge.

Rédei-Funktionen induzierten Permutationen. Das vorliegende System ist eine Verallgemeinerung des von R. LIDL und W. B. MÜLLER in [3] vorgeschlagenen Systems, und zwar von $Z/(m)$, m quadratfrei, auf $Z/(m)$, m beliebig.

2. Einige grundlegende Tatsachen. Wir wollen zunächst einige allgemeine Bemerkungen über rationale Funktionen machen, die Permutationen von $Z/(m)$ induzieren. Sei m eine beliebige natürliche Zahl und sei $f(x)=g(x)/h(x)$ Quotient von ganzzahligen Polynomen, welche teilerfremd in $Z[x]$ sind. Man nennt $f(x)$ Permutationsfunktion von $Z/(m)$, wenn $h(u)$ für jedes ganze u eine prime Restklasse mod m ist und wenn die Abbildung $\pi: u \to g(u)h(u)^{-1}$ mod m von $Z/(m)$ in sich eine Permutation ist (vgl. [6]). Ist speziell $h(x)=1$ und $f(x)=g(x)/1$ eine Permutationsfunktion von $Z/(m)$, so nennt man $f(x)$ Permutationspolynom von $Z/(m)$. Ist $m=ab$ mit[2] $(a,b)=1$, so ist $f(x)$ genau dann Permutationsfunktion von $Z/(ab)$, wenn es Permutationsfunktion von $Z/(a)$ und von $Z/(b)$ ist. Weiters ist $f(x)$ genau dann Permutationsfunktion von $Z/(p^e)$, $e>1$, wenn gilt: $f(x)$ ist Permutationsfunktion von $Z/(p)$, und $f'(u)\not\equiv 0$ mod p für jedes ganze u (vgl. [6]).

Man nennt zwei Permutationsfunktionen $f_1(x)$, $f_2(x)$ von $Z/(m)$ äquivalent, wenn es ein lineares Polynom $p(x)=cx+d$, $(c,m)=1$, gibt, sodaß gilt

$$f_2(x) = p^{-1}(x)\circ f_1(x)\circ p(x),$$

wobei $p^{-1}(x)$ das bezüglich der Komposition $\circ$ zu $p(x)$ inverse Polynom $c^{-1}x-c^{-1}d$ bezeichnet.

Sei n eine ungerade natürliche Zahl, und sei α eine ganze Zahl mit α Nichtquadratelement in Z, also mit α Nichtquadratelement in Q, dem Körper der rationalen Zahlen. Seien $g_n(x)$, $h_n(x)\in Z[x]$ definiert durch

$$(x+\sqrt{\alpha})^n = g_n(x)+h_n(x)\sqrt{\alpha}. \tag{2.1}$$

Eine explizite Darstellung von $g_n(x)$ und $h_n(x)$ ist gegeben durch[3]

$$g_n(x) = \sum_{i=0}^{[n/2]} \binom{n}{2i} \alpha^i x^{n-2i}, \quad h_n(x) = \sum_{i=0}^{[n/2]} \binom{n}{2i+1} \alpha^i x^{n-2i-1}.$$

Es gilt $h_n(x)\neq 0$ in $Q(\sqrt{\alpha})(x)$, dem rationalen Funktionenkörper über $Q(\sqrt{\alpha})$, und somit $h_n(x)\neq 0$ in $Z[x]$. Denn wäre $h_n(x)=0$, so würde folgen $(x+\sqrt{\alpha})^n = g_n(x)$, also $(\sqrt{\alpha})^n\in Z$, und dies ergäbe einen Widerspruch.

Die Polynome $g_n(x)$, $h_n(x)$ sind teilerfremd in $Z[x]$, denn für $d_n=(g_n(x), h_n(x))$ erhält man aus (2.1) durch Herausheben von $d_n(x)$ unter Beachtung der Tatsache,

[2]) $(a_1, \ldots, a_n)$ bezeichne den größten gemeinsamen Teiler, $[a_1, \ldots, a_n]$ das kleinste gemeinsame Vielfache der Zahlen $a_1, \ldots, a_n$.

[3]) $[a]$ bezeichne die nächstkleinere ganze Zahl von a.

daß $Q(\sqrt{\alpha})[x]$ ein ZPE-Ring ist: $d_n(x)=(x+\sqrt{\alpha})^s$ mit $0\leqq s<n$. Daraus ergibt sich $s=0$, also $d_n(x)=1$.

Wir setzen nun $f_n(x)=g_n(x)/h_n(x)$. Nach den obigen beiden Bemerkungen ist der Nenner $h_n(x)$ der rationalen Funktion $f_n(x)$ von 0 verschieden, und die Darstellung $g_n(x)/h_n(x)$ ist bereits gekürzt. In $Q(\sqrt{\alpha})(x)$ gilt

$$\left(\frac{x+\sqrt{\alpha}}{x-\sqrt{\alpha}}\right)^n=\frac{f_n(x)+\sqrt{\alpha}}{f_n(x)-\sqrt{\alpha}}. \tag{2.2}$$

Daraus folgt

$$\frac{f_{kn}(x)+\sqrt{\alpha}}{f_{kn}(x)-\sqrt{\alpha}}=\frac{f_k(f_n(x))+\sqrt{\alpha}}{f_k(f_n(x))-\sqrt{\alpha}},$$

und man erhält

$$f_k(x)\circ f_n(x)=f_{kn}(x) \tag{2.3}$$

für beliebige natürliche Zahlen k und n.

Für eine ungerade Zahl $m=p_1^{e_1}\dots p_r^{e_r}$ soll die Menge aller Permutationen von $Z/(m)$ untersucht werden, die durch bestimmte Permutationsfunktionen $f_n(x)$ induziert werden. Daher wird als erstes nach Bedingungen gefragt, under denen $f_n(x)$ Permutationsfunktion von $Z/(m)$ ist.

Es sei $m=p^e$ (p ungerade Primzahl, $e\geqq 1$), α ein quadratischer Nichtrest mod p und n eine natürliche Zahl mit $(n, p^{e-1}(p+1))=1$, dann ist $f_n(x)$ Permutationsfunktion von $Z/(p^e)$. Für $e=1$ folgt dies aus der Arbeit von L. Rédei [8]. Für $e>1$ erhält man aus (2.2) durch beiderseitiges Differenzieren

$$n\left(\frac{x+\sqrt{\alpha}}{x-\sqrt{\alpha}}\right)^{n-1}\frac{-2\sqrt{\alpha}}{(x-\sqrt{\alpha})^2}=\frac{-2f_n'(x)\sqrt{\alpha}}{(f_n(x)-\sqrt{\alpha})^2},$$

also

$$f_n'(x)=\frac{n(x+\sqrt{\alpha})^{n-1}(f_n(x)-\sqrt{\alpha})^2}{(x-\sqrt{\alpha})^{n+1}}=$$

$$=\frac{n(x^2-\alpha)^{n-1}(f_n(x)-\sqrt{\alpha})^2}{(x-\sqrt{\alpha})^{2n}}=\frac{n(x^2-\alpha)^{n-1}(f_n(x)-\sqrt{\alpha})^2}{(g_n(x)-h_n(x)\sqrt{\alpha})^2}=\frac{n(x^2-\alpha)^{n-1}}{h_n(x)^2},$$

und daraus folgt $f_n'(u)\not\equiv 0 \mod p$ für alle ganzen u. Wir nennen derartige Permutationsfunktionen Rédei-Funktionen. Es sei P_{p^e} die Menge aller jener Permutationen von $Z/(p^e)$, die durch Rédei-Funktionen mit einem festen α induziert werden. Wegen (2.3) bildet P_{p^e} bezüglich der Komposition eine Halbgruppe, die als Unterhalbgruppe der vollen Permutationsgruppe von $Z/(p^e)$ regulär und endlich, also sogar eine Gruppe ist. (Im Spezialfall $e=1$ folgt dies ebenfalls aus [8]).

Betrachtet man den allgemeinen Fall $m=p_1^{e_1}\dots p_r^{e_r}$, so folgt aus dem Vorherigen, daß $f_n(x)$ eine Permutationsfunktion von $Z/(m)$ ist, wenn $\left(n, p_i^{e_i-1}(p_i+1)\right)=1$ gilt und α ein quadratischer Nichtrest mod p_i, $i=1, \dots, r$, ist. Ist P_m die Menge aller durch Rédei-Funktionen mit gegebenem α induzierten Permutationen von $Z/(m)$, dann bildet — wiederum wegen (2.3) — P_m eine kommutative Halbgruppe, die regulär und endlich, also sogar eine Gruppe ist.

Die Struktur dieser Gruppe ist unabhängig von der speziellen Wahl von α: Ersetzt man α durch $\alpha\beta^2$, $\beta\not\equiv 0 \bmod p_i$, $i=1, \dots, r$, so gehen die Permutationsfunktionen $f_n(x)$ über in die äquivalenten Permutationsfunktionen $\beta f_n(x/\beta)$, wie man mit Hilfe von Gleichung (2.1) leicht erkennt. Bezeichnet τ die durch βx induzierte Permutation von $Z/(m)$, so geht also P_m über in die isomorphe Gruppe $\tau P_m \tau^{-1}$.

Die Klärung der Struktur der Gruppe P_m wird in Abschnitt 4 vorgenommen; dabei wird als wesentliches Hilfsresultat die in Abschnitt 3 berechnete Anzahl der Fixpunkte von Permutationen $\pi_n \in P_m$ herangezogen.

3. Fixpunkte. Zur Berechnung der Fixpunktanzahl von Permutationen $\pi_n \in P_m$ werden Kenntnisse über einen speziellen Erweiterungsring von $Z/(p^e)$ benötigt. Sei p eine ungerade Primzahl, sei α eine ganze Zahl mit α quadratischer Nichtrest mod p, und sei $e\geqq 1$. Man bilde den Faktorring $Z[x]/(x^2-\alpha, p^e)$ des Polynomrings $Z[x]$. Da

$$u(x)(x^2-\alpha)+v(x)p^e = a \quad \text{mit} \quad a\in Z$$

dann und nur dann gilt, wenn $a\equiv 0 \mod p^e$, ist durch

$$\eta(a \mod p^e) = a \mod (x^2-\alpha, p^e)$$

ein Monomorphismus von $Z/(p^e)$ in $Z[x]/(x^2-\alpha, p^e)$ definiert, also kann man $Z/(p^e)$ in $Z[x]/(x^2-\alpha, p^e)$ einbetten. Bezeichnet man die Restklasse von x mit $\sqrt{\alpha}$, dann gilt $(\sqrt{\alpha})^2=\alpha$. Somit läßt sich jedes Element von $Z[x]/(x^2-\alpha, p^e)$ darstellen in der Form $a\sqrt{\alpha}+b$ mit $a, b\in Z/(p^e)$. Da aus

$$ax+b = u(x)(x^2-\alpha)+v(x)p^e$$

folgt $a\equiv b\equiv 0 \bmod p^e$, ist diese Darstellung eindeutig. Wir setzen im folgenden $Z(p^e, \alpha)=Z[x]/(x^2-\alpha, p^e)$.

Es gilt: Ist ξ der kanonische Epimorphismus von $Z/(p^e)$ auf $Z/(p)$, so ist durch $\delta(a\sqrt{\alpha}+b)=(\xi a)\sqrt{\alpha}+\xi b$ ein Epimorphismus von $Z(p^e, \alpha)$ auf $Z(p, \alpha)$ definiert, der ebenfalls als der kanonische Epimorphismus bezeichnet werden soll. Wir zeigen nun

Lemma 1. *Die invertierbaren Elemente von $Z(p^e, \alpha)$ sind genau die Elemente $a\sqrt{\alpha}+b$, für die nicht gleichzeitig $a\equiv 0 \mod p$ und $b\equiv 0 \bmod p$ gilt.*

Beweis. Ist $\beta\in Z(p^e, \alpha)$ invertierbar, dann ist auch $\delta\beta\in Z(p, \alpha)$ invertierbar, also gilt nicht gleichzeitig $a\equiv 0 \bmod p$ und $b\equiv 0 \mod p$. Gilt umgekehrt nicht gleichzeitig $a \equiv 0 \mod p$ und $b \equiv 0 \mod p$, dann gilt wegen der Wahl von α

$$\begin{vmatrix} b & a \\ \alpha a & b \end{vmatrix} = b^2 - \alpha a^2 \not\equiv 0 \mod p,$$

also ist die Matrix $\begin{pmatrix} b & a \\ \alpha a & b \end{pmatrix}$ über $Z/(p^e)$ invertierbar, also ist das lineare Gleichungssystem

$$bu + av \equiv 0 \mod p^e,$$
$$\alpha a u + bv \equiv 1 \mod p^e$$

lösbar, und für die Lösung des Systems gilt $(a\sqrt{\alpha}+b)(u\sqrt{\alpha}+v)=1$. Somit ist $a\sqrt{\alpha}+b$ invertierbar.

Es werde im folgenden mit G_{p^e} die Gruppe der invertierbaren Elemente von $Z(p^e, \alpha)$ bezeichnet. Wegen Lemma 1 gilt $|G_{p^e}|=(p^e)^2-(p^{e-1})^2=(p^{e-1})^2(p^2-1)$. In G_{p^e} bilden die invertierbaren Elemente von $Z/(p^e)$ eine Untergruppe Z_{p^e} der Ordnung $p^{e-1}(p-1)$. Somit gilt $|G_{p^e}/Z_{p^e}|=p^{e-1}(p+1)$.

Klarerweise ist δ ein Epimorphismus von G_{p^e} auf G_p. Grundlegend für das folgende ist

Lemma 2. *Die Gruppe G_{p^e}/Z_{p^e} ist zyklisch.*

Beweis. Da $Z(p, \alpha)$ ein Körper ist, ist G_p zyklisch. Daher ist auch G_p/Z_p zyklisch. Sei gZ_p erzeugendes Element von G_p/Z_p und sei β ein Urbild von g bei δ. Sei o die Ordnung von βZ_{p^e}, dann gilt $\beta^o \in Z_{p^e}$. Es folgt $g^o \in Z_p$, also $o=(p+1)r$. Die Ordnung des Elements $(\beta Z_{p^e})^r=\beta^r Z_{p^e}$ beträgt somit $p+1$, und wir haben gezeigt: In G_{p^e}/Z_{p^e} gibt es ein Element der Ordnung $p+1$.

Wir betrachten nun das Element $\gamma=(1+p\sqrt{\alpha})\in Z(p^e, \alpha)$. Es gilt $\gamma^{p^0}=1+ +p^1\sqrt{\alpha}+p^2 r_0$ mit $r_0 \in Z(p^e, \alpha)$. Es sei für ein i mit $0 \leqq i < e-1$ schon gezeigt, daß

$$\gamma^{p^i} = 1+p^{i+1}\sqrt{\alpha}+p^{i+2}r_i \quad \text{mit} \quad r_i \in Z(p^e, \alpha).$$

Dann gilt

$$\gamma^{p^{i+1}} = (\gamma^{p^i})^p = (1+p^{i+1}\sqrt{\alpha})^p + p^{i+3}s_i = 1+p^{i+2}\sqrt{\alpha}+p^{i+3}r_{i+1}.$$

Daraus folgt, daß die Ordnung von γZ_{p^e} den Wert p^{e-1} hat, und damit haben wir gezeigt: In G_{p^e}/Z_{p^e} gibt es ein Element der Ordnung p^{e-1}.

In abelschen Gruppen gilt: Haben zwei Elemente x_1, x_2 die teilerfremden Ordnungen o_1 und o_2, dann hat das Element $x_1 x_2$ die Ordnung $o_1 o_2$. Somit hat in G_{p^e}/Z_{p^e} das Element $\gamma\beta^r Z_{p^e}$ die Ordnung $p^{e-1}(p+1)$, und Lemma 2 ist bewiesen.

Lemma 3. *In der Gruppe G_{p^e}/Z_{p^e} bilden die Elemente $(r\sqrt{\alpha}+s)Z_{p^e}$ mit $r \equiv 0 \mod p$ eine zyklische Untergruppe der Ordnung p^{e-1}.*

Beweis. Die Menge der $r\sqrt{\alpha}+s\in G_{p^e}$ mit $r\equiv 0 \mod p$ ist die Urbildmenge von Z_p bei δ, also selbst eine Untergruppe $U_{p^e}\subset G_{p^e}$ mit $Z_{p^e}\subset U_{p^e}$. Somit ist U_{p^e}/Z_{p^e} Untergruppe von G_{p^e}/Z_{p^e}, die als Untergruppe einer zyklischen Gruppe zyklisch ist. Wegen $|U_{p^e}|=p^{e-1}(p-1)p^{e-1}$ folgt $|U_{p^e}/Z_{p^e}|=p^{e-1}$, womit Lemma 3 bewiesen ist.

Es soll nun die Anzahl der Fixpunkte der durch $f_n(x)$, $(n, p^{e-1}(p+1))=1$, induzierten Permutationen π_n von $Z/(p^e)$ bestimmt werden. Dazu zunächst eine Vorbemerkung: In $Q(\sqrt{\alpha})[x]$ bildet $Z[\sqrt{\alpha}][x]$ einen Unterring; es sei ϱ der kanonische Epimorphismus von $Z[\sqrt{\alpha}][x]$ auf $Z(p^e, \alpha)[x]$. Dann erkennt man durch Anwendung von ϱ auf (2.1), daß

$$(x+\sqrt{\alpha})^n = g_n(x)+h_n(x)\sqrt{\alpha}$$

auch in $Z(p^e, \alpha)[x]$ gilt. Zum Abzählen der Fixpunkte von π_n benötigen wir folgendes

Lemma 4. *Die Anzahl der Fixpunkte von π_n ist gleich der Anzahl der Elemente $u\in Z/(p^e)$, für welche $((u+\sqrt{\alpha})Z_{p^e})^{n-1}=Z_{p^e}$ gilt.*

Beweis. Sei u Fixpunkt von π_n. Dann gilt $f_n(u)\equiv u \mod p^e$, also $g_n(u)\equiv u\cdot h_n(u) \mod p^e$, und somit gilt in $Z(p^e, \alpha)$

$$(u+\sqrt{\alpha})^n = h_n(u)(u+\sqrt{\alpha}).$$

Da $u+\sqrt{\alpha}$ regulär ist, folgt $(u+\sqrt{\alpha})^{n-1}=h_n(u)\in Z_{p^e}$, und daher gilt $((u+\sqrt{\alpha})Z_{p^e})^{n-1}= =Z_{p^e}$.

Sei umgekehrt $((u+\sqrt{\alpha})Z_{p^e})^{n-1}=Z_{p^e}$, also $(u+\sqrt{\alpha})^{n-1}=y\in Z_{p^e}$. Dann gilt $(u+\sqrt{\alpha})^n=yu+y\sqrt{\alpha}=g_n(u)+h_n(u)\sqrt{\alpha}$, und es folgt $g_n(u)\equiv uh_n(u) \mod p^e$, d.h. $f_n(u)\equiv u \mod p^e$. Damit ist Lemma 4 bewiesen.

Da die Elemente von U_{p^e}/Z_{p^e} kein Element der Gestalt $\sqrt{\alpha}+u$, die übrigen Elemente von G_{p^e}/Z_{p^e} aber genau ein Element dieser Gestalt enthalten, ist die Anzahl der Fixpunkte von π_n gleich der Anzahl der Lösungen der Gleichung $\xi^{n-1}=1$ in der Gruppe G_{p^e}/Z_{p^e} minus der Anzahl der Lösungen in der Gruppe U_{p^e}/Z_{p^e}. Da $|G_{p^e}/Z_{p^e}|=p^{e-1}(p+1)$, gilt $\xi^{n-1}=1$ in G_{p^e}/Z_{p^e} genau dann, wenn $\xi^{(n-1, p^{e-1}(p+1))}=1$. Die Anzahl der Lösungen dieser Gleichung in der zyklischen Gruppe G_{p^e}/Z_{p^e} beträgt $(n-1, p^{e-1}(p+1))$. Ferner gilt wegen $|U_{p^e}/Z_{p^e}|=p^{e-1}$ in U_{p^e}/Z_{p^e} genau dann $\xi^{n-1}=1$, wenn $\xi^{(n-1, p^{e-1})}=1$; die Anzahl der Lösungen dieser Gleichung in der zyklischen Gruppe U_{p^e}/Z_{p^e} beträgt $(n-1, p^{e-1})$. Wegen $(n-1, p^{e-1}(p+1))= =(n-1, p^{e-1})(n-1, p+1)$ gilt also folgendes

Lemma 5. *Sei $(n, p^{e-1}(p+1))=1$. Dann ist* fix (p^e, n), *die Anzahl der Fixpunkte der durch $f_n(x)$ dargestellten Permutation von $Z/(p^e)$, gegeben durch*

$$\text{fix}\,(p^e, n) = (n-1, p^{e-1})((n-1, p+1)-1).$$

Satz 1. *Sei m eine ungerade natürliche Zahl mit der Primfaktorzerlegung* $m = p_1^{e_1} \dots p_r^{e_r}$, $e_i \geqq 1$, *und sei α eine ganze Zahl mit α quadratischer Nichtrest* $\bmod p_i$, $i=1, \dots, r$. *Sei* $v = [p_1^{e_1-1}(p_1+1), \dots, p_r^{e_r-1}(p_r+1)]$, *sei n eine natürliche Zahl mit* $(n, v)=1$ *und sei* $d=(n-1, v)$. *Dann ist* $\operatorname{fix}(m, n)$, *die Anzahl der Fixpunkte der durch $f_n(x)$ dargestellten Permutation von $Z/(m)$, gegeben durch*

$$\operatorname{fix}(m, n) = \prod_{i=1}^{r} (d, p_i^{e_i-1})((d, p_i+1)-1).$$

Beweis. Aus dem Chinesischen Restsatz ergibt sich $\operatorname{fix}(m, n) = \prod_{i=1}^{r} \operatorname{fix}(p_i^{e_i}, n)$. Gemäß Lemma 5 gilt $\operatorname{fix}(p_i^{e_i}, n) = (n-1, p_i^{e_i-1})((n-1, p_i+1)-1)$. Aus $p_i^{e_i-1} | v$ folgt $(n-1, p_i^{e_i-1}) = (n-1, v, p_i^{e_i-1}) = ((n-1, v), p_i^{e_i-1}) = (d, p_i^{e_i-1})$, und aus $(p_i+1) | v$ folgt $(n-1, p_i+1) = (n-1, v, p_i+1) = ((n-1, v), p_i+1) = (d, p_i+1)$. Somit erhält man $\operatorname{fix}(p_i^{e_i}, n) = (d, p_i^{e_i-1})((d, p_i+1)-1)$, und daraus ergibt sich die Behauptung.

4. Die Gruppenstruktur. Es seien m, α, v, n und d wie in Satz 1, und es bezeichne π_n die durch $f_n(x)$ induzierte Permutation von $Z/(m)$.

Lemma 6. *Genau dann induziert $f_n(x)$ die Einheitspermutation ε von $Z/(m)$, wenn gilt* $n \equiv 1 \bmod v$.

Beweis. Genau dann gilt $\pi_n = \varepsilon$, wenn jedes Element von $Z/(m)$ Fixpunkt bezüglich π_n ist, und dies ist gleichbedeutend mit $\operatorname{fix}(m, n) = m$. Nach Satz 1 gilt

$$\operatorname{fix}\Big(\prod_{i=1}^{r} p_i^{e_i}, n\Big) = \prod_{i=1}^{r} p_i^{e_i}$$

genau dann, wenn gilt $(d, p_i^{e_i-1}) = p_i^{e_i-1}$ und $(d, p_i+1) = p_i+1$ für $i=1, \dots, r$, also dann und nur dann, wenn $p_i^{e_i-1} | d$ und $(p_i+1) | d$, $i=1, \dots, r$, und dies ist gleichbedeutend mit $v|d$. Da nach Definition von d stest gilt $d|v$, ist somit $\pi_n = \varepsilon$ äquivalent zu $v=d$, und damit ist die Behauptung bewiesen.

Lemma 7. *Genau dann induzieren $f_k(x)$ und $f_n(x)$ dieselbe Permutation von $Z/(m)$, wenn gilt* $k \equiv n \bmod v$.

Beweis. Sei $\pi_k = \pi_n$. Man wähle $l > 0$, so, daß $ln \equiv 1 \bmod v$. Gemäß Lemma 6 gilt

$$\varepsilon = \pi_{ln} = \pi_l \circ \pi_n = \pi_l \circ \pi_k = \pi_{lk}.$$

Aus $\varepsilon = \pi_{lk}$ folgt — wiederum aus Lemma 6 — $lk \equiv 1 \bmod v$, also $lk \equiv ln \bmod v$, und daraus erhält man $k \equiv n \bmod v$.

Sei nun andererseits $k \equiv n \bmod v$. Wieder wähle man $l > 0$ so, daß $ln \equiv 1 \bmod v$; es gilt dann auch $lk \equiv 1 \bmod v$. Mit Hilfe von Lemma 6 erhält man

$$\pi_k = \pi_k \circ \pi_{ln} = \pi_k \circ \pi_l \circ \pi_n = \pi_{kl} \circ \pi_n = \pi_n.$$

Satz 2. *Die Gruppe P_m aller jener Permutationen von $Z/(m)$, die durch eine Funktion $f_n(x)$ mit gegebenem α und $(n, v)=1$ induziert werden, ist isomorph zu Z_v, der primen Restklassengruppe von $Z/(v)$.*

Beweis. Nach Lemma 7 ist durch $\psi(\pi_n)=n \bmod v$ eine wohldefinierte und bijektive Abbildung von P_m nach Z_v gegeben. Diese ist wegen (2.3) mit $\circ$ verträglich, also sogar ein Isomorphismus.

Es sollen nun alle ungeraden m ermittelt werden, für die P_m zyklisch ist. Entsprechende Resultate für andere durch Permutationsfunktionen dargestellte Permutationsgruppen findet man z.B. in [2], [5] und in [7].

Satz 3. *Die Gruppe P_m ist genau dann zyklisch, wenn einer der beiden folgenden Fälle vorliegt:*

(a) $m=3$,

(b) $m>3$, *m quadratfrei, und es gibt eine ungerade Primzahl q, sodaß sämtliche Primteiler p_i von m darstellbar sind in der Gestalt*

$$p_i = 2q^{k_i}-1, \quad k_i \geqq 1.$$

Beweis. Nach bekannten Sätzen der Zahlentheorie ist Z_w genau dann zyklisch, wenn w gleich einem der folgenden Werte ist:

$$1, 2, 4, q^e, 2q^e \quad (q \text{ ungerade Primzahl, } e \geqq 1). \tag{3.1}$$

Nach Satz 2 ist P_m isomorph zu $Z_{v(m)}$. Wir haben also alle ungeraden natürlichen Zahlen $m \geqq 3$ zu bestimmen, für die $v(m)$ einen der Werte (3.1) annimmt. (Da es keine quadratischen Nichtreste modulo 1 gibt, existiert P_1 nicht.)

Es gilt für alle ungeraden m mit $m \geqq 3$, daß $v(m) \geqq 4$, also nimmt $v(m)$ für kein in Frage kommendes m die Werte 1 oder 2 an. Weiters gilt $v(m)=4$ genau dann, wenn $m=3$.

Sei im folgenden q eine feste ungerade Primzahl, und sei $e \geqq 1$.

Angenommen, es gibt ein ungerades $m \geqq 3$ mit $v(m)=q^e$. Sei p_i ein Primteiler von m, dann gilt $(p_i+1)|v(m)$, also $(p_i+1)|q^e$. Daraus folgt $2|q^e$, und dies ergibt einen Widerspruch. Es gibt also keine ungeraden Zahlen m mit $v(m)=q^e$.

Sei nun $m \geqq 3$ eine ungerade Zahl mit $v(m)=2q^e$. Sei p_i ein Primteiler von m, und sei $v_{p_i}(m)$ die Vielfachheit, mit der p_i in der Faktorzerlegung von m vorkommt. Wäre $v_{p_i}(m)>1$, dann gälte $p_i(p_i+1)|v(m)$, also $p_i(p_i+1)|2q^e$, und dies ergäbe einen Widerspruch zu p_i ungerade. Also gilt $v_{p_i}(m)=1$. Wegen $(p_i+1)|v(m)$ gilt $(p_i+1)|2q^e$, und daraus folgt $p_i+1=2q^s$ mit $1 \leqq s \leqq e$, also $p_i=2q^s-1$. Die Zahl m ist also von der Gestalt (b).

Sei andererseits m von der Gestalt (b), und sei r die Anzahl der Primfaktoren von m. Dann gilt

$$v(m) = [2q^{k_1}, \ldots, 2q^{k_r}] = 2q^{\max\{k_1, \ldots k_r\}},$$

d.h. $v(m)$ ist von der Gestalt $2q^e$, und P_m ist zyklisch. Damit ist Satz 3 vollständig bewiesen.

Als unmittelbare Folgerung erhält man: Mit Ausnahme von 3 gibt es keine natürlichen Zahlen m mit $m \equiv 3 \mod 4$, für die P_m zyklisch ist.

5. Eigenschaften der Fixpunktanzahl. Es sollen nun einige mit der Fixpunktanzahl fix (m, n) in Zusammenhang stehende Fragen erörtert werden. Wie Satz 1 zeigt, ist fix (m, n) bei gegebenem m durch d eindeutig bestimmt. Bezeichnet man für einen festen Teiler d von v die Anzahl der Permutationen $\pi_n \in P_m$, für die gilt $(n-1, v)=d$, mit $\sigma(d, v)$, dann gilt

Satz 4. *Sind* $v=\prod_{j=1}^{s} q_j^{g_j}$, $g_j \geqq 1$, *und* $d=\prod_{j=1}^{s} q_j^{h_j}$, $0 \leqq h_j \leqq g_j$, *die Primfaktorzerlegungen der Zahlen* v *und* d, *so gilt*

$$\sigma(d, v) = (v/d) \prod_{j=1}^{s} (1-\varepsilon_j/q_j) \quad \text{mit} \quad \varepsilon_j = \begin{cases} 2 & \text{für} \quad h_j = 0, \\ 1 & \text{für} \quad 0 < h_j < g_j, \\ 0 & \text{für} \quad h_j = g_j. \end{cases}$$

Beweis. (Vgl. [4], wo ein analoges Resultat für die Gruppe der durch die Potenzen x^n induzierten Permutationen von $Z/(m)$ hergeleitet wird.) Klarerweise ist $\sigma(d, v)$ die Anzahl der Restklassen a mod v mit $(a, v)=d$ und $(a+1, v)=1$. Nach dem Chinesischen Restsatz kann man die Restklassen a mod v bijektiv zuordnen den s-Tupeln $(a_1, \ldots, a_s)$, in denen a_j jeweils alle Restklassen modulo $q_j^{g_j}$ durchläuft. Mit Hilfe der Gleichungen $a=a_j+k_j q_j^{g_j}$, $j=1, \ldots, s$, erkennt man

$$(a, v) = \prod_{j=1}^{s} (a, q_j^{g_j}) = \prod_{j=1}^{s} (a_j+k_j q_j^{g_j}, q_j^{g_j}) = \prod_{j=1}^{s} (a_j, q_j^{g_j}).$$

Da der Restklasse $a+1$ das s-Tupel $(a_1+1, \ldots, a_s+1)$ entspricht, ist $(a+1, v)=1$ gleichbedeutend mit $(a_j+1, q_j^{g_j})=1$ für alle j und dies wiederum ist gleichbedeutend mit $a_j \not\equiv -1 \mod q_j$, $j=1, \ldots, s$. Ferner ist $(a_j, q_j^{g_j})=q_j^{h_j}$ gleichbedeutend damit, daß $a_j=bq_j^{h_j}$ mit $(b, q_j)=1$. Die Anzahl der verschiedenen Restklassen a_j mod $q_j^{g_j}$, die diese und die vorhergehende Bedingung erfüllen, ist also gegeben durch

$$q_j^{g_j-h_j-1}(q_j-\varepsilon_j) = q_j^{g_j-h_j}(1-\varepsilon_j/q_j),$$

woraus die Behauptung folgt.

Lemma 8. *Sei* d *ein Teiler von* v. *Es gilt* $\sigma(d, v)=0$ *genau dann, wenn* d *ungerade ist.*

Beweis. Da m ungerade ist, hat m einen ungeraden Primteiler p_i, und es folgt $(p_i+1)|v$, also $2|v$. Sei o.B.d.A. $q_1=2$. Aufgrund von Satz 4 gilt $\sigma(d, v)=0$ genau dann, wenn für ein $j \in \{1, \ldots, s\}$ gilt $1-\varepsilon_j/q_j=0$, d.h. wenn für ein j gilt $\varepsilon_j=q_j$.

Wegen $\varepsilon_j \leqq 2 \leqq q_j$ gilt dies höchstens für $q_j=2$, also für $j=1$. Es gilt $\varepsilon_1=q_1$, also $\varepsilon_1=2$ genau dann, wenn $h_1=0$, also wenn d ungerade ist. Damit ist das Lemma bewiesen.

Für kryptographische Anwendungen sind speziell die beiden folgenden Problemstellungen von Interesse: (i) Welches ist die kleinste Zahl $w_{\min}$, die als Fixpunktanzahl einer Permutation $\pi_n \in P_m$ auftreten kann? (ii) Wieviele Permutationen $\pi_n \in P_m$ gibt es, die genau $w_{\min}$ Fixpunkte aufweisen?

Aufgrund von Satz 1 und Lemma 8 treten als Fixpunktanzahlen von Permutationen $\pi_n \in P_m$ genau die Zahlen

$$\tau(d, m) = \prod_{i=1}^{r} (d, p_i^{e_i-1})\big((d, p_i+1)-1\big), \quad d \text{ gerader Teiler von } v$$

auf. Setzt man $d=2$, so erhält man $\tau(2, m)=1$. Es gibt also Permutationen $\pi_n \in P_m$ mit nur einem Fixpunkt. Um die Anzahl aller $\pi_n \in P_m$ mit nur einem Fixpunkt bestimmen zu können, benötigt man

Satz 5. *Die Funktion $\tau(d, m)$ ist streng monoton auf dem Verband der geraden Teiler von v.*

Beweis. Es ist zu zeigen, daß $\tau(c, m) < \tau(d, m)$, wenn c ein echter Teiler von d ist. Da dann $(c, p_i^{e_i-1}) \mid (d, p_i^{e_i-1})$ und $(c, p_i+1) \mid (d, p_i+1)$ für alle i, also $(c, p_i^{e_i-1}) \leqq (d, p_i^{e_i-1})$ und $(c, p_i+1) \leqq (d, p_i+1)$, folgt jedenfalls $\tau(c, v) \leqq \tau(d, v)$. Sei q_j eine Primzahl, die in c mit der Vielfachheit $v_{q_j}(c)$ und in d mit der Vielfachheit $v_{q_j}(d) > v_{q_j}(c)$ vorkommt. Wegen $d \mid v$ gilt $v_{q_j}(d) \leqq v_{q_j}(v) = \max_{1 \leqq i \leqq r} \{v_{q_j}(p_i^{e_i-1}(p_i+1))\}$. Also gibt es ein i mit $q_j^{v_{q_j}(d)} \mid p_i^{e_i-1}(p_i+1)$. Ist $q_j = p_i$, dann gilt $(c, p_i^{e_i-1}) < (d, p_i^{e_i-1})$. Ist aber $q_j \neq p_i$, dann gilt $(c, p_i+1) < (d, p_i+1)$. Daher gilt jedenfalls $(c, p_i^{e_i-1})\big((c, p_i+1)-1\big) < (d, p_i^{e_i-1})\big((d, p_i+1)-1\big)$, und daraus folgt $\tau(c, m) < \tau(d, m)$.

Folgerung 1. *Die Anzahl der Permutationen $\pi_n \in P_m$ mit nur einem Fixpunkt beträgt*

$$(v/2\delta) \prod_{j=2}^{s} (1-2/q_j) \quad \textit{mit} \quad \delta = \begin{cases} 1 & \text{für} \quad v \not\equiv 0 \bmod 4 \\ 2 & \text{für} \quad v \equiv 0 \bmod 4. \end{cases}$$

Beweis. Sei d ein gerader, von 2 verschiedener Teiler von v. Dann ist 2 echter Teiler von d, und aus Satz 5 folgt $1 = \tau(2, m) < \tau(d, m)$. Somit ist die Anzahl der Permutationen π_n von $Z/(m)$ mit nur einem Fixpunkt gleich $\sigma(2, v)$. Aufgrund von Satz 4 folgt daraus unmittelbar die Behauptung.

6. Kryptographische Anwendung. Es soll nun die Beschreibung eines Public-Key Kryptosystems auf der Basis der Rédei-Funktionen erfolgen.

Jeder potentielle Kommunikationsteilnehmer C wählt eine Faktorenanzahl r und r große Primfaktoren $p_1, \dots, p_r$ mit zugehörigen Vielfachheiten $e_1, \dots, e_r$, bildet das Produkt $m = \prod_{i=1}^{r} p_i^{e_i}$ und berechnet die gemäß Satz 1 definierte Größe v. Weiters wählt C eine ganze Zahl α mit α Nichtrest mod p_i, $i=1, \dots, r$ — etwa durch sukzessives Testen zufällig gewählter Testzahlen a mit Hilfe des Eulerschen Kriteriums. Schließlich wählt C einen Chiffrierschlüssel $n>0$ mit

(6.1) $$(n, v) = 1$$

und

(6.2) $$(n-1, v) = 2$$

und berechnet zu diesem n durch Lösen der linearen Kongruenz

(6.3) $$nk \equiv 1 \bmod v$$

einen zugehörigen Dechiffrierschlüssel $k>0$. Im öffentlich zugänglichen Schlüsselverzeichnis veröffentlicht C die Größen $m_C=m$, $\alpha_C=\alpha$ und $n_C=n$, hält jedoch die Faktorzerlegung von m sowie $k_C=k$ und $v_C=v$ geheim.

Angenommen, A möchte an B die Nachricht φ übersenden. A sucht aus dem öffentlich zugänglichen Schlüsselverzeichnis die Schlüsselparameter von B, also m_B, α_B und n_B, stellt die Nachricht φ als Folge von Blöcken x_i, $x_i \in Z/(m_B)$, dar, chiffriert die x_i mittels

(6.4) $$x_i \to y_i = f_{n_B}(x_i) \bmod m_B$$

und übersendet die y_i an B. Der Empfänger berechnet mit Hilfe des nur ihm bekannten Dechiffrierexponenten k_B aus den y_i die Nachrichtenblöcke x_i:

$$f_{k_B}(y_i) = f_{k_B} \circ f_{n_B}(x_i) = f_{k_B n_B}(x_i) = f_{1+tv_B}(x_i) \equiv x_i \bmod m_B.$$

Dabei steht t für eine geeignete natürliche Zahl, und die letzte Gleichung gilt aufgrund von Lemma 6.

Da zur Berechnung von v_B die Faktorzerlegung von m_B benötigt wird, jedoch bis heute keine schnellen Algorithmen zur Faktorisierung großer Zahlen bekannt sind, ist es nicht möglich, aufgrund der öffentlich bekannten Informationen m_B, α_B und n_B das zur Berechnung des Dechiffrierschlüssels k_B benötigte v_B zu ermitteln. Forderung (6.2) garantiert, daß die durch $f_n(x)$ induzierte Chiffrierfunktion nur *einen* Fixpunkt aufweist.

Literatur

[1] W. DIFFIE und M. HELLMAN, New directions in cryptography, *IEEE Trans. Information Theory*, IT—22 (1976), 644—654.

[2] H. HULE und W. B. MÜLLER, Grupos cíclicos de permutaciones inducidas por polinomios sobre campos de Galois, *An. Acad. Brasil. Cienc.*, 45 (1973), 63—67.

[3] R. LIDL und W. B. MÜLLER, Permutation polynomials in RSA-cryptosystems, in: *Proceedings Crypto 83*, University California, Santa Barbara, 1983.

[4] W. B. MÜLLER und W. NÖBAUER, Über die Fixpunkte der Potenzpermutationen, *Österr. Akad. Wiss. Math. Naturwiss. Kl. Sitzungsber.*, II (1983), 93—97.

[5] W. NÖBAUER, Über eine Gruppe der Zahlentheorie, *Monatsh. Math.*, 58 (1954), 181—192.

[6] W. NÖBAUER, Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen, *Monatsh. Math.*, 69 (1965), 230—238.

[7] W. NÖBAUER, Über Gruppen von Dickson-Polynomfunktionen und einige damit zusammenhängende zahlentheoretische Fragen, *Monatsh. Math.*, 77 (1973), 330—344.

[8] L. RÉDEI, Über eindeutig umkehrbare Polynome in endlichen Körpern, *Acta Sci. Math.*, 11 (1946), 85—92.

[9] R. RIVEST, A. SHAMIR und L. ADLEMAN, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, 21 (1978), 120—126.

UBW KLAGENFURT
UNIVERSITÄTSSTRASSE 67
9010 KLAGENFURT, AUSTRIA

Acta Sci. Math., 50 (1986), 299—330

Some sufficient conditions for hereditarily finitely based varieties of semigroups

G. POLLÁK

Introduction

The proofs of most theorems saying that one or another variety is hereditarily finitely based are very similar to each other (in so far as syntactic proofs are concerned). The general scheme of such proofs has been described in [6] (see also Theorem 2.5 of the present paper); however, this description does not help much more in future proofs as finger-posts do in alpinism. The essential difficulty usually lies in proving that the objects and relations in the scheme are what they ought to be (sometimes it is not even easy to construct them). We think therefore that every unification which renders possible to claim that a more or less broad class of varieties is h.f.b. is of interest.

In the present paper we give sufficient conditions of the following two types: a) if J is a fully invariant ideal of the countably generated free semigroup F, and a certain quasi-ordered set (connected with $F\setminus J$) is well-quasi-ordered then the variety $SG(J)$ defined by all identities $u=v$, $u, v\in J$ is h.f.b.; b) if V is a variety, $M\subset F$ is a standard form for elements of J (i.e. every $w\in J$ equals to some $w^*\in M$), and M itself, as well as the "process of standardization" are subject to certain conditions, then every variety in the lattice interval $[V, V\cap SG(J)]$ is finitely based over V. Furthermore, we show that certain concrete subsets of F satisfy these conditions. As an application, we find all h.f.b. identities in one of the four classes of "candidates" to such identities (see [3]; class (d)). This result accomplishes, in a certain sense, the investigations concerning such identities; namely, classes (c) and (d), as well as balanced h.f.b. equations are completely described now (see [1], [4], [6]), homotypical and some other equations of class (b) are settled in [5], and it looks likely that presently known *syntactic* methods cannot help us much further.

Received October 3, 1983.

Part I. General sufficient conditions

1. Preliminary. We need rather a lot of not generally known concepts and of notations running through this paper; so we have collected most of them here.

By the free semigroup F we always mean the countably generated free semigroup $F(X)$ on the set of generators $X=\{x_1, x_2, \dots\}$. As we need also the free monoid F^0, we shall call the elements of F *terms*, the elements of F^0 *words* (i.e. a word can be empty, a term cannot). The coincidence of words will be denoted by $u\equiv v$; the formula $u=v$ is an identity which holds in some subvariety V of the variety of all semigroups SG. The empty word, as well as the empty set, we denote by $\emptyset$; this will not lead to confusion.

The set of all variables (letters) which occur in u will be denoted by $X(u)$. Furthermore, $|u|$ denotes the length of u, and $|u|_i$ the number of occurrences of x_i in u. The words $u_{(l)}$, $u^{(l)}$ are the prefix and the suffix of length l of the word u (of length $\geqq l$), resp.:

$$u \equiv u_{(l)}u' \equiv u''u^{(l)}, \quad |u| \geqq l, \quad |u_{(l)}| = |u^{(l)}| = l. \tag{1.1}$$

A third kind of denoting equality is defined by

$$u =! \, u_1u_2 \overset{\text{def}}{\Leftrightarrow} u \equiv u_1u_2 \quad \text{and} \quad X(u_1)\cap X(u_2) = \emptyset. \tag{1.2}$$

Note that $u=!\,u_1u_2$ implies $|X(u)|=|X(u_1)|+|X(u_2)|$. If a word has no decomposition of the form (1.2), it is said to be *irreducible*. Every word has a unique irreducible decomposition:

$$u =!! \prod_{i=1}^{r} u_i \overset{\text{def}}{\Leftrightarrow} u =! \prod_{i=1}^{r} u_i, \quad u_i \text{ irreducible for } i = 1, \dots, r. \tag{1.3}$$

We call the components u_i the *irreducible factors* of u. The word u is said to be *semiirreducible* if $|u_i|>1$ for every i (in particular, $\emptyset$ is semiirreducible). The decomposition

$$u =! \, w_0 \prod_{j=1}^{s} x_{c(i)}w_i, \quad w_i \text{ semiirreducible} \tag{1.4}$$

will be called the *semiirreducible factorization* of u, and $w_0, \dots, w_s$ its *semiirreducible factors*. A word is said to be *simple* if its semiirreducible factors are empty (i.e. if no letter occurs in it more than once). Besides (1.4), we shall also make use of the *reduced semiirreducible factorization*

(1.5)

$$u =! \, w_0 \prod_{i=1}^{s} a_i\tilde{w}_i, \quad \tilde{w}_i \text{ semiirreducible, } a_i \text{ simple, } \tilde{w}_i,\ a_i \not\equiv \emptyset \text{ for } i = 1, \dots, s-1.$$

Clearly, both (1.4) and (1.5) are unique.

By $F_{(n)}$ we denote the set of all words having only semiirreducible factors of length $\leqq n$. In particular, $F_{(0)}=F_{(1)}$ consists of all simple words. Obviously, $F_{(n)}\subset F_{(n+1)}$ for every $n\geqq 1$, and $F^0\setminus F_{(n)}=J_{(n)}$ is a fully invariant ideal in F. Let $M\subset F^0$. Set

$$(1.6)\qquad M^{[m]}=\{u:\ u\equiv a_0\prod_{i=1}^{t}u_ia_i,\ |a_0\ldots a_t|\leqq m,\ \bar{u}=!\ \bar{u}_1\ldots\bar{u}_t\in M\},$$

$$(1.7)\qquad M^{(m)}=\{u:\ u\in M^{[m]},\ X(a_0\ldots a_t)\cap X(\bar{u})=\emptyset\}.$$

It is easy to see that

Lemma 1.1. *$F_{(n)}^{[m]}\subseteqq F_{(n)}^{(m(n+1))}$ if $n\geqq 1$.*

Indeed, if $u\in F_{(n)}^{[m]}$, then at most m factors of the factorization (1.4) of u can contain some element of $X(a_0\ldots a_t)$ (as $|X(a_0\ldots a_t)|\leqq m$), and every such factor is of length $\leqq n$. Put

$$u\equiv a_0'\prod_{i=1}^{t'}u_i'a_i'$$

where every a_i' is equal to a factor of (1.4) which contains a letter of $a_0\ldots a_t$. Clearly,

$$|a_0'\ldots a_{t'}'|\leqq(n+1)m,\quad\text{and}\quad X(a_0'\ldots a_{t'}')\cap X(u_1'\ldots u_{t'}')=\emptyset.$$

Two words u, u' are said to be of the same type if there is an automorphism $\alpha\in\operatorname{Aut}F^0$ which maps u into u': $u\alpha=u'$. The set of all words of the same type (an orbit of $\operatorname{Aut}F^0$) is called a *type*. E.g. X and $0=\{\emptyset\}$ are types. The type of u will be denoted by $T(u)$. If u is irreducible, simple etc., the same is said about $T(u)$.

An endomorphism $\varphi\in\operatorname{End}F^0$ is said to be *disjoint* if $X(x_i\varphi)\cap X(x_j\varphi)=\emptyset$ provided $i\neq j$. The endomorphism φ is *finite* if $|x_i\varphi|>1$ for at most finitely many x_i's. The number

$$\gamma(\varphi)=\sum_{i=1}(|x_i\varphi|-1)$$

is called the *growth* of φ. The set of all disjoint endomorphisms will be denoted by Dend F^0, that of all finite disjoint endomorphisms by Fde F^0.

The proof of the following facts is straightforward (see also [4]).

Lemma 1.2. *If $u\notin X$ is (semi)irreducible and $\varphi\in$ Dend F^0, then $u\varphi$ is (semi)-irreducible.*

Lemma 1.3. *If $u=!\prod_{i=1}^{m}w_i$ and $\varphi\in$ Dend F^0 then $u\varphi=!\prod_{i=1}^{m}w_i\varphi$.*

Let $r(u)$ $(=r)$, $s(u)(=s)$ be the number of factors in (1.3) and (1.4), respectively.

Lemma 1.4. *If $\varphi\in$ Fde F^0 then $r(u)\leqq r(u\varphi)\leqq r(u)+\gamma(\varphi)$, $s(u)\leqq s(u\varphi)\leqq s(u)+\gamma(\varphi)$, and the image of an irreducible factor $u_i\notin X$ of u is an irreducible factor of $u\varphi$.*

We have to deal with several order and quasi-order relations. The most important order relation will be the lexicographical order of words defined by

$$u <_{\text{lex}} v \overset{\text{def}}{\Leftrightarrow} v \equiv uv', \quad v' \in F \quad \text{or} \quad u \equiv wx_i u', \quad v \equiv wx_j v', \quad i<j.$$

The lexicographical order is not a well-order on F^0, however, it is a well-order on $F^0 \setminus F^n$ (the set of words of length $<n$).

Let V be a variety of semigroups, and $F(V)$ the free semigroup in V on the infinite set of generators $\{x_1 v, x_2 v, \ldots\}$, where $v\colon F \to F(V)$ is the canonical homomorphism. A fully invariant ideal J is said to be a *V-ideal* if J is the full inverse image of Jv. In particular,

$$J(V) = \{u \in F\colon \text{there is a } v \in F \text{ such that } v \not\equiv u,\ V \models u=v\}$$

is a V-ideal.

Let σ be a set of identities. By $V(\sigma)$ we denote the subvariety of V consisting of those algebras which satisfy σ. If J is a fully invariant ideal then

$$V(J) = V(\tau) \quad \text{where} \quad \tau = \{u = v\colon\ u, v \in J\}$$

(i.e. $V(J)$ is generated by the algebra $F(V)/J$).

Following Petrich, we term an identity $u=v$ *homotypical* if $X(u)=X(v)$ and *heterotypical* else. The ideal

$$J_0(V) = \{u \in F\colon \text{ there is a } v \in F \text{ such that } X(u) \neq X(v),\ V \models u=v\}$$

is a V-ideal, too. Obviously, $J_0(V) \subseteq J(V)$, and $J_0(V)v$ is the kernel of $F(V)$.

Two systems of identities σ_1, σ_2 are said to be *V-equivalent* if

$$V \models \sigma_1 \Leftrightarrow \sigma_2.$$

Similarly, a system σ is *V-finite, V-independent* etc., if it is V-equivalent to a finite system, not V-equivalent to any proper subsystem of itself etc. Furthermore, $V'(\subseteq V)$ is said to be *finitely based over* V if $V' = V(\sigma)$, σ finite (or, equivalently, V-finite). The interval $[V', V)$ of the lattice of varieties is finitely based if every element of $[V', V)$ is finitely based over V. If V is finitely based, too, then we say that $[V', V]$ is finitely based.

We say that the system of identities σ (or, also, the identity $u=v$ in the case $\sigma = \{u=v\}$) is hereditarily finitely based (h.f.b. for short) if the variety $SG(\sigma)$ is, where SG is the variety of all semigroups (which, by definition, means that every subvariety of $SG(\sigma)$ is finitely based).

Let J be a fully invariant ideal in F. A subset $M \subseteq F$ is termed a *standard form for* V *in* J (or, for short, M *is standard for* V *in* J) if for every $u \in J$ there is a $u^* \in M$ such that $V \models u = u^*$ (neither uniqueness nor the existence of an algorithm for finding u^* is demanded). Clearly, if M is a standard form, then so is every $M' \supseteq M$. Moreover, if J is a V-ideal, $u \in J$ and $u = u^*$ imply $u^* \in J$. Thus, $J \cap M$ is also a standard form for V in J. However, sometimes it is more convenient to work with larger standard forms. If $J=F$ we simply say that M is a standard form for V. Usually we state our theorems for standard forms in an arbitrary J because the more elegant special case of standard forms for V does not suffice in the applications.

Finally, if $\sigma=\{u_s=v_s\}$ then by $\bar\sigma$ we denote the system $\sigma\cup\{v_s=u_s\}$.

2. Well-quasi-orders and h.f.b. varieties. A quasi-order relation $\prec$ is said to be a *well-quasi-order* (*wqo* for short) if there are neither infinite (strictly) descending $\prec$-chains nor infinite $\prec$-antichains or, equivalently, if every infinite sequence contains an infinite (not necessarily strictly) ascending subsequence ([2]). The following quasi-orderings on subsets $M\subseteq F^0$ will occur:

$$u \lhd u' \quad \text{iff} \quad u' \equiv u_1\cdot u\varphi\cdot u_2 \quad \text{for some} \quad \varphi\in\operatorname{End}F^0, \quad u_1, u_2\in F^0,$$

$$u \lhd_V u' \quad \text{iff} \quad V\models u' = u_1\cdot u\varphi\cdot u_2 \quad \text{for some} \quad \varphi\in\operatorname{End}F^0, \quad u_1, u_2\in F^0,$$

$$u \lhd_h u' \quad \text{iff} \quad u' \equiv u\varphi \quad \text{for some} \quad \varphi\in\operatorname{End}F^0,$$

$$u \ll u' \quad \text{iff} \quad u' \equiv u\varphi \quad \text{for some} \quad \varphi\in\operatorname{Fde}F^0.$$

Note that in the last case it is sufficient to find a $\varphi'\in\operatorname{Dend}F^0$ such that $u'\equiv u\varphi'$: this can be always modified so as to obtain a $\varphi\in\operatorname{Fde}F^0$.

Let, furthermore, $\mathbf{P}$ denote the set of positive integers and Σ the symmetric group on $\mathbf{P}$. For every $k\in\mathbf{P}$ we define two quasi-orders, one on $M\times\Sigma$ and one on $M^2\times\Sigma$ as follows:

$$(u,\pi) \ll_k (u',\pi') \quad \text{iff} \quad \exists\varphi\in\operatorname{Fde}F^0(u\varphi\equiv u',\ x_{i\pi}\varphi\equiv x_{i\pi'} \text{ for } 1\leqq i\leqq k),$$

$$(u,v;\pi) \ll_k^2 (u',v';\pi') \quad \text{iff} \quad \exists\varphi\in\operatorname{Fde}F^0 \quad (u\varphi\equiv u',\ x_{i\pi}\varphi\equiv x_{i\pi'}$$
$$\text{for } 1\leqq i\leqq k,\ v\varphi\in M).$$

The remark made above about φ is valid here, too. Also, it is worth noting that in the definition of $\ll_k^2$ the word v' does not play any role, and that $\ll$ is a wqo if $\ll_k$ is.

In proving varieties to be h.f.b., often it is crucial to know that one or the other of these quasi-orders is a wqo for some standard form M. As for the second one, this is even indispensable:

Lemma 2.1. *If V is h.f.b., then $\lhd_V$ is a wqo on F^0.*

Proof. Obviously, no infinite descending $\lhd_V$-chain can exist. If $u_1, u_2, \ldots$ were an infinite $\lhd_V$-antichain, then consider the system $\sigma=\{u_{2k-1}=u_{2k}\colon k=1,2,\ldots\}$. We are going to show that $V(\sigma)$ is not finitely based, moreover, if $\sigma_k=\sigma\setminus\{u_{2k-1}=u_{2k}\}$ then $V(\sigma_k)\not\models u_{2k-1}=u_{2k}$. Indeed, suppose there exist $(u_{2k-1}\equiv)v_1, \ldots, v_l(\equiv u_{2k})$ such that $v_i\equiv v_i'\cdot w_i\varphi_i\cdot v_i''$, $v_{i+1}\equiv v_i'\cdot w_i'\varphi_i\cdot v_i''$ for $i=1,\ldots,l-1$, where $\varphi_i\in\operatorname{End}F$, $v_i', v_i''\in F^0$ and either $V\models w_i=w_i'$ or $w_i=w_i'\in\bar\sigma_k$. If it is always the first instance that prevails then $V\models u_{2k-1}=u_{2k}$, which is not the case. Let i be the minimal index such that $V \not\models v_i = v_{i+1}$, and, say, $w_i \equiv u_{2r-1}$, $w_i' \equiv u_{2r}$, $r \neq k$. Then $V \models u_{2k-1} = v_i \equiv \equiv v' \cdot u_{2r-1}\varphi_i \cdot v_i''$, contrary to the assumption.

Clearly, if $\ll_k$ is a wqo (for some fixed M) then $\ll_l$ for $0 \leqq l < k$ is a wqo, too. However, already the condition that $\ll_1$ is a wqo on some $M \times \Sigma$ is rather restrictive as the following lemma shows.

Lemma 2.2. *If $\ll_1$ is a wqo on $M \times \Sigma$ then there is a natural number p such that $|u|_i \leqq p$ for every $u \in M$ and $i \in \mathbf{P}$.*

Proof. Put $p(u) = \max |u|_i$, and suppose $p(u_1) < p(u_2) < \ldots$, $|u_j|_{k(j)} = p(u_j)$. Then we obtain an infinite $\ll_1$-antichain (u_j, π_j), $j = 1, 2, \ldots$ by putting $\pi_j = =(1\ k(j))$: if φ is disjoint and $x_{k(j)}\varphi \equiv x_{k(i)}$, $j \neq i$, then $|u_j\varphi|_{k(i)} = p(j) \neq p(i)$ whence $u_j\varphi \not\equiv u_i$.

Let $G_{n,k} = \{(a_1, \ldots, a_r) \in (F^0)^r \colon |a_1 \ldots a_r| \leqq n,\ |X(a_1 \ldots a_r)| \leqq k\}$. The following proposition enables a more flexible handling of $\ll_k$.

Proposition 2.3. *$\langle M \times \Sigma, \ll_k \rangle$ is wqo iff $M \times G_{n,k}$ is wqo for every n under*

$$(u;\ a_1, \ldots, a_r) \prec (u';\ a_1', \ldots, a_{r'}') \quad \textit{iff} \quad r = r' \quad \textit{and} \tag{2.1}$$
$$\exists \varphi \in \mathrm{Fde}\, F^0 (u\varphi \equiv u',\ a_i\varphi \equiv a_i' \textit{ for } i = 1, \ldots, r).$$

Proof. The sufficiency is obvious because $(u, \pi) \ll_k (u', \pi')$ is equivalent to $(u; x_{1\pi}, \ldots, x_{k\pi}) \prec (u'; x_{1\pi'}, \ldots, x_{k\pi'})$. Now let $\ll_k$ be a wqo, and let $x_{s(1)}, \ldots, x_{s(q)}$ be the variables of $a_1 \ldots a_r$ (in the order of their first occurrence). Set

$$\pi = \begin{pmatrix} 1 & \ldots & q \\ s(1) & \ldots & s(q) \end{pmatrix},$$

and put $(u; a_1, \ldots, a_r) \prec_0 (u'; a_1', \ldots, a_{r'}')$ iff $r = r'$, $T(a_1 \ldots a_r) = T(a_1' \ldots a_{r'}')$, $T(a_i) = =T(a_i')$ for $i = 1, \ldots, r$, $(u, \pi) \ll_q (u', \pi')$. Now $\prec_0$ is a wqo because $q \leqq k$ and r, $T(a_1 \ldots a_r)$, $T(a_i)$ can take only a finite number of different "values". Furthermore, $(u; a_1, \ldots, a_r) \prec_0 (u'; a_1', \ldots, a_{r'}')$ implies $(u; a_1, \ldots, a_r) \prec (u'; a_1', \ldots, ar')$ because the very endomorphism φ which satisfies $u\varphi \equiv u'$, $x_{s(j)}\varphi \equiv x_{s'(j)}$ maps a_i on a_i'. Hence $\prec$ is a wqo.

The following proposition shows that the conditions that $\ll_k$ is a wqo for different numbers k are not very far from each other.

Proposition 2.4. *If $M \subset F^0$, and there is a natural number q such that $uv \in M$ implies $|X(u) \cap X(v)| \leqq q$, furthermore, $\ll_{2q+1}$ is a wqo on M, then $\ll_k$ is a wqo on M for every k.*

Proof. For $k \leqq 2q+1$ (in particular, for $k=1$) the assertion is obvious. So suppose it holds for some k. For $(u, \pi) \in M \times \Sigma$ consider the decomposition

$$u \equiv u_0 \prod_{i=1}^{r} x_{t_i\pi} u_i,\ t_i \leqq k,\ X(u_i) \cap \{x_{1\pi}, \ldots, x_{k\pi}\} = \emptyset,$$

and put

$$\hat{u} \equiv \prod_{i=1}^{r} x_{t_i\pi}, \quad \bar{u} \equiv u_0 \dots u_r, \quad \bar{u}_i \equiv u_0 \dots u_{i-1}, \quad \bar{\bar{u}}_i \equiv u_i \dots u_r,$$

$$X_i(u) = (X(\bar{u}_i) \cap X(\bar{\bar{u}}_i)) \setminus \{x_{(k+1)\pi}\}, \quad \bar{X}(u) = \bigcup_{i=1}^{r} X_i(u), \quad \bar{X}(u_i) = \bar{X}(u) \cap X(u_i).$$

It is easy to see that $r \leqq kp$ where p is the bound from Lemma 2.2, $|\bar{X}(u)| \leqq rq$, and $\bar{X}(u_i) \subseteq X_i(u) \cup X_{i+1}(u)$, whence $q_i = |\bar{X}(u_i)| \leqq 2q$. Choose permutations $\pi_0, \dots, \pi_r$ such that $1\pi_i = (k+1)\pi$, $x_{2\pi_i}, \dots, x_{(q_i+1)\pi_i}$ are the different elements of $\bar{X}(u_i)$ (e.g. in the order of their first occurrence in u_i), and define

$$(u, \pi) \prec (u', \pi') \quad \text{iff} \quad (u, \pi) \ll_k (u', \pi'),$$

(2.2)

$$(u_i, \pi_i) \ll_{2q+1} (u_i', \pi_i') \quad \text{for} \quad i = 1, \dots, r, \quad \text{and} \quad T\Big(\prod_{i=0}^{r} \prod_{t=1}^{q_i+1} x_{t\pi_i}\Big) = T\Big(\prod_{i=0}^{r} \prod_{t=1}^{q_i'+1} x_{t\pi_i'}\Big).$$

As $(u, \pi) \ll_k (u', \pi')$ implies $T(\hat{u}) = T(\hat{u}')$, r is the same for (u, π) and for (u', π'), and the definition makes sense. Furthermore, (2.2) implies that $q_i = q_i'$ for $0 \leqq i \leqq r$, because $1\pi_i = (k+1)\pi$, $1\pi_i' = (k+1)\pi'$ for every i; in particular, $x_{(k+1)\pi}$ and $x_{(k+1)\pi'}$ are the first letters of the corresponding products, and this fixes the length of the inner products.

From the assumptions it follows that $\prec$ is a wqo on $M \times \Sigma$, so it is sufficient to show that $\prec$ is weaker than $\ll_{k+1}$, i.e. if (2.2) holds then there is a $\varphi \in$ Fde F^0 such that $u\varphi \equiv u'$, $x_{t\pi}\varphi \equiv x_{t\pi'}$ for $t \leqq k+1$. By (2.2), there are disjoint endomorphisms ψ, $\varphi_0, \dots, \varphi_r$ such that

$$u\psi \equiv u', \quad x_{t\pi}\psi \equiv x_{t\pi'} \quad \text{for} \quad 1 \leqq t \leqq k,$$

$$u_i\varphi_i \equiv u_i', \quad x_{t\pi_i}\varphi_i \equiv x_{t\pi_i'} \quad \text{for} \quad 1 \leqq t \leqq q_i + 1, \quad i = 1, \dots, r.$$

Put

$$x_s\varphi \equiv \begin{cases} x_s\varphi_i & \text{if} \quad x_s \in X(u_i), \\ x_s\psi & \text{if} \quad x_s \notin X(\bar{u}). \end{cases}$$

Then φ is well-defined: if $x_s \in X(u_i) \cap X(u_j)$, $i<j$, then $s = i\pi_i = t'\pi_j$ for some $t \leqq q_i + 1$, $t' \leqq q_j + 1$, however, then, the third condition in (2.2) guarantees that $t\pi_i' = t'\pi_j'$, i.e. $x_s\varphi_i \equiv x_s\varphi_j$. Also, it is not difficult to see that φ is disjoint. Furthermore, $\hat{u}\psi \equiv \hat{u}'$ whence $\hat{u}' \equiv \Pi x_{t_i\pi'}$ (in general, the sequence $t_1, \dots, t_r$ depends on (u, π)). Thus, $u\varphi \equiv u'$, $x_{t\pi}\varphi \equiv x_{t\pi'}$ for $t = 1, \dots, k+1$.

In [6], the generally used syntactic method of proving varieties to be h.f.b. is formulated in Proposition 2.1. Here we give a slightly different version. Let $M \subset F^0$, V a variety, and J a fully invariant ideal of F. We say that M is a *good standard form for V in J* (or a *good standard form for V* if $J = F$) if there exist a linear order relation

$<$ on M and a quasi-order relation $\prec$ on $M^*=\{(u,v)\colon u>v\}\subset M^2$ such that the following conditions are fulfilled:

C) For every $u\in J$ there is a $u^*\in M$ such that $V\models u=u^*$;

O) $(M,<)$ is a well-ordered set;

Q) $(M^*,\prec)$ is a wqo set;

A) If $(u,v),(u',v')\in M^*$, $(u,v)\prec(u',v')$ then there is a $w\in M$ such that $w<u'$ and $V\models(u=v\Rightarrow u'=w)$.

If one replaces F^r by J in the first part of the proof of Proposition 2.1 in [6], one obtains

Proposition 2.5. *If there is a good standard form for V in J then the interval $[V(J),V)$ is finitely based.*

It is easy to see that if M is a good standard form for V in J then it is a good standard form in the minimal V-ideal J_V which contains J. Thus, $J_V\cap M$ is a standard form for V in J (even in J_V).

In order to obtain a sufficient condition for V to be h.f.b., we need the following

Proposition 2.6. *Let V be a variety and J a V-ideal. If the interval $[V(J),V)$ is finitely based and $V(J)$ is h.f. b. over V then every subvariety of V is finitely based over V.*

The proof is based on

Lemma 2.7. *Let V be a variety, J a fully invariant ideal in F, and $V'=V(J)$. Let, furthermore, σ be a system of identities and $u\in F$ such that $V(\sigma)\not\models u=v$ for any $v\in J$. Then $V'(\sigma)\models u=u'$ implies ($u'\notin J$ and) $V(\sigma)\models u=u'$.*

Proof. Let $(u\equiv)\ v_1,v_2,\dots,v_l\ (\equiv u')$ be a sequence of terms such that $v_j\equiv\equiv v_j'\cdot w_j\varphi_j\cdot v_j''$, $v_{j+1}\equiv v_j'\cdot w_j'\varphi_j\cdot w_j''$ for $j=1,\dots,l-1$, where $v_j',v_j''\in F^0$, $\varphi_j\in\mathrm{End}\,F$, and either $w_j,\ w_j'\in J$ or $V\models w_j=w_j'$ or $(w_j=w_j')\in\bar\sigma$. Suppose l_0 is the least index for which $w_{l_0},\ w_{l_0}'\in J$. Then $V(\sigma)\models u=v_{l_0}\in J$, contrary to the assumption. Hence $v_j\notin J$ $(j=1,\dots,l)$ and $v_1,\dots,v_l$ yields a proof of $u=u'$ in $V(\sigma)$.

Proof of Proposition 2.6. A system of identities σ can be supposed, without loss of generality, to consist of three parts $\sigma_J=\{(u=u')\in\sigma\colon u,u'\in J\}$, $\sigma_J'==\{(u=u')\in\sigma\colon u,u'\notin J\}$ and $\sigma_0=\{(u=u')\in\sigma\colon u\in J,u'\notin J\}$. Using Lemma 2.1, we can replace all but finitely many members of σ_0 by identities of type σ_J: if $(u=u')$, $(v=v')\in\sigma_0$ and $u'\lhd_{V(J)}v'$ then $V(J)\models v'=u_1\cdot u'\varphi\cdot u_2$ $(u_1,u_2\in F^0,\ \varphi\in\mathrm{End}\,F)$; however, $v'\notin J$ whence $V\models v'=u_1\cdot u'\varphi\cdot u_2$ and therefore $\{u=u',\ v=v'\}$ is V-equivalent to $\{u=u',\ v=u_1\cdot u'\varphi\cdot u_2\}$. Thus, one can assume that σ_0 is finite. The same holds for σ_J' because $V(J)(\sigma_J')$ is finitely based by assumption, whence σ_J' is $V(J)$-equivalent to some finite system σ^*, but then Lemma 2.7 implies also $V(\sigma_J')=V(\sigma^*)$.

Finally, $V(\sigma_J)\in[V(J), V]$ and therefore is finitely based over V. This completes the proof.

Putting together Propositions 2.5 and 2.6, we obtain a condition which can be used in proving varieties to be h.f.b. In these applications, the following lemma will be referred to several times.

Lemma 2.8. *Let V be a variety, J a fully invariant ideal in F, and M a standard form for V in J subject to the condition*

(i) *for every $u\in J$ there is a $u^*\in M$ such that $V\models u=u^*$ and $|X(u^*)|\leqq|X(u)|$.*

If $u, v\in J$, $X(u)\nsubseteq X(v)$ then for every $\varphi\in\mathrm{Dend}\,F$ with $|X(u\varphi)|\neq 1$ there is a $w\in M$ such that $|X(w)|<|X(u\varphi)|$ and $V\models u=v\Rightarrow u=w$.

Proof. Choose an arbitrary $y\in X(v\varphi)\cap X(u\varphi)$ if $X(v\varphi)\cap X(u\varphi)\neq\emptyset$ and put $y\equiv x_1$ else. Define $\psi\in\mathrm{End}\,F$ by

$$x\psi\equiv\begin{cases}x\varphi & \text{if } x\in X(u),\\ y & \text{if } x\notin X(u).\end{cases}$$

Then $u\psi\equiv u\varphi$, and $X(v\psi)=X(v\varphi)\cap X(u\varphi)$ if $X(v\varphi)\cap X(u\varphi)\neq\emptyset$, $X(v\psi)=\{y\}$ else. Now $X(v)\cap X(u)\subset X(u)$; hence $X(v\varphi)\cap X(u\varphi)\subset X(u\varphi)$ because φ is disjoint. Thus, $|X(v\psi)|<|X(u\varphi)|$, and, in virtue of (i), the term $w\equiv(v\psi)^*$ meets the requirements.

Now we give a sufficient condition, which may seem rather sophisticated at first glance, however, can be applied to reasonable classes of varieties. By $\langle u, v\rangle$ we denote the greatest common prefix of u and v, i.e. the longest subword w such that $u\equiv w\bar{u}$, $v\equiv w\bar{v}$.

Theorem 2.9. *Let V be a variety of semigroups, J a fully invariant ideal in F, $M_i\subseteqq F^0$ for $i=1, \dots, l$, and let*

$$M=\{u\equiv u_1\dots u_l\colon u_i\in M_i,\ \ \textit{and}\ u\equiv\tilde{u}\bar{u}\Rightarrow X(\tilde{u})\cap X(\bar{u})<g\}$$

be a standard form for V in J with some natural number g. Suppose, moreover, that the following conditions are fulfilled with some natural numbers n and $k\geqq n+(l-1)g+2$; condition (i) *from* Lemma 2.7, *furthermore,*

(ii) *$\langle M_i\times\Sigma, \ll_k\rangle$ is a wqo set for $i=1, \dots, l$;*

(iii) *if $v\equiv\tilde{v}\bar{v}\equiv v_1\dots v_l\in M$, $\tilde{v}\equiv v_1\dots v_{j-1}\tilde{v}_j$, $v_j\equiv\tilde{v}_j\bar{v}_j$, $\varphi\in\mathrm{Fde}\,F^0$, and $v\varphi$ is a prefix of some $v'\equiv v_1'\dots v_l'\in M$ such that $v_i'\equiv v_i$ for $i<j$, furthermore, $|\tilde{v}^{(n)}\varphi|=n$, then* (i) *is satisfied for $v\varphi$ with some $(v\varphi)^*$ s. th. either $(v\varphi)_i^*\equiv\equiv v_i\varphi$ for $i=1, \dots, j-1$, $|\langle v_j\varphi, (v\varphi)_j^*\rangle|\geqq|\tilde{v}_j\varphi|-n$ or, for some $h\leqq j$, $(v\varphi)_i^*\equiv\equiv v_i\varphi$ for $i<h$, $(v\varphi)_h^*$ is a proper prefix of $v_h\varphi$ (of $\tilde{v}_j\varphi$, if $h=j$).*

Then $[V(J), V)$ is finitely based.

Proof. Fix a factorization $u \equiv u_1 \dots u_l$, $u_i \in M_i$, for every $u \in M$. Define $<$ on M by

$$v < u \quad \text{iff either} \quad |X(v)| < |X(u)|,$$
$$\text{or} \quad |X(v)| = |X(u)|, \quad v_i \equiv u_i \quad \text{for} \quad i = 1, \dots, j-1, \quad v_j <_{\text{lex}} u_j.$$

Furthermore, for $(u, v) \in M^*$ set $u_i \equiv v_i$ if $i<j$, $u_j \not\equiv v_j$, and

$$u \equiv w x_e \bar{u}, \quad w \equiv u_1 \dots u_{j-1} \tilde{v}_j, \quad \tilde{v}_j \equiv \langle u_j, v_j \rangle,$$

$$v_j \equiv \begin{cases} \tilde{v}_j & \text{or} \\ \tilde{v}_j x_d \hat{v} \bar{v}_j, \end{cases} \quad |\hat{v}| = n \quad \text{or} \quad |\hat{v}| < n, \quad \bar{v}_j = \emptyset, \quad v \equiv \begin{cases} w\bar{v} & \text{or} \\ w x_d \hat{v} \bar{v}. \end{cases}$$

If $v_j \equiv \tilde{v}_j$, we put $d=e$, $\hat{v} \equiv \emptyset$. Let u_0 denote the product of all different variables of $\bigcup_{i<h} (X(u_i) \cap X(u_h)) = \bigcup_{i=1}^{l-1} (X(u_1 \dots u_i) \cap X(u_{i+1} \dots u_l))$ (which shows that $|u_0| \leqq (l-1)g$) in the order of their first occurrence in u, say. Suppose that $x_{c(1)}, \dots, x_{c(r)}$ is the sequence of all different letters of $a \equiv x_d x_e (w x_d \hat{v})^{(n)} u_0$; clearly, $r \leqq |a| \leqq (l-1)g + n + 2 = k$. Choose $\pi \in \Sigma$ such that $t\pi = c(t)$ for $t \leqq r$, and for $(u, v), (u', v') \in M^*$ put

$$(u, v) \prec (u', v') \quad \text{iff} \quad (u_i, \pi) \ll_k (u_i', \pi') \quad \text{for} \quad i = 1, \dots, l,$$
$$r = r', \quad j = j', \quad |w|_e = |w'|_{e'}, \quad T(x_d x_e \hat{v}) = T(x_{d'} x_{e'} \hat{v}'),$$
$$|X(u)| = |X(v)| \Leftrightarrow |X(u')| = |X(v')|, \quad w \equiv v \Leftrightarrow w' \equiv v', \quad \tilde{v}_j \equiv v_j \Leftrightarrow \tilde{v}_j' \equiv v_j'$$

(letters with $'$ denote objects which belong to (u', v')).

Lemma 2.2 implies that $(M, <)$ is a well-ordered set, because $|u| \leqq p|X(u)|$ with some constant p. Furthermore, as $r, j, |w|_e$ and $|x_d x_e \hat{v}|$ are bounded, and the equivalences decompose M^* in eight $\prec$-independent classes, the qo-set $(M^*, \prec)$ is wqo in virtue of (ii). Thus, it remains to prove that (A) is satisfied.

If $(u, v) \prec (u', v')$ then there are disjoint endomorphisms $\varphi_1, \dots, \varphi_l$ such that $u_i \varphi_i \equiv u_i'$, $x_{c(t)} \varphi_i \equiv x_{c'(t)}$ for $t = 1, \dots, r$ and $i = 1, \dots, l$; in particular, φ_i and φ_h coincide on $X(u_i) \cap X(u_h)$. Hence the endomorphism φ given by

$$x_s \varphi \equiv \begin{cases} x_s \varphi_i & \text{if} \quad x_s \in X(u_i), \\ x_s \varphi_1 & \text{if} \quad x_s \notin X(u) \end{cases}$$

is well-defined and disjoint. We have $u_i \varphi \equiv u_i'$, $u\varphi \equiv u'$. Hence $V \models u' = (v\varphi)^*$, and all we have to show is $(v\varphi)^* < u'$. Clearly, we can suppose $|x_s \varphi| = 1$ for $x_s \notin X(u)$; hence, by (i),

$$|X(u')| - |X((v\varphi)^*)| \geqq |X(u\varphi)| - |X(v\varphi)| \geqq |X(u)| - |X(v)| \geqq 0.$$

This proves the assertion for the case $|X(v)| < |X(u)|$ (in virtue of Lemma 2.8, even for $X(v) \neq X(u)$ if $|X(u')| \neq 1$). So let $|X(v)| = |X(u)|$, $|X(u')| = |X((v\varphi)^*)|$. Then we have also $|X(u')| = |X(v')|$. Next note that $|w|_e = |w'|_{e'}$ and $x_e \varphi \equiv x_{e'}$ (as $e = 2\pi$, $e' = 2\pi'$) guarantee $w\varphi \equiv w'$. If, moreover, $\tilde{v}_j \equiv v_j$ then $\tilde{v}_j' \equiv v_j'$, i.e. $v_i \varphi \equiv v_i'$ for the first j

components of v'. Hence, according to (iii), either $(v\varphi)_1^* \equiv v_1', \ldots, (v\varphi)_{h-1}^* \equiv v_{h-1}'$, $(v\varphi)_h^*$ is a proper prefix of v_h' for some $h \leqq j$ or $(v\varphi)_i^* \equiv v_i'$ for $i=1, \ldots, j$. In the first case $(v\varphi)^* < v' < u'$, in the second one $(v\varphi)^* < u'$, too, because $v_j' <_{\text{lex}} u_j'$. If, on the other hand, $v_j \equiv \tilde{v}_j x_d \hat{v} \bar{v}_j$, then $v_j' \equiv \tilde{v}_j' x_{d'} \hat{v}' \bar{v}_j'$, $d<e$, $d'<e'$ (because $v<u$, $v'<u'$), and $T(x_d x_e \hat{v}) = T(x_{d'} x_{e'} \hat{v}')$ implies, in particular, $|\hat{v}| = |\hat{v}'|$. Now either $|\hat{v}|<n$, then we have $v_j' \equiv \tilde{v}_j' x_{d'} \hat{v}' \equiv (\tilde{v}_j x_d \hat{v})\varphi \equiv v_j \varphi$, and the same argument as for the case $\tilde{v}_j \equiv v_j$ prevails (only $v_j' < u_j'$ follows now from $d'<e'$); or $|\hat{v}|=n$, and, again by (iii), either there is an $h \leqq j$ such that $(v\varphi)_i^* \equiv v_i \varphi \equiv v_i'$ for $i<h$, $(v\varphi)_h^*$ is a proper prefix of v_h' (of $\tilde{v}_j' x_{d'} \hat{v}'$ if $h=j$) whence $(v\varphi)^* < v'$, or $(v\varphi)_i^* \equiv v_i'$ for $i=1, \ldots, j-1$, $|\langle v_j', (v\varphi)_j^* \rangle| \geqq |\tilde{v}_j' x_{d'} \hat{v}'|$, i.e. $(v\varphi)_j^* \equiv v_j' x_{d'} \bar{w}_j <_{\text{lex}} u_j'$, which yields the proof for this case, the last one.

In the special case $l=1$ Condition (iii) reads somewhat simpler:

Corollary 2.10. *Let V be a variety of semigroups, J a fully invariant ideal in F, and $M \subset F^0$ standard for V in J. Suppose that $\langle M, \ll_k \rangle$ is a wqo set for some $k \geqq 2$,* (i) *holds, and for some $n \leqq k-2$ we have*

(iii′) *if $v \equiv \tilde{v} \bar{v} \in M$, $\varphi \in \mathrm{Fde}\, F^0$, $\tilde{v}\varphi$ is a prefix of some $v' \in M$, and $|\tilde{v}^{(n)}\varphi| = n$, then* (i) *satisfied for some standard form $(v\varphi)^*$ of $v\varphi$ such that either $(v\varphi)^*$ is a prefix of $v\varphi$ or $|\langle v\varphi, (v\varphi)^* \rangle| \geqq |v\varphi| - n$.*

Then $[V(J), V)$ is finitely based.

Remark 1. If V is homotypical (i) is fulfilled.

Remark 2. It is not difficult to distil from the proof that (iii) can be weakened in the following manner. Instead of $v \in M$ we consider pairs $(v, \varrho) \in M \times \Sigma$, and we require (iii) only for those $\varphi \in \mathrm{Fde}\, F^0$ such that $|\chi_i \varphi| = 1$ for $1 \leqq i \leqq k-n-2$. This enables us to dispose not only of the elements of $X(x_d x_e (w x_d \hat{v})^{(n)} u_0)$ but of some more variables, too, provided k is sufficiently large. It is precisely in this form that Theorem 2.9 will be applied at the end of the paper.

The next two theorems are devoted to special cases where the conditions can be weakened.

Theorem 2.11. *Let I be a fully invariant ideal of F. If $\langle (F \setminus I) \times \Sigma, \ll_2 \rangle$ is a wqo set then $SG(I)$ is h.f.b.*

Proof. Choose an $a \in I$, and set $M = (F \setminus I) \cup \{a\}$. Define $v < u$ iff either $v \equiv a$, $u \in F \setminus I$ or $v, u \in F \setminus I$ and $v <_{\text{lex}} u$. By Lemma 2.2, $<$ is a well-order.

For $(u, v) \in M^*$ put

$$u \equiv w x_e \bar{u}, \quad v \equiv \begin{cases} w & \text{or} \\ w x_d \bar{v}, & d \neq e, \end{cases} \quad \pi = \begin{pmatrix} 1 & 2 \ldots \\ d & e \ldots \end{pmatrix}$$

if $v \not\equiv w$. Define

$$(u, v) \prec (u', v') \quad \text{iff either} \quad u \ll u', \quad v \equiv a, \quad \text{or} \quad u \ll u', \quad v \equiv w,$$

$$\text{or} \quad (u, \pi) \ll_2 (u', \pi'), \quad v' \not\equiv a, w.$$

Clearly, $\prec$ is a wqo relation on M^*. Note that $u, u' \not\equiv a$ and if $v \equiv w$ then also $v \not\equiv a$.

Anyway, there is a $\varphi \in \mathrm{Fde}\, F$ such that $u' \equiv u\varphi$. If $|X(v)| < |X(u)|$ then we can suppose that $|X(v\varphi)| < |X(u\varphi)|$ whence $v\varphi < u\varphi$. Now let $|X(v)| = |X(u)|$. If $u \ll u'$, $v \equiv a$ then $u' \equiv u\varphi = (v\varphi)^* \equiv a < u'$. If $u \ll u'$, $v \equiv w$, then $u' \equiv u\varphi \equiv w\varphi \cdot (x_e \bar{u})\varphi > w\varphi \equiv v\varphi$. If $v, v' \notin \{a, w\}$, $(u, \pi) \ll_2 (u', \pi')$, then $u' \equiv u\varphi$, $x_{d'} \equiv x_d \varphi$, $x_{e'} \equiv x_e \varphi$, $d' < e'$. Hence $u\varphi \equiv w\varphi \cdot x_{e'} \cdot \bar{u}\varphi$, $v\varphi \equiv w\varphi \cdot x_{d'} \cdot \bar{v}\varphi$, and either $v\varphi \in I$, $(v\varphi)^* \equiv a < u'$, or $v\varphi \in F \setminus I$, $v\varphi <_{\mathrm{lex}} u'$ whence $v\varphi < u'$. This completes the proof.

Theorem 2.12. *If V, J, M are as in* Corollary 2.10, (i) *holds, and $\langle M^2 \times \Sigma, \ll_2^2 \rangle$ is wqo, then $[V(J), V)$ is finitely based.*

Proof. Define $<$ by

$$v < u \quad \text{iff either} \quad |X(v)| < |X(u)| \quad \text{or} \quad |X(v)| = |X(u)|, \quad v <_{\mathrm{lex}} u.$$

For $(u, v) \in M^*$ set $w \equiv \langle u, v \rangle$, $u \equiv w x_e \bar{u}$, $v \equiv w$ or $v \equiv w x_d \bar{v}$, $d < e$, and put $d = 1 + \max\{i : x_i \in X(u) \cup X(v)\}$, $\bar{v} \equiv \emptyset$ if $v \equiv w$. Let

$$\pi = \begin{pmatrix} 1 & 2 \ldots \\ d & e \ldots \end{pmatrix},$$

and define

$$(u, v) \prec (u', v') \quad \text{iff} \quad (u, v; \pi) \ll_2^2 (u', v'; \pi'), \quad |w|_e = |w'|_{e'},$$

$$X(v) = X(u) \Leftrightarrow X(v') = X(u'), \quad v \equiv w \Leftrightarrow v' \equiv w'.$$

Obviously, $<$ is a well-order on M and $\prec$ is a wqo on M^*. If $X(v) \neq X(u)$ and $|X(u')| \neq 1$ then (A) follows from Lemma 2.8. If $|X(u')| = 1$ then $|X(u)| = 1$ by $u \ll u'$ and $|X(v')| = |X(v)| = 1$ by $v' < u'$, $v < u$. If, besides, $X(v) \neq X(u)$ then $X(v') \neq X(u')$; hence $u \equiv x_e^m, v \equiv x_d^n, u' \equiv x_{e'}^{m'}$, $v' \equiv x_{d'}^{n'}$, $d < e$, $d' < e'$, $m | m'$, and putting $x_e \varphi \equiv x_{e'}^{m'/m}$, $x_d \varphi \equiv x_{d'}$, we have $u' \equiv u\varphi$, $v\varphi = (v\varphi)^* < u'$. Finally, let $X(v) = X(u)$. Then $X(v') = X(u')$, and there is a $\varphi \in \mathrm{Fde}\, F^0$ such that $u\varphi \equiv u'$, $x_d \varphi \equiv x_{d'}$, $x_e \varphi \equiv x_{e'}$, $v\varphi \in M$. Now $|w|_e = |w'|_{e'}$ implies $w\varphi \equiv w'$, and either $v \equiv w$, $v\varphi \equiv w\varphi \equiv w' \equiv v' < u'$ or $v \equiv w x_d \bar{v}$, $v\varphi \equiv w' x_{d'} \cdot \bar{v}\varphi < u'$ because $d' < e'$. This completes the proof.

Remark. Of course, $\langle M^2 \times \Sigma, \ll_2^2 \rangle$ is wqo if and only if $\langle M^* \times \Sigma, \ll_2^2 \rangle$ is. Hence we could have defined in advance and replaced M^2 by M^* in the text of the theorem. This will be our way in the next section (Lemma 3.7).

3. Standard forms and h.f.b. varieties. In this section we show some (comparatively large) particular subsets of F^0 to be good standard forms whenever they are standard and part of the conditions (i)—(iii) (or (iii′)) is satisfied.

Theorem 3.1. *If $F^{(p)}_{(n)}$ is standard for V in J and* (i), (iii′) *hold* (*with some* $n\geqq 0$), *then* $[V(J), V)$ *is finitely based.*

Proof. By Corollary 2.10, it is sufficient to show that $\langle F^{(p)}_{(n)}\times\Sigma, \ll_k\rangle$ is a wqo set for every k. The proof will be accomplished through a succession of lemmas.

Lemma 3.2. *$F_{(n)}$ is wqo under $\ll$.*

Proof. Denote by T_n the set of all semiireducible types of length $\leqq n$, and define the quasi-order relation $\prec$ on $\mathbf{P}\times\mathsf{T}_n$ by

$$(k,T)\prec(k',T') \quad \text{iff} \quad k<k', \quad T=T'.$$

As T_n is finite, $\mathbf{P}\times\mathsf{T}_n$ is a wqo set under $\prec$, and, according to [2], so is the set V of vectors $(\alpha_1,\dots,\alpha_l)$, $\alpha_i\in\mathbf{P}\times\mathsf{T}_n$, of arbitrary length under the relation

$$(\alpha_1,\dots,\alpha_l)\prec(\beta_1,\dots,\beta_m) \quad \text{if there is a sequence} \quad i(1)<\dots<i(l)=m \quad \text{such that} \quad \alpha_j\prec\beta_{i(j)}$$

(the additional condition $i(l)=m$ accepted here obviously does not change the situation). Assign to $u\in F_{(n)}$ the vector $\mathbf{a}(u)=(\alpha_1,\dots,\alpha_{\bar{s}})$ where $\alpha_i=(|a_i|, T(\tilde{w}_i))$ (see (1.5)), and put

$$u\prec u' \quad \text{iff} \quad \mathbf{a}(u)\prec\mathbf{a}(u') \quad \text{and} \quad T(\tilde{w}_0)=T(\tilde{w}_0').$$

This relation is a wqo, too, because $F^0_{(n)}\to V\times\mathsf{T}_n$ $(u\mapsto(\mathbf{a}(u), T(\tilde{w}_0)))$ is a strict homomorphism of $(F^0_{(n)}, \prec)$ onto a wqo set. On the other hand, if $u\prec u'$ then we can construct a $\varphi\in\mathrm{Fde}\,F^0$ such that $u\varphi\equiv u'$: there exist endomorphisms $\varphi_j\in\mathrm{Fde}\,F^0$, $j=0,\dots,\bar{s}$, with $(a_j\tilde{w}_j)\varphi_j\equiv a'_{i(j)}\tilde{w}'_{i(j)}$ (where $i(0)=0$, $a_0\equiv a_0'\equiv\emptyset$). Denote the first letter of a_j by $x_{r(j)}$, and put

$$x_t\varphi\equiv\begin{cases} x_t\varphi_j & \text{if} \quad x_t\in X(a_jw_j), \quad t\neq r(j),\\ \Big(\prod\limits_{k=i(j-1)+1}^{i(j)-1} a_k'\tilde{w}_k'\Big)\cdot x_{r(j)}\varphi_j & \text{if} \quad t=r(j),\\ x_{t+N} & \text{if} \quad x_t\notin X(u),\end{cases}$$

where $N=\max\limits_{x_i\in X(u')} i$. It is easy to see that φ fits for our aim.

Lemma 3.3. *If M is closed for subwords, $\ll$ is a wqo on M, and the length of the irreducible elements of M is bounded then $\ll_k$ is a wqo on $M\times\Sigma$ for every $k\geqq 0$.*

Proof. Let $(u,\pi)\in M\times\Sigma$ and suppose that $u_{i(1)},\dots,u_{i(l)}$ $(i(1)<\dots<i(l))$ are those irreducible factors of u which contain some $x_{s\pi}$, $s\leqq k$. Put $u_\pi\equiv u_{i(1)}\cdots$

$\ldots u_{i(l)}$ and suppose that $x_{s\pi}$ occurs in u_π for the first time at the m_s-th place (i.e. $u_\pi \equiv \bar{u}_\pi x_{s\pi} \bar{\bar{u}}_\pi$, $x_{s\pi} \notin X(\bar{u}_\pi)$, $|\bar{u}_\pi| = m_s - 1$); if $x_{s\pi} \notin X(u)$ put $m_s = \infty$. Clearly, $u =! \, v_0 \prod_{j=1}^{l} u_{i(j)} v_j$. Assign to (u, π) the vector

$$\mathbf{b}(u, \pi) = \langle m_1, \ldots, m_k; l; T(u_{i(1)}), \ldots, T(u_{i(l)}); v_0, \ldots, v_l \rangle$$

and set

$$\mathbf{b}(u, \pi) \prec \mathbf{b}(u', \pi') \quad \text{iff} \quad m_s = m_s', \quad l = l', \quad T(u_{i(r)}) = T(u'_{i(r)}),$$

$$v_j \ll v_j' \quad \text{for} \quad 1 \leqq s \leqq k, \quad 1 \leqq r \leqq l, \quad 0 \leqq j \leqq l.$$

Then $(u, \pi) \prec (u', \pi') \Leftrightarrow \mathbf{b}(u, \pi) \prec \mathbf{b}(u', \pi')$ defines a wqo on $M \times \Sigma$. Indeed, $(u, \pi) \mapsto \mathbf{b}(u, \pi)$ is then a strict homomorphism between quasi-ordered sets, and the set of the vectors $\mathbf{b}$ is wqo under $\prec$ because if N is an upper bound of $|u|$ for irreducible $u \in M$ then $l \leqq k$, $m_s \leqq |u_\pi| \leqq kN$, and $T(u_{i(r)})$ can take also only a finite number of different values and the assertion follows from Lemma 3.2. Furthermore, if $(u, \pi) \prec (u', \pi')$ then we can define $\varphi \in \operatorname{Fde} F^0$ so that $v_j \varphi \equiv v_j'$, $u_{i(r)} \varphi \equiv u'_{i(r)}$, and then $|u_\pi| = |u'_{\pi'}|$, $m_s = m_s'$ guarantees also $x_{s\pi} \varphi \equiv x_{s\pi'}$ for $s = 1, \ldots, k$, i.e. $(u, k) \ll_k (u', \pi')$.

As an immediate consequence of Lemmas 3.2 and 3.3 we get

Corollary 3.4. *$F_{(n)} \times \Sigma$ is wqo under $\ll_k$ for every $k > 0$.*

Note, however, that Lemma 3.3 is only seemingly more general than Corollary 3.4 because it is not difficult to see that if the conditions of the lemma are fulfilled then $M \subseteqq F_{(n)}$ for some n.

Finally we prove

Lemma 3.5. *$F_{(n)}^{(p)} \times \Sigma$ is a wqo set under $\ll_k$ for every $k > 0$.*

Proof. For $(u, \pi) \in F_{(n)}^{(p)} \times \Sigma$ let $s_1 < \ldots < s_l \leqq k$ be those indices for which $x_{s_i \pi} \in X(a_0 \ldots a_t)$ (see (1.6)), and suppose that $x_{s_i \pi}$ occurs in $a_0 \ldots a_t$ for the first time at the m_i-th place. Assign to (u, π) the vector

$$\mathbf{c}(u, \pi) = \mathbf{c}\langle l, t; s_1, \ldots, s_l; m_1, \ldots, m_l; T(a_0), \ldots, T(a_t), T(a_0 \ldots a_t); \tilde{u}_1, \ldots, \tilde{u}_t \rangle$$

and put

$$\mathbf{c}(u, \pi) \prec \mathbf{c}(u', \pi') \quad \text{if the first} \quad 2l + t + 4 \quad \text{components of both}$$

$$\text{vectors coincide and} \quad (\tilde{u}_j, \pi) \ll_k (\tilde{u}_j', \pi') \quad \text{for} \quad j = 1, \ldots, t.$$

Define $(u, \pi) \prec (u', \pi') \Leftrightarrow \mathbf{c}(u, \pi) \prec \mathbf{c}(u', \pi')$. As in the proof of Lemma 3.4, we can see that $F_{(n)}^{(p)} \times \Sigma$ is a wqo set under $\prec$. Furthermore, if $(u, \pi) \prec (u', \pi')$ then we can define $\varphi_0 \in \operatorname{Fde} F^0$ such that $(a_0 \ldots a_t) \varphi_0 \equiv a_0' \ldots a_t'$ which guarantees also $x_{s_i \pi} \varphi_0 \equiv x_{s_i \pi'}$, $a_r \varphi_0 = a_r'$ for $i = 1, \ldots, l$; $r = 0, \ldots, t$, and $\varphi_j \in \operatorname{Fde} F^0$ such that $\tilde{u}_j \varphi_j \equiv \tilde{u}_j'$, $x_{s\pi} \varphi_j \equiv x_{s\pi'}$. Putting together $\varphi_0, \ldots, \varphi_j$ (which is possible in virtue of (1.6)—(1.7)), we obtain a $\varphi \in \mathrm{Fde}\, F^0$ with $u\varphi \equiv u'$, $x_{s\pi}\varphi \equiv x_{s\pi'}$ for $s=1, \ldots, k$. This proves the lemma and also the theorem.

In some special cases one can omit condition (iii′). We give here one theorem of this kind.

Theorem 3.6. *If $F_{(1)}^{(p)}$ is standard for V in J and* (i) *holds then $[V(J), V)$ is finitely based.*

In virtue of Theorem 2.12, it suffices to prove

Lemma 3.7. *$F_{(1)}^{(p)*} \times \Sigma$ is a wqo set under $\ll_k^2$ for every $k \geqq 1$.*

Proof. Let $(u, v; \pi) \in F_{(1)}^{(p)*} \times \Sigma$, $v \equiv b_0 \prod_{i=1}^{r} \tilde{v}_i b_i$ be the decomposition of v indicated in (1.6). By Lemma 3.5 and Proposition 2.3, $F_{(1)}^{(p)} \times G_{2p+k,k}$ is wqo under $\prec$ defined in (2.1). Put

$$(u, v;\ \pi) \prec (u', v';\ \pi') \overset{\text{def}}{\Leftrightarrow}$$

$$\overset{\text{def}}{\Leftrightarrow} (u;\ x_{1\pi}, \ldots, x_{k\pi}, a_0, \ldots, a_t, b_0, \ldots, b_r) \prec (u';\ x_{1\pi'}, \ldots, x_{k\pi'}, a_0', \ldots, a_{t'}', b_0', \ldots, b_{r'}'),$$

$$t = t', \quad r = r', \quad |a_i| = |a_i'|, \quad |b_j| = |b_j'|.$$

Clearly $\prec$ is a wqo on $F_{(1)}^{(p)*} \times \Sigma$, and there is a $\varphi \in \mathrm{Fde}\, F^0$ such that $u\varphi \equiv u'$, $a_i\varphi \equiv \equiv a_i'$, $b_j\varphi \equiv b_j'$. Moreover, we can suppose that $x_l\varphi$ is simple for every $x_l \in X$ (for $x_l \in X(u)$ this holds automatically, as $\tilde{u}\varphi \equiv \tilde{u}'$, and $|x_l\varphi| = 1$ for $x_l \in X(a_1 \ldots a_r)$). Thus, $v\varphi \equiv b_0' \prod_{i=1}^{r} \tilde{v}_i\varphi \cdot b_i' \in F_{(1)}^{(p)}$, because $\tilde{v}_i\varphi \in F_{(1)}$, $\left|\prod_{i=0}^{r} b_i'\right| \leqq p$. This proves the lemma.

Theorem 3.8. *Let $M_i \subseteqq F_{(n)}^{(p)}$ for $i=1, \ldots, l$. If*

$$M = \{u \equiv u_1 \ldots u_l\colon\ u_i \in M_i,\ |X(u_i) \cap X(u_j)| \leqq q \text{ for } i \neq j\}$$

is standard for V in J and (i), (iii) *hold (with some $n \geqq 0$), then $[V(J), V)$ is finitely based.*

Proof. It is easy to see that if $\tilde{u}\bar{u} \in M$ then $|X(\tilde{u}) \cap X(\bar{u})| \leqq (n+p)/2 + l^2q/4$. Now the assertion follows from Lemma 3.5 and Theorem 2.9.

We mention two more special cases.

Theorem 3.9. *If $F_{(n)}$ is a standard form for V and* (i) *holds then V is h.f.b.*

Proof. The theorem becomes a special case of Theorem 3.1 (with $J=F$) if we show that (iii′) holds (with $n+1$ instead of n). So let $v \equiv \tilde{v}\bar{v} \in F_{(n)}$, $v \equiv v_0 \prod_{i=1}^{s} x_{c(i)} v_i$

its semiirreducible factorization, $|v_i|\leqq n$,

$$\tilde v =!\, v_0 \prod_{i=1}^{l-1} x_{c(i)} v_i \cdot x_{c(l)} \tilde v_l, \quad \bar v = !\bar v \prod_{i=l+1}^{s} x_{c(i)} v_i, \quad \tilde v_l \bar v_l \equiv \bar v,$$

and $\varphi \in$ F de F^0,

$$\tilde v \varphi =!\, v_0' \prod_{j=1}^{r} x_{d(j)} v_j',$$

$|v_j'|\leqq n$ (i.e. $\tilde v\varphi \in F_{(n)}$), $|v^{(n+1)}\varphi| = n+1$. As $|\tilde v_l|\leqq n$, we have $|x_{c(l)}\varphi|=1$. Furthermore, by Lemma 1.3, $v\varphi =!\, w\cdot x_{c(l)}\varphi \cdot \bar w$. Hence $w\cdot x_{c(l)}\varphi\cdot \bar w^* \in F_{(n)}$, since it can be obviously achieved that $X(w\cdot x_{c(l)}\varphi)\cap X(\bar w^*)=\emptyset$. This proves the assertion, as $|\tilde v\varphi| = |\tilde v| < n$.

Proposition 3.10. *Let* $J=F_{(n)}^{(p)}$. *The variety* $SG(J)$ *is h.f.b.*

Proof. Follows from Theorem 2.11 and Lemma 3.5.

Part II. Application: a class of h.f.b. identities

The aim of this part is to prove the following

Theorem A. *A non-balanced identity of the form*

$$(*) \qquad u \equiv x_1 \dots x_i x_{i+1} x_i x_{i+2} \dots x_n = x_{1\pi}^{e(1)} \dots x_{m\pi}^{e(m)} \equiv v \quad (\pi\in\Sigma,\, e(j)\leqq 2)$$

is h.f.b. if and only if v is not of the form

$$(**) \qquad v \equiv x_1 \dots x_{i-1} x_{i\pi}^2 x_{(i+1)\pi}^2 x_{i+2} \dots x_n \quad (\pi = (i\ i+1) \text{ or identical},\ n>2).$$

The assertion will be broken up into several propositions. From know on V denotes $SG(*)$.

4. Two special cases. To start with, we settle the negative part of the assertion. Of course, here one cannot utilize the results of Part I.

Proposition 4.1. *The identity*

$$(\tau) \qquad x_1 \dots x_i x_{i+1} x_i x_{i+2} \dots x_n = x_1 \dots x_{i-1} x_i^2 x_{i+1}^2 x_{i+2} \dots x_n$$

is h.f.b. iff $n=2$.

Proof. The fact that $xyx=x^2y^2$ is h.f.b. has been proved in [5]. So let $n>2$ and, say, $i>1$. Consider the identity

$$(\sigma_m) \qquad tyztx_1^2 \dots x_{2m}^2 = tyztx_1^2 \dots x_{2m-2}^2 x_{2m}^2 x_{2m-1}^2$$

and the infinite systems $(\sigma)=\{\sigma_m\colon m=1, \dots\}$, $(\sigma^k)=\{\sigma_m\colon m\neq k\}$. We claim that the system $\sigma\cup\{\tau\}$ is independent. Clearly τ does not follow from σ, so we have to prove that $\sigma^k\cup\{\tau\}\not\vdash\sigma_k$. To see this, we show that if $\sigma^k\cup\{\tau\}\vdash tyztx_1^2\dots x_{2k}^2=w$ then

$$\text{(4.1)}\qquad \begin{gathered} w=!(tyzt)\cdot\Big(\prod_{j=1}^{l}p_j\Big),\quad p_j\in T(xyx)\cup T(x^2),\\ p_l\equiv x_{2k}^2 \ \text{ or } \ p_l\equiv x_{2k-1}x_{2k}x_{2k-1},\quad X\Big(\prod_{j=1}^{l}p_j\Big)=\{x_1,\dots,x_{2k}\}, \end{gathered}$$

whence $w\not\equiv tyztx_1^2\dots x_{2k-2}^2x_{2k}^2x_{2k-1}^2$. Indeed, let $w_0(\equiv tyzt\,x_1^2\dots x_{2k}^2)$, $w_1,\dots,w_r(\equiv w)$ be a sequence of terms such that, for every $s=1,\dots,r$, there exist $w_s', w_s''\in F^0$, $\varphi_s\in\operatorname{End}F$, and $(u_s=v_s)\in\overline{\sigma^k\cup\{\tau\}}$ which satisfy $w_{s-1}\equiv w_s'\cdot u_s\varphi_s\cdot w_s''$, $w_s\equiv w_s'\cdot v_s\varphi_s\cdot w_s''$, Suppose, furthermore, that w_{s-1} is of the form (4.1) for some $s\leqq r$ (this certainly is the case for $s=1$). First let $u_s=v_s\in\sigma^k$; by symmetry, we can assume that $u_s\equiv tyztx_1^2\dots x_{2m}^2$. Sure enough, $m<k$ because $tyztx_1^2\dots x_{2m}^2\not\triangleleft w_{s-1}$ for $m>k$. Moreover, the only subword of w_{s-1} which is an endomorphic image of $tyzt$ is $tyzt$ itself, and the only subwords which are squares are those of the form x_j^2. Hence $u_s\varphi\in T(u_s)$ and

$$w_{s-1}=!\,u_s\varphi_s\prod_{j=2m+1}^{l}p_j\equiv tyztx_{1\pi}^2\dots x_{(2m)\pi}^2\prod_{j=2m+1}^{l}p_j,\quad w_s=!\,v_s\varphi_s\cdot\prod_{j=2m+1}^{l}p_j,$$

$\pi\in\Sigma_{2m}$, $l\geqq 2m+2$, whence also w_s is of the form (4.1). If

$$u_s\equiv x_1\dots x_{i-1}x_i^2x_{i+1}^2x_{i+2}\dots x_n,\quad v_s\equiv x_1\dots x_ix_{i+1}x_ix_{i+2}\dots x_n$$

then $(x_i^2x_{i+1}^2)\varphi_s\in T(x^2y^2)$ by the same reason as above, i.e. $(x_i^2x_{i+1}^2)\varphi_s\equiv p_{j-1}p_j$ for some $j\leqq l$, and w_s differs from w_{s-1} only in these factors which are replaced by some $p_j'\in T(xyx)$; thus, w_s again is of the form (4.1) because if $j=l$ (which, by the way, can occur only if $i+1=n$) then $x_{2k-1}^2x_{2k}^2$ is replaced by $x_{2k-1}x_{2k}x_{2k-1}$. Finally, if $u_s\equiv x_1\dots x_ix_{i+1}x_ix_{i+2}\dots x_n$ then $(x_ix_{i+1}x_i)\varphi_s\in T(xyx)$ because the only subwords of w_{s-1} which are endomorphic images of xyx are those of the form $x_qx_rx_q$ ($\equiv p_j$ for some j) and $tyzt$, but this latter one is out of consideration because if $(x_ix_{i+1}x_i)\varphi_s\in tyzt$ then $u_s\varphi\equiv u_s'tyxtu_s''$ with $u_s'\not\equiv\emptyset$ since $i>1$, which is impossible. Therefore this case is similar to the previous one.

If $i=1$ then $n>i+1$ and we can consider the identities

$$(\sigma_m')\qquad x_1^2\dots x_{2m}^2tyzt=x_2^2x_1^2x_3^2\dots x_{2m}^2tyzt$$

instead of σ_m, and dualize the above reasoning (with the only — unessential — difference that here $p_1\equiv x_1^2$ or $x_1x_2x_1$ which is not dual to $p_l\equiv x_{2k-1}x_{2k}x_{2k-1}$). This completes the proof.

Next we deal with a special case.

Lemma 4.2. *The identity*

(4.2) $$(u \equiv)\, x_1 \dots x_i x_{i+1} x_i \dots x_n = x_{1\pi} \dots x_{m\pi} (\equiv v) \quad (\pi \in \Sigma)$$

is h.f.b.

Proof. First suppose that the symmetrical difference $X(u) \div X(v) = \{x_i\}$. By repeated applications of (4.2), any word w of F^{n+1} can be brought to the form $w^* \equiv \equiv w^*_{(i-1)} x^{d(1)}_{c(1)} \dots x^{d(k)}_{c(k)} w^{*(n-i-1)}$, $d(j) \leqq 2$; besides, the number of variables either does not change or decreases by 1 at every step. Furthermore, applying (4.2) twice, using the endomorphisms

$$x_j\varphi \equiv \begin{cases} x_{2i} & \text{if } j = i, \\ x_{2i+j} & \text{if } j \neq i, \end{cases} \qquad x_j\psi \equiv \begin{cases} x_{i+j} & \text{if } j \leqq i, \\ x_{2i+j} & \text{if } j > i+2, \\ x_{2i} \dots x_{3i-1} & \text{if } j = i+1, \\ x_{3i+1} x_{2i} x_{3i+2} & \text{if } j = i+2, \end{cases}$$

respectively, we obtain

$$x_1 \dots x_{2i-1} x^2_{2i} x_{2i+1\pi} \dots x_{2i+(n-1)\pi} x_{2i+n+1} \dots x_{2n+i-1} =$$

$$= x_1 \dots x_{2i-1} x^2_{2i} \cdot v\varphi \cdot x_{2i+n+1} \dots x_{2n+i+1} = x_1 \dots x_{2i-1} x^2_{2i} \cdot u\varphi \cdot x_{2i+n+1} \dots x_{2n+i-1} =$$

$$= x_1 \dots x_{2i-1} x^2_{2i} x_{2i+1} \dots x_{3i-1} x_{2i} x_{3i+1} x_{2i} x_{3i+2} \dots x_{2n+i-1} =$$

$$= x_1 \dots x_i \cdot u\psi \cdot x_{2i+n+1} \dots x_{2n+i-1} = x_1 \dots x_i \cdot v\psi \cdot x_{2i+n+1} \dots x_{2n+i-1} =$$

$$= x_1 \dots x_i w x_{2i} w' x_{2i} w'' x_{2i+n+1} \dots x_{2n+i-1}, \quad w' \not\equiv \emptyset,$$

and a third application of (4.2) relieves us from x_{2i}. Hence $V \models w^* = w^{**} \equiv \equiv w^{**}_{(2i-1)} x_{f(1)} \dots x_{f(r)} w^{**(2n-i-2)} \in F^{[2n+i-3]}_{(1)}$ and $X(w^{**}) \subseteq X(w^*) \subseteq X(w)$. Thus, by Lemma 1.1 and Theorem 3.6 $[V(F^{2n+i-3}), V)$ is finitely based, whence the assertion follows obviously.

If (4.2) is heterotypical, and $X(u) \div X(v) \neq \{x_i\}$, we can assume that $k\pi > n$ for some $k \leqq m$ (i.e. $x_{k\pi} \notin X(u)$). Indeed, if this is not the case, then there is a $j \leqq n$, $j \neq i$, such that $j\pi^{-1} > m$ (i.e. x_j does not occur on the right side). First let $j \neq i+1$, say $j > i+1$, and let j be maximal. Executing in (4.2) the substitution $x_j \mapsto x_j x_{n+1}$ on the one hand, and $x_{j+1} \mapsto x_{n+1}$, $x_{j+2} \mapsto x_{j+1}$, ..., $x_n \mapsto x_{n-1}$ on the other, we obtain

$$u \equiv x_1 \dots x_i x_{i+1} x_i \dots x_n = x_1 \dots x_i x_{i+1} x_i \dots (x_j x_{n+1}) x_{j+1} \dots x_n = x_{1\varrho} \dots x_{(n+1)\varrho}$$

where $\varrho = \pi \cdot (n+1\; n \dots j+1)$, and x_{n+1} occurs on the right side. Furthermore, if $i+1 \notin \{1, \dots, m\}$ then

$$x_1 \dots x_i x_{i+1} x_i \dots x_{n+2} = x_1 \dots x_i x_{i+3} x_i x_{i+2} x_{i+3} \dots x_{n+2}$$

and by means of the substitution $x_{i-1} \mapsto x_{i-1} x_i$, $x_i \mapsto x_{i+3}$, $x_{i+1} \mapsto x_i x_{i+2}$, $x_{i+t} \mapsto \mapsto x_{i+t+2}$ $(2 \leqq t \leqq n)$ we can bring about that x_{i+2} did not figure on the right side which is the previous case.

Now if $x_{k\pi} \notin X(u)$, $k \leqq m$ then (4.2) implies

$$x_1 \dots x_m = x_1 \dots x_{k-1}(x_k x_{k'}) \dots x_m$$

and every term is equal to one of length $\leqq m$ in the variety $V = SG(u = x_{1\pi} \dots x_{m\pi})$ whence V is h.f.b.

Now let (4.2) be homotypical. Next we show that (4.2) implies either

$$x_1 \dots x_k x_{k+1} x_k \dots x_l = x_1 \dots x_l \tag{4.3}$$

for some $k \geqq i$, $l \geqq n$ or the dual of (4.3) — the latter if $\pi = (i\, i+1)$. In this case, as well as if $\pi = \iota$ (identical), the assertion is obvious. In the opposite case there is an $r \leqq n$, $r \notin \{i, i+1\}$, $r\pi \neq r$. Let e.g. $r < i$ and minimal. Then

$$\begin{aligned} x_0 \dots x_n &= x_0 \dots x_{r-1} x_{r\pi^{-1}} \dots x_{i\pi^{-1}} x_{(i+1)\pi^{-1}} x_{i\pi^{-1}} \dots x_{n\pi^{-1}} = \\ &= x_0 \dots x_{r-2} x_r \dots (x_{r-1} x_{r\pi^{-1}}) \dots x_n . \end{aligned} \tag{4.4}$$

Thus, (4.3) implies a permutative identity

$$x_1 \dots x_{n+2} = x_1 \dots x_{r-1} x_{r\varrho} \dots x_{s\varrho} x_{s+1} \dots x_{n+1}, \quad r\varrho \neq r, \quad s\varrho \neq s,$$

and, according to [7], for sufficiently large l we have

$$x_1 \dots x_l = x_1 \dots x_{r-1} x_{r\sigma} \dots x_{(s+l-n-1)\sigma} x_{s+l-n} \dots x_l$$

for every permutation σ of the symbols $r, \dots, s+l-n-1$ whence, in particular, (4.3) follows.

Using (4.3), an arbitrary word w can be easily transformed to the form $w = w_{(k-1)} w' w^{(l-k-1)}$, $xyx \not\triangleleft w'$, i.e. the irreducible factors of w' are contained in $X \cup T(x^2)$. However, (4.3) implies also

$$\begin{aligned} x_1 \dots x_k x_{k+1}^2 x_{k+2} \dots x_l &= x_1 \dots x_k x_{k+1} x_k x_{k+1} \dots x_l = \\ &= x_1 \dots x_k x_{k+1} x_k x_{k+2} \dots x_l = x_1 \dots x_l \end{aligned}$$

whence $w = w_{(k)} w'' w^{(l-k-1)}$, $w'' \in F_{(1)}$. Thus, $w^* \equiv w_{(k)} w'' w^{(l-k-1)} \in F_{(1)}^{[l-1]} \subseteqq F_{(1)}^{(2l-2)}$, and (i) holds as (4.4) is homotypical. Hence the assertion of the lemma follows by Theorem 3.6 (here $J = F$).

5. Some auxiliary identities. From now on we can suppose, in virtue of Lemma 4.2 and the results of [6], that

$$e(k) = 2 \quad \text{for some} \quad k \leqq m, \quad k\pi^{-1} \neq i. \tag{5.1}$$

We proceed by some identities which follow from $(*)$ and (5.1). Note that

$$(*) \vdash x^{n+2} = x^{n+4} \tag{5.2}$$

as $(*)$ is supposed to be non-balanced. Hence $(x^{2n})v$ is an idempotent in $F(V)$. Moreover, if $(*)$ is homotypical then

$$(5.3)\qquad (*)\vdash x^{n+2}=x^{n+3}$$

and already $(x^{n+2})v$ is idempotent.

Lemma 5.1. *Suppose that* (5.1) *holds. If* (5.3) *holds, too, then*

$$(5.4)\qquad (*)\vdash x^{n+2}y^q z^{n+2}=x^{n+2}yz^{n+2}\quad for\quad q\geqq 1.$$

If $(*)$ *is heterotypical (in particular, if* (5.3) *does not hold) then*

$$(5.5)\quad (*)\vdash x^{n+2}y^{2q+1}z^{n+2}=x^{n+2}yz^{n+2},\quad x^{n+2}y^{2q}z^{n+2}=x^{n+2}z^{n+2}\quad for\quad q\geqq 0.$$

Proof. If (5.3) holds and $(*)$ is heterotypical then [5], Lemma 2 yields even $x^{n+2}yz^{n+2}=x^{n+2}z^{n+2}$. So let $(*)$ be homotypical, and first suppose $\pi\neq\iota$, $\pi\neq(i\,i+1)$. There is a $k\notin\{i,i+1\}$ such that $k\pi\neq k$; let e.g. $k<i$ and choose k to be minimal. Furthermore, there is an $l\neq i$ such that $e(l)=2$, as $(*)$ is non-balanced. Now put $k=s\pi$ and

$$x_t\varphi\equiv\begin{cases}x^{n+2} & \text{if}\quad t<k,\\ y & \text{if}\quad t=k,\\ z^{n+2} & \text{if}\quad t>k;\end{cases}\qquad x_t\psi\equiv\begin{cases}y^{e(s)} & \text{if}\quad t=l\pi,\\ z^{n+2} & \text{else};\end{cases}$$

$$x_t\varphi'\equiv\begin{cases}y^2 & \text{if}\quad t=k,\\ x_t\varphi & \text{else.}\end{cases}$$

We have in virtue of $(*)$

$$\begin{aligned}x^{n+2}yz^{n+2}&=x^{n+2}\cdot u\varphi\cdot z^{n+2}=x^{n+2}\cdot v\varphi\cdot z^{n+2}=\\&=x^{n+2}z^{n+2}y^{e(s)}z^{n+2}=x^{n+2}z^{n+2}\cdot u\psi\cdot z^{n+2}=\\&=x^{n+2}z^{n+2}\cdot v\psi\cdot z^{n+2}=x^{n+2}z^{n+2}y^{2e(s)}z^{n+2}=\\&=x^{n+2}\cdot v\varphi'\cdot z^{n+2}=x^{n+2}\cdot u\varphi'\cdot z^{n+2}=x^{n+2}y^2z^{n+2},\end{aligned}$$

which implies (5.4). If, on the other hand, $\pi=\iota$, then the substitution of

$$x_t\chi\equiv\begin{cases}x^{n+2} & \text{if}\quad t<l,\\ y & \text{if}\quad t=l,\\ z^{n+2} & \text{if}\quad t>l,\end{cases}$$

in $(*)$ yields (5.4) immediately.

If $(*)$ is heterotypical, we can confine ourselves, by the remark made above, to the case where (5.3) does not hold. According to [5], Lemma 2, it suffices to prove $x^{2n}y^{2n}x^{2n}=x^{2n}$. However, in our case there is a $k<m$ with $e(k)=2$, $k\pi>n$. The substitution

$$x_t\vartheta \equiv \begin{cases} y^n & \text{if } t = k\pi, \\ x^{2n} & \text{else} \end{cases}$$

in $(*)$ yields the required identity.

Define

$$m_1 = \min\{j\colon j\pi \neq j\}, \quad m_2 = \min\{j\colon e(j) = 2\};$$

if $m_1 > \min(m, n) \neq \max(m, n)$, we put $\pi = (m+1 \;\; m+2)$, $m_1 = m+1$, and if $m_1 > \max(m, n)$, let $\pi = \iota$, $m_1 = \infty$.

Lemma 5.2. *If* $(*) \vdash x^{n+2} = x^{n+3}$ *and either* $m_1 < m_2$ *or* $m_2 \notin \{i, i+1\}$ *or* $m_1 = m_2 = i+1$ *then*

(5.6) $$(*) \vdash x_1 \dots x_{n-1} y^{n+2} = x_1 \dots x_{n-2} x_{n-1}^2 y^{n+2}.$$

Proof. First consider the case $m_1 < m_2$. Choose $\varphi, \psi \in \operatorname{End} F$ such that

$$x_t\varphi \equiv \begin{cases} x_t & \text{if } t < m_1 \\ x_{m_1} & \text{if } t = m_1\pi, \\ y^{n+2} & \text{else;} \end{cases} \quad x_t\psi \equiv \begin{cases} x_{m_1}^2 & \text{if } t = m_1\pi, \\ x_t\varphi & \text{else.} \end{cases}$$

In virtue of $(*)$ and Lemma 5.1 we have

$$x_1 \dots x_{m_1} y^{n+2} = v\varphi \cdot y^{n+2} = u\varphi \cdot y^{n+2} = x_1 \dots x_{m_1-1} (y^{n+2} x_{m_1})^{\varepsilon} y^{n+2} =$$
$$= x_1 \dots x_{m_1-1} (y^{n+2} x_{m_1}^2) y^{n+2} = u\psi \cdot y^{n+2} = v\psi \cdot y^{n+2} = x_1 \dots x_{m_1-1} x_{m_1}^2 y^{n+2}$$

$$\left(\varepsilon = \begin{cases} 2 & \text{if } m_1\pi = i, \\ 0 & \text{if } m_1\pi > n, \\ 1 & \text{else} \end{cases} \right).$$

Hence (5.6) follows.

Next let $m_2 \leqq \min(i-1, m_1)$, and put

$$x_t\varphi \equiv \begin{cases} x_t & \text{if } t \leqq m_2, \\ y^{n+2} & \text{if } t > m_2. \end{cases}$$

Then

$$x_1 \dots x_{m_2} y^{n+2} = u\varphi \cdot y^{n+2} =$$
$$= v\varphi \cdot y^{n+2} = \begin{cases} x_1 \dots x_{m_2-1} x_{m_2}^2 y^{n+2} & \text{if } m_2 < m_1, \\ x_1 \dots x_{m_2-1} y^{n+1} x_{m_2}^{e(s)} y^{n+2} & \text{if } m_2 = m_1 = s\pi. \end{cases}$$

In the second case we define $\psi \in \operatorname{End} F$ by

$$x_t\psi \equiv \begin{cases} x_{m_2}^2 & \text{if } t = m_2 \\ x_t & \text{else} \end{cases}$$

and obtain

$$x_1 \dots x_{m_2-1} y^{n+2} x_{m_2}^{e(s)} y^{n+2} = x_1 \dots x_{m_2-1} y^{n+2} x_{m_2}^{2e(s)} y^{n+2} =$$
$$= v\psi \cdot y^{n+2} = u\psi \cdot y^{n+2} = x_1 \dots x_{m_2-1} x_{m_2}^2 y^{n+2}.$$

In both cases (5.6) follows.

If $i+1 < m_2 \leqq m_1$, we get, by obvious substitutions in $(*)$,

$$x_1 \dots x_{i+1} y^{n+2} = x_1 \dots x_i x_{i+1} x_i y^{n+2} = x_1 \dots x_i x_{i+1} x_i x_{i+1} y^{n+2} = \dots$$
$$\dots = x_1 \dots x_i x_{i+1} x_i x_{i+1}^{n+2} y^{n+2} = x_1 \dots x_i x_{i+1}^{n+2} y^{n+2} = x_1 \dots x_i x_{i+1}^2 y^{n+2}.$$

Finally, if $m_1 = m_2 = i+1$, put

$$x_t\varphi \equiv \begin{cases} x_t & \text{if} \quad t \leqq i, \\ y^{n+2} & \text{if} \quad t > i; \end{cases} \quad x_t\psi \equiv \begin{cases} x_t\varphi & \text{if} \quad t \leqq i+1, \\ x_i^{n+2} & \text{if} \quad t > i+1; \end{cases} \quad x_t\chi \equiv \begin{cases} x_i^{n+2} & \text{if} \quad t \leqq i, \\ y^{n+2} & \text{if} \quad t > i. \end{cases}$$

Applying $(*)$ and Lemma 5.1, we obtain

$$x_1 \dots x_i y^{n+2} = v\varphi \cdot y^{n+2} = u\varphi \cdot y^{n+2} = x_1 \dots x_i y^{n+2} x_i y^{n+2} =$$
$$= x_1 \dots x_i y^{n+2} x_i^{n+2} y^{n+2} = u\psi \cdot x_i^{n+2} y^{n+2} = v\psi \cdot x_i^{n+2} y^{n+2} = x_1 \dots x_{i-1} (x_i^{n+2} y^{n+2})^2 =$$
$$= x_1 \dots x_{i-1} \cdot u\chi \cdot y^{n+2} = x_1 \dots x_{i-1} \cdot v\chi \cdot y^{n+2} = x_1 \dots x_{i-1} x_i^{n+2} y^{n+2} = x_1 \dots x_{i-1} x_i^2 y^{n+2}.$$

This completes the proof.

Lemma 5.3. *If $(*)$ is heterotypical and either $m_1 \leqq m_2$ or $m_2 \neq i$, then*

(5.7) $$(*) \vdash x_1 \dots x_{n-1} y^{n+2} = x_1 \dots x_{n-1} x_n^2 y^{n+2}.$$

Proof. If $m_1 \leqq m_2$ then set

$$x_t\varphi \equiv \begin{cases} x_t & \text{if} \quad t < m_1, \\ y^{2n} & \text{if} \quad t \geqq m_1, \end{cases} \quad x_t\psi \equiv \begin{cases} x_{m_1}^2 & \text{if} \quad t = m_1\pi, \\ x_t\varphi & \text{else.} \end{cases}$$

By $(*)$ and Lemma 5.1, we have (taking in account that $e(m_1) \neq 0$ as $m_1 \leqq m_2 \leqq m$)

$$x_1 \dots x_{m_1-1} y^{n+2} = v\varphi \cdot y^{n+2} = u\varphi \cdot y^{n+2} = u\psi \cdot y^{2n} x_{m_1}^{2/e(m_1)} y^{n+2} =$$
$$= v\psi \cdot y^{n+2} = x_1 \dots x_{m_1-1} x_{m_1}^2 y^{n+2},$$

which implies (5.7).

If $i \neq m_2 < m_1$ then $(*) \vdash x^{n+1} = x^{n+2}$ and in consequence of Lemma 5.2 and Lemma 5.1 we have even

$$x_1 \dots x_{n-1} y^{n+1} = x_1 \dots x_{n-2} x_{n-1}^2 y^{n+1} = x_1 \dots x_{n-2} x_{n-1}^{n+1} y^{n+1} =$$
$$= x_1 \dots x_{n-2} x_{n-1}^{n+1} x_n^{n+1} y^{n+1} = x_1 \dots x_{n-1} x_n^{n+1} y^{n+1} = x_1 \dots x_n y^{n+1}.$$

Clearly, both (5.6) and (5.7) imply

(5.8) $$x_1 \dots x_{n-1} y^{n+2} = x_1 \dots x_{n-2} x_{n-1}^3 y^{n+2}.$$

Furthermore, it is easy to see that

(5.9) $\quad (5.6) \vdash x_1 \dots x_n y^{n+2} = x_1 \dots x_{n-2} x_{n-1}^2 x_n y^{n+2} = x_1 \dots x_{n-2} x_{n-1}^{n+2} x_n y^{n+2},$

(5.10) $\quad (5.7) \vdash x_1 \dots x_n y^{n+2} = x_1 \dots x_{n-1} x_{n+1}^2 x_n y^{n+2},$

(5.11) $\quad (5.8) \vdash x_1 \dots x_n y^{n+2} = x_1 \dots x_{n-2} x_{n-1}^3 x_n y^{n+2} = x_1 \dots x_{n-2} x_{n-1}^{2n+1} x_n y^{n+2},$

(5.12) $\quad (5.6) \wedge (5.7) \vdash x_1 \dots x_n y^{n+2} = x_1 \dots x_{n-1} y^{n+2} = x_1 \dots x_{n-2} x_n y^{n+2}.$

Remark. The only cases when neither the conditions of the Lemmas 5.2, 5.3, nor those of their duals are fulfilled, are given by $(**)$ and

(5.13) $$v \equiv x_1 \dots x_{i-1} x_i^2 x_{i+1} \dots x_n.$$

Lemma 5.4. $(*) \vdash (x^{2n} y^{2n})^2 = x^{2n} y^{2n}$.

Proof. If $(*)$ is heterotypical the assertion follows from Lemma 5.1. So let $(*)$ be homotypical. We indicate the substitutions in $(*)$ which yield the required identity.

If $\pi = \iota$, substitute

$$x_t \equiv \begin{cases} x^{2n} & \text{if } t \leqq i, \\ y^{2n} & \text{if } t > i. \end{cases}$$

If $k\pi \neq k$ for some $k \notin \{i, i+1\}$ (suppose e.g. $k < i$), choose k to be minimal and set

$$x_t \varphi \equiv \begin{cases} x^{2n} & \text{if } t \leqq k, \\ y^{2n} & \text{if } t > k. \end{cases}$$

The remaining case $\pi = (i \ i+1)$ is dual to $\pi = \iota$.

Lemma 5.5. *If* $\pi \neq \iota$, $\pi \neq (i \ i+1)$ *then*

$$(*) \vdash x_1^{n+2} yz x_2^{n+2} = x_1^{n+2} zy x_2^{n+2}.$$

Proof. If $(*)$ is heterotypical and $(*) \vdash x^{n+2} = x^{n+3}$ then $x_1^{n+2} yz x_2^{n+2} = x_1^{n+2} x_2^{n+2} = x_1^{n+2} zy x_2^{n+2}$. If ($(*)$ is heterotypical and) $(*) \vdash x^{n+1} = x^{n+3}$ then, by (5.10),

$$x_1^{n+2} yz x_2^{n+2} = x_1^{n+2} (yz)^{2n+1} x_2^{n+2} = x_1^{n+2} z^{2n} y^{2n} (yz)^{2n+1} x_2^{n+2} =$$
$$= x_1^{n+2} z^{2n} y^{2n+1} z x_2^{n+2} = x_1^{n+2} z^{2n} y^{2n+1} z^{2n+1} x_2^{n+2}.$$

Put

$$x_t \varphi \equiv \begin{cases} z & \text{if } t = i, \\ y^{2n+1} & \text{if } t = i+1, \\ z^{2n} & \text{else.} \end{cases}$$

Then

$$x_1^{n+2} z^{2n} y^{2n+1} z^{2n+1} x_2^{n+2} = x_1^{n+2} z^{2n+1} \cdot u\varphi \cdot z^{2n} x_2^{n+2} =$$
$$= x_1^{n+2} z^{2n+1} \cdot v\varphi \cdot z^{2n} x_2^{n+2} = x_1^{n+2} z^{2n+1} y^{2n+1} z^{2n} x_2^{n+2}$$

and, by symmetry, $x_1^{n+2} z^{2n+1} y^{2n+1} z^{2n} x_2^{n+2} = x_1^{n+2} zy x_2^{n+2}$.

If $(*)$ is homotypical then $k\pi \neq k$ for some $k \notin \{i, i+1\}$; say, $k<i$. Set

$$x_t\varphi \equiv \begin{cases} x_1^{n+2} & \text{if } t < m_1-1, \\ y & \text{if } t = m_1-1, \\ z & \text{if } t = m_1, \\ x_2^{n+2} & \text{if } t > m_1; \end{cases} \qquad x_t\psi \equiv \begin{cases} x_1^{n+2} & \text{if } t < m_1, \\ yx_2^{n+2} & \text{if } t = m_1, \\ zx_2^{n+2} & \text{if } t = m_1\pi, \\ x_2^{n+2} & \text{else.} \end{cases}$$

We obtain (using also (5.4) and Lemma 5.4 if $m_1\pi = i$)

$$x_1^{n+2}yzx_2^{n+2} = x_1^{n+2}\cdot u\varphi \cdot x_2^{n+2} = x_1^{n+2}\cdot v\varphi \cdot x_2^{n+2} =$$

$$= x_1^{n+2}yx_2^{n+2}z^{e(s)}x_2^{n+2} = x_1^{n+2}yx_2^{n+2}(zx_2^{n+2})^{\varepsilon} =$$

$$= x_1^{n+2}\cdot u\psi \cdot x_2^{n+2} = x_1^{n+2}\cdot v\psi \cdot x_2^{n+2} = x_1^{n+2}(zx_2^{n+2})^{e(m_1)}(yx_2^{n+2})^{e(s)} = x_1^{n+2}zx_2^{n+2}yx_2^{n+2},$$

where $s\pi = m_1$ and

$$\varepsilon = \begin{cases} 2 & \text{if } m_1\pi = i, \\ 1 & \text{else.} \end{cases}$$

By symmetry, $x_1^{n+2}zx_2^{n+2}yx_2^{n+2} = x_1^{n+2}zyx_2^{n+2}$.

Corollary 5.6. *Either* $(*) \vdash x_1^{n+2}yzyx_2^{n+2} = x_1^{n+2}y^2zx_2^{n+2}$ *or* $(*) \vdash x_1^{n+2}yzyx_2^{n+2} = x_1^{n+2}zy^2x_2^{n+2}$.

Proof. If $\pi \neq \iota$, $\pi \neq (i\, i+1)$ then both identities hold by Lemma 4.8. If $\pi = \iota$ then $x_1^{n+2}yzyx_2^{n+2} = x_1^{n+2}y^{e(i)}zx_2^{n+2} = x_1^{n+2}y^2zx_2^{n+2}$ by Lemma 5.1. The case $\pi = (i\, i+1)$ is dual.

(5.9), (5.10) and Corollary 5.6 imply

Corollary 5.7. *If either the assumptions of Lemma 5.2 or those of Lemma 5.3 are fulfilled then either*

(5.14) $$(*) \vdash x_1 \dots x_{n-1}ztzx_ny^{n+2} = x_1 \dots x_{n-1}z^2tx_ny^{n+2}$$

or

(5.14′) $$(*) \vdash x_1 \dots x_{n-1}ztzx_ny^{n+2} = x_1 \dots x_{n-1}tz^2x_ny^{n+2}.$$

Furthermore, applying (5.9), (5.10), (5.14), (5.14′), we obtain

Corollary 5.8. *If either the assumptions of Lemma 5.2 or those of Lemma 5.3 are fulfilled then*

(5.15) $$(*) \vdash wy^{n+2} = w_{(n)}x_{c(1)} \dots x_{c(l)}y^{n+2},$$

$$c(j) \neq c(k) \quad \text{if} \quad j \neq k, \quad \{x_{c(1)}, \dots, x_{c(l)}\} \subseteq X(w)$$

for every $w \in F^n$.

6. Standard forms. Now we are able to construct standard forms for V in the V-ideal J defined by

$$J=\{w\colon \text{there are arbitrarily long terms which equal to } w \text{ in } V\},$$

and for $V(J)$. Although the considerations below could be performed in the same generality as till now, some special cases, in particular the one where $(*)$ is homotypical and $e(k)=2$ only if $k=(i+1)\pi^{-1}$, would demand a separate consideration. Therefore we continue the investigation of $(*)$ accepting in what follows the further restriction

(T) $e(k)=2$ for at least two different values of k.

This suffices for the proof of Theorem A, since the case when $e(k)=2$ for exactly one k has been settled in [6].

Lemma 6.1. *If $(*)$ is homotypical,* (T) *holds, and $|w_j|\geqq n^2-n$ for $j=1,2,3$ then $w\equiv w_1w_2^2w_3\in J$.*

Proof. There is a k such that $e(k)=2$, $k\pi\neq i$. let e.g. $k\pi>i$. First we show that if $|u_j|\geqq n$ for $j=1,2,3$ then there exist $v_1, v_2, v_3\in F$ such that

$$\begin{gathered} u_0\equiv u_1u_2^2u_3=v_1v_2^2v_3\equiv v_0,\quad u_2\equiv u_2'v_2, \\ |v_0|_s>|u_0|_s \quad \text{for} \quad x_s\in X(v_2),\quad |v_j|\geqq|u_j|-n+2 \quad \text{for} \quad j=1,2,3. \end{gathered} \tag{6.1}$$

Indeed, put $u_1\equiv u_1'x_{c(1)}\dots x_{c(i-1)}$, $u_2\equiv x_{c(i)}x_{c(i+1)}\dots x_{c(k\pi)}\bar{u}$, $u_3\equiv x_{c(k\pi+1)}\dots x_{c(n)}u_3'$. Then

$$\begin{gathered} u_0\equiv u_1'x_{c(1)}\dots x_{c(i)}(x_{c(i+1)}\dots x_{c(k\pi)}\bar{u})x_{c(i)}x_{c(i+1)}\dots \\ \dots x_{c(k\pi-1)}(x_{c(k\pi)}\bar{u})x_{c(k\pi+1)}\dots x_{c(n)}u_3'=u_1'u_1''(x_{c(k\pi)}\bar{u})^2u_3''u_3' \end{gathered} \tag{$*$}$$

with some $u_1'', u_3''\in F^0$, and $v_1\equiv u_1'u_1''$, $v_2\equiv x_{c(k\pi)}$, $v_3\equiv u_3''u_3'$ meet all requirements of (6.1).

If w is as stated then (6.1) can be applied n times. The term $w=\bar{w}_1\bar{w}_2^2\bar{w}_3$ thus obtained contains every variable of $\bar{w}_2$ at least $n+1$ times. Now suppose some $\tilde{w}\in F$ contains a letter x_s at least $n+1$ times. Then $\tilde{w}$ is of the form $\tilde{w}\equiv u_0\prod_{j=1}^{n+1}x_su_j$ where $u_j\in F^0$ for $j=0,\dots,n+1$. Put

$$x_t\varphi\equiv\begin{cases} u_{t-1}x_s & \text{if} \quad t<i,\\ x_s & \text{if} \quad t=i,\\ u_ix_su_{i+1} & \text{if} \quad t=i+1,\\ x_su_t & \text{if} \quad t>i+1.\end{cases}$$

Then $\tilde{w}\equiv u\varphi$, and $|v\varphi|>|\tilde{w}|$, $|v\varphi|_s>|w|_s$, i.e. we can obtain from $\tilde{w}$ a longer word of the same form, and therefore $\tilde{w}\in J$. The same holds, then, for $\bar{w}$ and hence also for w.

Lemma 6.2. *Suppose* (T) *holds. If* $(*)$ *is heterotypical then*

$$J = \{w\colon\ u \lhd w \ \text{or}\ v \lhd w\}. \tag{6.2}$$

If $(*)$ *is homotypical and* $e(k)=2$ *for some* $k \notin \{i\pi^{-1}, (i+1)\pi^{-1}\}$ *then* J *contains the subset*

$$L = \{w\colon\ w \equiv w_{(2n^2-n)}\hat{w}w^{(2n^2-n)},\ u \lhd \hat{w}\}.$$

If $(*)$ *is homotypical,* $e(k)=2$ *iff* $k\pi \in \{i, i+1\}$, *but* v *is not of the form* (4.1), *then* J *contains the subset*

$$L' = \{w\colon\ w \equiv w_{(n^2+n)}\hat{w}w^{(n^2+n)},\ w_i \notin T(xyx) \cup T(x^2) \cup X$$

$$\text{for some irreducible factor } w_i \text{ of } w\} \cup$$

$$\cup \{w\colon\ w \equiv w'x_c x_d x_c w'' x_r x_s x_r w'''; \ |w'|, |w'''| \geqq n^2+2n,\ |w''| \geqq n-2\}.$$

Proof. The first assertion is trivial. If $(*)$ is homotypical, $e(k)=2$, $k\pi \notin \{i, i+1\}$, say, $k\pi > i+1$, and $w \in L$ then $w \equiv w_{(2n^2-n)}w' \cdot u\varphi \cdot w''w^{(2n^2-n)}$ with some $\varphi \in \operatorname{End} F$, and we can modify the mapping φ in such a way that $x_t\varphi' \equiv x_t\varphi$ if $t < k\pi$, $|x_{k\pi}\varphi'| = n^2$, $|x_t\varphi'| = 1$ if $t > k\pi$, and $w \equiv w_{(2n^2-n)}w' \cdot u\varphi' \cdot w'''w^{(n^2-n)}$. However, then

$$w = w_{(2n^2-n)}w' \cdot v\varphi' \cdot w''' w^{(n^2-n)} \equiv$$

$$\equiv w_{(2n^2-n)}w'(x_{1\pi}^{e(1)} \dots x_{(k-1)\pi}^{e(k-1)})\varphi' \cdot (x_{k\pi}\varphi')^2 \cdot (x_{(k+1)\pi}^{e(k+1)} \dots x_{n\pi}^{e(n)})\varphi' w''' w^{(n^2-n)},$$

and the assumptions of Lemma 6.1 are fulfilled.

Now let $k\pi = i$, $k'\pi = i+1$, $e(k)=e(k')=2$, $e(j) \leqq 1$ if $j \neq k, k'$. Suppose first that w is contained in L_1', the first component of L'.

a) If $w \equiv w_{(n^2-n)}\tilde{w}w^{(n^2-n)}$, $|\tilde{w}|_c > 2$ for some $c \in \mathbf{P}$ (in particular, if $|\hat{w}|_c > 2$), then n consecutive applications of $(*)$ with substituting each time $\varphi_j\colon x_i \mapsto x_c$, $\varphi_j\colon x_{i+1} \mapsto b_j$, $|b_j|_c > 0$ gives us a word w^* with $|w^*|_c > n+1$, and the second part of the proof of Lemma 6.1 verifies the assertion.

b) If $w \equiv w_{(n^2)}\tilde{w}w^{(n^2)}$, $xyxy \lhd \tilde{w}$ (in particular, if $xyxy \lhd \hat{w}$), then $w \equiv$ $\equiv w'x_c a x_c a w''$, and choosing $\varphi_2 \in \operatorname{End} F$ such that $x_i\varphi \equiv a$, $x_{i+1}\varphi \equiv x_c$, $w\varphi \equiv$ $\equiv w_{(n^2-n)}\bar{w} \cdot u\varphi \cdot \bar{\bar{w}}w^{(n^2-n)}$, we have $|\bar{w} \cdot v\varphi \cdot \bar{\bar{w}}|_c > 2$, and this case can be reduced to a).

c) If $xyzx \lhd \hat{w}$, then $w \equiv w'x_r b x_r w''$, $|b| \geqq 2$. Putting $x_i\varphi \equiv x_r$, $x_{i+1}\varphi \equiv b$, $w \equiv \bar{w} \cdot u\varphi \cdot \bar{\bar{w}}$ with $|\bar{w}|$, $|\bar{\bar{w}}| \geqq n^2$, we have $(*) \vdash \bar{w} \cdot v\varphi \cdot \bar{\bar{w}}$, which gives us case b) as b^2 is a subword of $v\varphi$.

It is easy to see that all possibilities are exhausted by a)—c). Finally, let $w \in L_2'$. By assumption, $\pi \neq \iota$, $\pi \neq (i\ i+1)$, whence there is an $l \neq i$, $i+1$ such that $l\pi \neq l$; let e.g. $l > i+1$ and maximal (then, clearly, $l\pi < l$). Set $w \equiv w_1 \cdot u\psi \cdot w_2 \cdot u\chi \cdot w_3$,

$|w_1|$, $|w_3| \geqq n^2+n$, $x_i\psi \equiv x_c$, $x_{i+1}\psi \equiv x_d$, $x_i\chi \equiv x_r$, $x_{i+1}\chi \equiv x_s$, and

$$x_t\vartheta \equiv \begin{cases} x_t\psi & \text{if } t<l, \\ (x_l \dots x_n)\psi \cdot w_2 \cdot (x_1 \dots x_{i+1})\chi & \text{if } t=l, \\ (x_i x_{i+2} \dots x_{i+1})\chi & \text{if } t=l+1, \\ x_t\chi & \text{if } t>l+1. \end{cases}$$

We have

$$w \equiv w_1 \cdot u\vartheta \cdot w_3 = w_1 \cdot v\vartheta \cdot w_3 \equiv ax_r bx_r a' \in L_1',$$

because $|a| \geqq |w_1| \geqq n^2+n$, $|a'| \geqq |w_3| \geqq n^2+n$, $|b| \geqq |x_s \cdot x_{(l\pi^{-1}+1)\pi}\vartheta| \geqq 2$. This completes the proof.

Lemma 6.2 and Proposition 3.10 immediately yield.

Proposition 6.3. *If (T) holds and v is not of the form (**) then SG(J) is h.f.b.*

Proof. Set $\mathrm{T} = \bigcup_{l=0}^{n-1} T(x_1^2 \dots x_l^2)$, and let $I(\mathrm{T})$ be the set of all $w \in F^0$ every semiirreducible factor of which is contained in T. Put

(6.3$_1$) $$M_1 = \{w\colon w_{(n)}\hat{w}w^{(n)},\ \hat{w} \in I(\mathrm{T})\} \cup \{w\colon |w| < 2n\},$$

(6.3$_2$) $$M_2 = \{w\colon w_{(2n^2)}\hat{w}w^{(2n^2)},\ \hat{w} \in I(\mathrm{T})\} \cup \{w\colon |w| < 4n^2\},$$

(6.3$_3$) $$M_3 = \{w\colon w_{(n^2+n)}\bar{w}\tilde{w}\bar{w}w^{(n^2+n)},\ |\bar{w}| \leqq n,\ \hat{w} \equiv \bar{w}y\bar{w} \in I(\mathrm{T})(y \notin X(\bar{w}\bar{w}))\} \cup \{w\colon |w| < 2n^2+2n\}.$$

Lemma 6.2 implies that $F \setminus J \subseteq M_j$ $(j=1, 2, 3)$, if either $(*)$ is heterotypical or $(*)$ is homotypical and $e(k)=2$ for some $k \notin \{i\pi^{-1}, (i+1)\pi^{-1}\}$ or $(*)$ is homotypical, $e(k)=2$ iff $k\pi \in \{i, i+1\}$, and $\pi \neq \iota$, $\pi \neq (i\,i+1)$, respectively. Indeed, if $w \notin M_j$ then w is long enough to be written in the form given in the first bracket of (6.3$_j$) but with $\hat{w}$ having a semiirreducible factor $w_j \notin I(\mathrm{T})$. Then either $x_i x_{i+1} x_i \lhd \hat{w}$ or $x_1^2 \dots x_n^2 \lhd \hat{w}$ and, consequently, if w' is a suffix of length n of $w_{(n)}$, $w_{(2n^2)}$, or $w_{(n^2+n)}$, resp., and, similarly, w'' a prefix of length n of $w^{(n)}$, $w^{(2n^2)}$, or $w^{(n^2+n)}$, we have $u \lhd w'\hat{w}w''$ or $v \lhd w'ww''$ (even $v \lhd \hat{w}$). As the latter case can be reduced to the first one, both imply $w \in J$ by Lemma 6.2. Hence the assertion of the proposition follows by Proposition 3.10, since $M_1 \subseteq F_{(2n)}^{[2n]}$, $M_2 \subseteq F_{(2n)}^{[4n^2]}$, $M_3 \subseteq F_{(2n)}^{[2n^2+2n]}$.

In order to obtain a standard form in J, we prove first

Lemma 6.4. *If (T) holds and $w \in J$ then there is a $\bar{w} \in J$ such that*

$$(*) \vdash w = \bar{w} \equiv w_1 x_c^{n+2} w_2,\quad x_c \in X.$$

Proof. If $(*)$ is heterotypical the assertion is obvious; so let $(*)$ be homotypical. There is a $k \leqq n$ which satisfies $e(k)=2$, $k\pi \neq i+1$. We are going to show that for every triple r, s, l of natural numbers there is an $x_c\in X$ and a term $\bar{w}$ such that $w= =\bar{w}\equiv w_0 \prod_{j=1}^{s} x_c^r w_j$, $|w_j|\geqq l$ for $j=0, \ldots, s$; this is somewhat more than stated. First consider the case $r=1$. Let $|X(w)|=\lambda$. As $w=w'$ implies now $X(w)=X(w')$, we only have to take a sufficiently long word $\bar{w}$, say, $|\bar{w}|>2l+\lambda(s-1)(l+1)$, in order to obtain a factorization of the required form. Now suppose the assertion holds for some $r>0$ and arbitrary s, l. In the same way as above, one can find a $w'=w$ such that the same subword $x_d x_c^r x_f$ occurs in w' a sufficiently large number of times and at a sufficiently large distance from each other (this is necessary in order to cover the cases where $k\pi=i-1$ or $k\pi=i+2$; c, d, f need not be different). Say, $w'\equiv \equiv w_0 \prod_{j=1}^{3s} x_d x_c^r x_f w_j$, $|w_j|\geqq n+l$. One can define endomorphisms $\varphi_1, \ldots, \varphi_s$ such that $x_{k\pi}\varphi_j\equiv x_c^r$ for $j=1, \ldots, s$ and $w'\equiv w_0' \prod_{j=1}^{s} u\varphi_j \cdot w_j'$, $|w_j'|\geqq l$. Applying (∗), we have $w'=w_0' \prod_{j=1}^{s} v_j \cdot w_j' \equiv w_0'' \prod_{j=1}^{s} x_c^{2r} w_j''$ with some w_j'', $|w_j''|\geqq|w_j'|$. This completes the proof.

Proposition 6.5. *If (T) holds and v is not of the form* (4.1) *then* $[V(J), V]$ *is finitely based.*

Proof. Let $w\in J$; we can suppose that $w\equiv w'x_c^{n+2}w''$ by Lemma 6.4. First let the assumptions of both Lemma 5.2 and its dual (or those of Lemma 5.3 and its dual) be fulfilled. In virtue of (5.9) (or (5.11)) and its dual, and by Corollary 5.8, we have

$$w = w_{(n-2)}x_d^{n+2}x_{c(1)}\ldots x_{c(l)}x_f^{n+2}w^{(n-2)} \equiv w^* \tag{6.4}$$

$$\bigl(c(j) \neq c(k) \text{ if } j \neq k\bigr).$$

Thus, $w^*\in F_{(1)}^{[4n]}$, and the assertion follows by Theorem 3.6, because (i) automatically holds if (∗) is homotypical, and if it is not, then, starting from an arbitrary $w'=w$ with a minimal number of variables in $X(w')$, we can transform it to the form (6.4) by steps of the following two types: 1) first, the insertion of the $(n+2)^{\text{nd}}$ power of some variable — however, doing so it is not necessary to introduce new variables, and 2) a sequence of applications of (5.10), (5.11) and (5.14) or (5.14′); besides, (5.10) is always used for reducing the power of the elements, and the other three transformations do not change the set of the variables involved.

For the rest we can suppose, according to the Remark made on p. 321, that the assumptions dual to those of Lemma 5.2 or 5.3 hold, but the assumptions of these lemmata do not, i.e., α) $v\equiv x_1\ldots x_{i-1}x_i^2v'$ if (∗) is heterotypical, and β) $v\equiv x_1\ldots \ldots x_{i-1}x_{i\pi}^2v'$ or γ) $v\equiv x_1\ldots x_i x_{i+1}^2 v'$ if (∗) is homotypical. Let $w\equiv w_{(i-1)}\bar{w}x_{c(0)}^{n+2}x_{c(1)}\ldots \ldots x_{c(l)}w^{(n-2)}$, and write $\bar{w}$ in the form

$$\bar{w} \equiv x_{d(1)}^{\gamma(1)}\ldots x_{d(p)}^{\gamma(p)}, \quad d(i) \neq d(i+1).$$

Suppose that w is chosen in such a way (from the class of all $w'=w$ of the same form), that the vector $\mathbf{v}=\mathbf{v}(w)=(|X(\bar{w})|, p, l)$ is minimal in the lexicographical ordering. We claim that

(6.5) $$X(\bar{w})\cap\{x_{c(0)}, \ldots, x_{c(l-1)}\} = \emptyset.$$

Indeed, let $d(q)=c(r)$, $r<l$, and set

$$w_{(i-1)}x_{d(1)}^{\gamma(1)}\ldots x_{d(q-1)}^{\gamma(q-1)} \equiv w_1, \quad x_{d(q+1)}^{\gamma(q+1)}\ldots x_{d(p)}^{\gamma(p)} \equiv w_2,$$

$$x_{c(1)}\ldots x_{c(r-1)} \equiv w_3, \quad x_{c(r+1)}\ldots x_{c(l)}w^{(n-2)} \equiv w_4.$$

If $m_2=i$, put

$$x_t\varphi \equiv \begin{cases} x_{d(q)}^{\gamma(q)} & \text{if } t=i,\\ w_2x_{c(o)}^{n+2}w_3 & \text{if } t=i+1,\\ x_{d(q)}^{2n} & \text{if } t>i+1,\end{cases}$$

$$(x_1\ldots x_{i-1})\varphi \equiv w_1.$$

We have by the dual of (5.11),

(6.6) $$w = w_1x_{d(q)}^{\gamma(q)}w_2x_{c(o)}^{n+2}w_3x_{d(q)}^{2n+1}w_4 =$$

$$= u\varphi\cdot x_{d(q)}^{2n+1}w_4 = v\varphi\cdot x_{d(q)}w_4 = \begin{cases} w_1x_{d(q)}^{2\gamma(q)}\tilde{w}x_{d(q)}^{2n+1}v_1 & \text{if } i\pi=i,\\ w_1(w_2x_{c(o)}^{n+2}w_3)^2v_2 & \text{if } i\pi=i+1,\\ w_1x_{d(q)}^{2n}v_3 & \text{if } i\pi>i+1\end{cases}$$

with some $\tilde{w}, v_1, v_2, v_3\in F^0$, and in the first case by iteration also

$$w = w_1x_{d(q)}^{2n}v_4.$$

We have a contradiction with the choice of w in all cases.

If $m_2=i+1$, set

$$x_t\varphi' \equiv \begin{cases} x_t\varphi & \text{if } t\leqq i+1,\\ x_{c(r+1)} & \text{if } t>i+1.\end{cases}$$

As in this case $(*)\vdash x^{n+2}=x^{n+3}$, we can make use of the dual of (5.9). Hence

$$\begin{aligned} w &= w_1x_{d(q)}^{\gamma(q)}w_2x_{c(o)}^{n+2}w_3x_{d(q)}^{\gamma(q)}x_{c(r+1)}^{n+2}x_{c(r+2)}\ldots x_{c(l)}w^{(n-2)} =\\ &= u\varphi\cdot x_{c(r+1)}^{n+2}x_{c(r+2)}\ldots x_{c(l)}w^{(n-2)} =\\ &= v\varphi\cdot x_{c(r+1)}^{n+2}x_{c(r+2)}\ldots x_{c(l)}w^{(n-2)} =\\ &= w_1x_{d(q)}^{\gamma(q)}(w_2x_{c(o)}^{n+2}w_3)^2x_{c(r+1)}^{n+2}x_{c(r+2)}\ldots x_{c(l)}w^{(n-2)} =\\ &= w_1x_{d(q)}^{\gamma(q)}\cdot w_2x_{c(o)}^{n+2}\cdot x_{c(o)}^{n+2}w_3\cdot w_2x_{c(o)}^{n+2}\cdot w_3^{n+2}x_{c(r+1)}\ldots x_{c(l)}w^{(n-2)} =\\ &= w_1x_{d(q)}^{\gamma(q)}w_2x_{c(o)}^{n+2}\cdot(x_{c(o)}^{n+2}w_3)^2w_3^{n+2}x_{c(r+1)}\ldots x_{c(l)}w^{(n-2)} =\\ &= w_{(i-1)}\bar{w}x_{c(o)}^{n+2}w_3x_{c(r+1)}\ldots x_{c(l)}w^{(n-2)} =\\ &= w_{(i-1)}\bar{w}x_{c(o)}^{n+2}x_{c(1)}\ldots x_{c(r-1)}x_{c(r+1)}\ldots x_{c(l)}w^{(n-2)}, \end{aligned} \tag{6.7}$$

if $r>0$ and

$$(6.8)\qquad w\equiv w_1x_{d(q)}^{\gamma(q)}w_2x_{d(q)}^{n+2}w_4=w_1x_{d(q)}^{\gamma(q)}w_2^2x_{d(q)}^{n+2}w_4=\ldots=w_1x_{d(q)}^{\gamma(q)}w_2^{n+2}x_{d(q)}^{n+2}w_4$$

if $r=0$. In the first case we have reduced l by 1; in the second, $w_1x_{d(q)}^{\gamma(q)}w_2^{n+2}\in J$ and we can create the $(n+2)^{\text{nd}}$ power of a variable in this part of the word by Lemma 5.10. This proves (6.5).

Furthermore, $w_{(i-1)}\bar{w}\notin J$ by the same lemma and (6.5). Let $w_{(l-1)}\bar{w}$ be the longest one of all words it equals to. Then $u\not\lhd w_{(l-1)}\bar{w}$ (else we could replace its subword of the form $u\psi$ by the longer word $v\psi$), and $x_1^2\ldots x_m^2x_{m+1}\ldots x_{m+n-i-1}\not\lhd w_{(l-1)}\bar{w}$. Indeed, if $e(k)=2$, $k\pi>i+1$ for some k then let

$$x_j\varphi\equiv w_j\equiv y_j\bar{w}_jz_j,\quad x_j\psi\equiv w_j'\equiv\begin{cases}w_j & \text{for } j<k\pi,\\ w_{k\pi}y_{k\pi+1} & \text{for } j=k\pi,\\ \bar{w}_jz_jy_{j+1} & \text{for } j>k\pi\end{cases}$$

($y_j\equiv z_j$ if $|w_j|=1$). We have even

$$v\varphi\cdot y_{m+1}\equiv\Big(\prod_{j=1}^{m}w_{j\pi}^{e(j)}\Big)y_{m+1}=u\varphi\cdot y_{m+1}\equiv w_1\ldots w_iw_{i+1}w_i\ldots w_ny_{m+1}\equiv$$

$$\equiv w_1'\ldots w_i'w_{i+1}'w_i'\ldots w_n'\equiv u\psi=v\psi\equiv w_{1\pi}'^{e(1)}\ldots w_{m\pi}'^{e(m)},$$

and $|v\psi|=|v\varphi|+2>|v\varphi\cdot y_{m+1}|$. If, on the other hand, $e(k)=2$ iff $k\pi\in\{i,i+1\}$ (this occurs only in case β) with $i\pi\in\{i,i+1\}$), then $\pi\neq\iota$, $\pi\neq(i\,i+1)$, whence $l\pi+1\neq(l+1)\pi$ for some $l\pi>i+1$. Put

$$x_t\psi\equiv\begin{cases}w_t & \text{if } t\in\{i,\,i+1,\,l\pi\},\\ w_{l\pi}w_{l\pi+1}^2 & \text{if } t=l\pi+1,\\ w_t^2 & \text{else.}\end{cases}$$

We have

$$w_{1\pi}^2\ldots w_{n\pi}^2x_1\ldots x_{n-i-1}=w_1^2\ldots w_{i-1}^2w_iw_{i+1}w_iw_{i+2}^2\ldots w_n^2x_1\ldots x_{n-i-1}\equiv$$

$$\equiv u\psi\cdot x_1\ldots x_{n-i-1}=v\psi\cdot x_1\ldots x_{n-i-1}\equiv w_{1\pi}^2\ldots w_{l\pi}\tilde{w}w_{l\pi}\ldots w_{n\pi}^2x_1\ldots x_{n-i-1}.$$

Applying (∗) to this latter word, we obtain some word w^* which contains $\tilde{w}^2$ and all factors w_t^2 which do not enter $\tilde{w}$, as well as $x_1,\ldots,x_{n-i-1}$. Hence $|w^*|>|w_{1\pi}^2\ldots$ $\ldots w_{n\pi}^2x_1\ldots x_{n-i-1}|$.

As in the proof of Lemma 4.14, we can conclude now that

$$(6.9)\qquad \begin{aligned}&\bar{w}\equiv\hat{w}\bar{w}^{(n-i-1)},\quad \hat{w}=!\,w_0\prod_{j=1}^{s}x_{f(j)}w_j,\quad w_j\in\bigcup_{t=0}^{m-1}T(x_1^2\ldots x_t^2),\\ &w^*\equiv w_{(l-1)}\overline{w}w^{(n-1)},\quad \overline{w}=!\,\bar{w}x_{c(o)}^{n+\delta}x_{c(1)}\ldots x_{c(l-1)}\quad(\delta=1\text{ or }2).\end{aligned}$$

Let M be the set of all words of the same form as w^*:

$$M_1 = \{w_1\colon |w_1| = i-1\},$$

$$M_2 = \Big\{\hat{w}\colon \hat{w} =!\, w_0 \prod_{j=1}^{s} x_{f(j)} w_j,\quad w_j \in \bigcup_{t=0}^{m-1} T(x_1^2 \dots x_t^2)\Big\},$$

$$M_3 = \{w_3\colon |w_3| = n-i-1\},\quad M_4 = T(x^{n+2}) \cup T(x^{n+1}),$$

$$M_5 = F_{(1)},\quad M_6 = \{w_6\colon |w_6| = n-1\},$$

$$M = \big\{w_1 \dots w_6\colon w_i \in M_i,\ X(w_i) \cap X(w_j) = \emptyset \text{ if } i,j \in \{2,4,5\},\ i \neq j\big\}.$$

We have seen that M is a standard form for V in J. Thus, by Theorem 2.9 and Lemma 3.5, the proof will be accomplished if we show that conditions (i) of Lemma 2.8 and (iii) of Theorem 2.9 are fulfilled. Now (i) holds — if $(*)$ is homotypical, by Remark 1 made after Corollary 2.10, and if $(*)$ is heterotypical, by the fact that in assuming that x_c^{n+2} is a subword of w, we could choose x_c as well from the variables of the original word which was to be transformed, and while transforming w to w^* we never needed to introduce a new variable. Furthermore, let $w \equiv \tilde{w}\bar{w} \in M$, $\varphi \in \operatorname{End} F^0$, $\tilde{w}\varphi$ a prefix of some $w' \in M$, and $|\tilde{w}^{(2m-1)}\varphi| = 2m-1$. By Remark 2 (after Corollary 2.10), we can confine ourselves for such φ that

$$|x_t\varphi| = 1 \quad \text{for} \quad x_t \in X(w_1 w_3 w_4 w_6).$$

If $|\tilde{w}| \leqq i-1$, (iii) holds obviously. If $\tilde{w} \equiv w_1 w_2 \bar{v}$, then $w\varphi \equiv u_1 u_2 u_3 u_4 \cdot w'$, $u_i \in M_i$, and we obtain $(w\varphi)^*$ by applying (several times) the dual of either 5.9 or 5.10, and that of 5.14 or of 5.14′, not changing thereby $\tilde{w}\varphi$. Finally, if $\tilde{w} \equiv w_{(i-1)}\tilde{w}_2\hat{v}$, $\tilde{w}_2\hat{v}$ a prefix of $\hat{w}$, and either $\hat{v} \equiv x_{f(j)} x_{d(1)}^2 \dots x_{d(t-1)}^2 x_{d(t)}$, $\lambda \leqq 2$, $|w_j| \geqq 2t$; then, by assumption, $|x_{f(j)}\varphi| = |x_{d(1)}\varphi| = \dots = |x_{d(t)}\varphi| = 1$, and $X(\tilde{w}_2\varphi) \cap X(\overline{w}\varphi) \subseteq X(w_6\varphi)$. Thus, we can transform $(w_{(i-1)} w_2 x_{f(j)})\varphi^{(i-1)}(x_{d(1)}^2 \dots x_{d(t)}\bar{w})$ to a standard form $\overline{\overline{w}}$ without changing either w_0 or w_6; thereby we "standardize" the whole word $w\varphi$, without changing $(w_{(i-1)}\tilde{w}_2 x_{f(j)})\varphi$. Or $\tilde{w}_2 \equiv \emptyset$, $|\hat{v}| = 2m-1$, and the assertion is obvious once more. This completes the proof.

Theorem A follows now from [6], Proposition 4.1, Lemma 4.2, Propositions 6.3, 6.5 and 2.5.

References

[1] А. Я. Айзенштат, О перестановочных тождествах, *Современная Алгебра*, 3 (1975), 3—12.

[2] G. Higman, Ordering by divisibility in abstract algebras, *Proc. London Math. Soc.* (3), **2** (1952), 326—336.

[3] G. Pollák, On identities which define hereditarily finitely based varieties of semigroups, in: *Algebraic Theory of Semigroups* (Proc. Conf. Szeged, 1976), Coll. Math. Soc. János Bolyai 20, North-Holland (Amsterdam, 1979); pp. 447—452.

[4] ———, A class of hereditarily finitely based varieties of semigroups, in: *Algebraic Theory of Semigroups* (Proc. Conf. Szeged, 1976), Coll. Math. Soc. János Bolyai, 20, North-Holland (Amsterdam, 1979); pp. 433—445.

[5] ———, On two classes of hereditarily finitely based semigroup identities, *Semigroup Forum*, **25** (1982), 9—33.

[6] G. Pollák—M. Volkov, On almost simple semigroup identities, in: *Semigroups* (Proc. Conf. Szeged, 1981), Coll. Math. Soc. János Bolyai 39, North-Holland (Amsterdam—Oxford—New York, 1985); pp. 287—324.

[7] M. S. Putcha—A. Yaqub, Semigroups satisfying permutation identities, *Semigroup Forum*, 3 (1971), 68—73.

SOMOGYI B. U. 7
6720 SZEGED, HUNGARY

Acta Sci. Math., 50 (1986), 331—333

The arity of minimal clones

P. P. PÁLFY

Clones play a central role in universal algebra and in multiple-valued logic. A set of finitary operations is a *clone of operations* if it is closed under composition and contains all projections. The clones on a fixed set form a complete lattice with respect to inclusion. If the set is finite, then the lattice of clones is atomic and coatomic. The coatoms, i.e. the maximal clones, were classified in Ivo ROSENBERG's profound paper [4]. On the contrary, quite little is known about the minimal clones. Recently BÉLA CSÁKÁNY [1], [2] determined all minimal clones on the three-element set.

By definition, the *arity of a minimal clone* of operations is the minimum of arities of the nontrivial operations in the clone. Identifying any two variables in such an operation turns this operation into a projection. As observed by ŚWIERCZKOWSKI [5], if such an operation has at least four variables then it is a *semiprojection*, i.e. there is an index i $(1\leqq i\leqq k)$ such that $f(a_1, \ldots, a_k)=a_i$ whenever $|\{a_1, \ldots, a_k\}|<k$. Since the arity of any nontrivial semiprojection does not exceed the cardinality of the underlying set, it follows that the arity k of a minimal clone of operations on an n-element set must satisfy

$$k \leqq \begin{cases} 3, & \text{if} \quad n=2, \\ n, & \text{if} \quad n\geqq 3 \end{cases}$$

(see [3, 4.4.7]). It is easy to find unary, binary and ternary minimal clones, for example those generated by a constant function, a semilattice operation, or a median operation of a lattice, respectively (see [3, pp. 114—115]). If $n>2$, then any minimal clone contained in the clone generated by an arbitrary nontrivial n-ary semiprojection has arity n. But for $3<k<n$ the existence of a k-ary minimal clone of operations on an n-element set was not known.

Theorem. *There exists a k-ary minimal clone of operations on an n-element set $(n\geqq 3)$ if, and only if, $1\leqq k\leqq n$.*

Received May 17, 1984.

Proof. By the preceding remarks it is enough to point out a k-ary minimal clone for $3 \leqq k < n$. Fix different elements $b_1, \ldots, b_k, b_{k+1} \in A$, where $|A| = n$. Define a k-ary nontrivial operation f by

$$f(a_1, \ldots, a_k) = \begin{cases} b_{k+1}, & \text{if } a_1 = b_1 \text{ and } \{a_2, \ldots, a_k\} = \{b_2, \ldots, b_k\}, \\ a_1, & \text{otherwise.} \end{cases}$$

Since f is a semiprojection, the clone $[f]$ generated by f is k-ary. We are going to prove that $[f]$ is a minimal clone. For any term t representing a function in $[f]$ (in short, $t \in [f]$) we denote the first (from the left) variable of t by $\sigma(t)$, for example $\sigma(f(f(x_2, x_1, x_3), x_1, x_1)) = x_2$.

First we show that f satisfies the following identities:

(1) $f(f, t_2, \ldots, t_k) = f$ for any k-ary $t_2, \ldots, t_k \in [f]$,

(2) $f(x_1, t_2, \ldots, t_k) = f$ if the k-ary terms $t_2, \ldots, t_k \in [f]$ are such that $\sigma(t_i) = x_i$ $(i = 2, \ldots, k)$,

(3) $f(x_1, t_2, \ldots, t_k) = x_1$ if $t_2, \ldots, t_k \in [f]$ and for some $i, 2 \leqq i \leqq k$, $\sigma(t_i) = x_1$,

(4) $f(x_1, t_2, \ldots, t_k) = x_1$ if $t_2, \ldots, t_k \in [f]$ and for some i and j, $2 \leqq i < j \leqq k$, $\sigma(t_i) = \sigma(t_j)$.

Indeed, substitute $a_1, a_2, \ldots \in A$ for the variables $x_1, x_2, \ldots$. Observe that, by the definition of f, if $t \in [f]$ and $\sigma(t) = x_i$, then at the given valuation t takes on a_i or b_{k+1} and the latter can occur only if $a_i = b_1$. Hence if $a_1 \neq b_1$ then (1)—(4) obviously hold. Suppose $a_1 = b_1$. In (3) t_i takes on b_1 or b_{k+1}, in both cases the left hand side is b_1. Similarly, in (4) either t_i and t_j have equal values or one of them takes on b_{k+1}, again forcing the left hand side to be b_1. If $\{a_2, \ldots, a_k\} = \{b_2, \ldots, b_k\}$ then f takes on b_{k+1} and we have equality in (1), moreover, in (2) the set of values of $t_2, \ldots, t_k$ is also $\{b_2, \ldots, b_k\}$ hence we have equality here as well. If $\{a_2, \ldots, a_k\} \neq \{b_2, \ldots, b_k\}$ then some b_i $(2 \leqq i \leqq k)$ cannot occur as the value of any k-ary term hence in (1) and (2) both sides take on b_1.

Now the minimality of $[f]$ will be derived from the identities (1)—(4). We prove by induction on the length that any term is either equal to a projection or it turns into f by suitable identification and permutation of variables. Take a term $t = f(t_1, \ldots, t_k)$. By the inductive hypothesis, if t_1 is not a projection then suitable identification and permutation of variables yields a term $t' = f(f, t'_2, \ldots, t'_k)$, where $t'_2, \ldots, t'_k$ are k-ary. By (1) we have $t' = f$. Now let t_1 be a projection. Without loss of generality we may assume that $t_1 = x_1$. If there is a t_i $(2 \leqq i \leqq k)$ with $\sigma(t_i) = x_1$ or there are t_i, t_j $(2 \leqq i < j \leqq k)$ such that $\sigma(t_i) = \sigma(t_j)$ then $t = x_1$ by (3) or (4), respectively. Otherwise, by permuting the variables we may assume that $\sigma(t_i) = x_i$ for $i = 2, \ldots, k$. Then identifying $x_{k+1}, \ldots$ with x_1 we obtain f by (2). Hence for any nontrivial $t \in [f]$ we have $f \in [t]$, therefore $[f]$ is a minimal clone. Thus the proof is complete.

Note that by our proof any nontrivial k-ary operation satisfying the identities (1)—(4) generates a minimal clone. Indeed, the minimality of a clone is an inner property, hence it can be advantageous to consider clones abstractly. Following W. TAYLOR [6, pp. 360—361], an *abstract clone* T is a heterogeneous algebra on a series of base sets $T_1, T_2, \ldots$ equipped with composition operations $C^r_m\colon T_r \times T^r_m \to T_m$ $(m, r=1, 2, \ldots)$ and constants (that correspond to the projections) $e^n_i \in T_n$ $(i=1, \ldots, n;\ n=1, 2, \ldots)$ satisfying the identities

$$C^r_m(t, C^n_m(u_1, v_1, \ldots, v_n), \ldots, C^n_m(u_r, v_1, \ldots, v_n)) =$$
$$= C^n_m(C^r_n(t, u_1, \ldots, u_r), v_1, \ldots, v_n) \quad (m, n, r = 1, 2, \ldots),$$
$$C^n_m(e^n_i, t_1, \ldots, t_n) = t_i \quad (m, n = 1, 2, \ldots;\ i = 1, \ldots, n),$$
$$C^n_n(t, e^n_1, \ldots, e^n_n) = t \quad (n = 1, 2, \ldots).$$

Subclones, homomorphisms, etc. are defined in the natural manner. An abstract clone is minimal if it is generated by any of its nontrivial members. Any homomorphism of a minimal abstract clone onto a nontrivial clone of operations on a set yields a minimal clone of operations. We will pursue this line of research in a forthcoming paper.

Acknowledgements. I am deeply indebted to Béla Csákány: his pioneering work in this area inspired several ideas of the present paper, and our correspondence and discussions helped me to develop these ideals. I am also grateful to Ágnes Szendrei for her advice and to László Szabó for calling my attention to this problem.

References

[1] B. CSÁKÁNY, Three-element groupoids with minimal clones, *Acta Sci. Math.*, **45** (1983), 111—117.

[2] B. CSÁKÁNY, All minimal clones on the three-element set, *Acta Cybernet.*, 6 (1983), 227—238.

[3] R. PÖSCHEL und L. A. KALUŽNIN, *Funktionen- und Relationenalgebren*, DVW (Berlin, 1979).

[4] I. G. ROSENBERG, Über die funktionale Vollständigkeit in den mehrwertigen Logiken, *Rozpr. ČSAV Řada Mat. Přír. Věd*, **80**, 4 (1970), 3—93.

[5] S. ŚWIERCZKOWSKI, Algebras which are independently generated by every n elements, *Fund. Math.*, 49 (1960), 93—104.

[6] W. TAYLOR, Characterizing Mal'cev conditions, *Algebra Universalis*, 3 (1973), 351—397.

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
REÁLTANODA UTCA 13—15
1053 BUDAPEST, HUNGARY

Acta Sci. Math., 50 (1986), 335—336

A note on minimal clones

ZS. LENGVÁRSZKY

For $3<k<n$ the existence of k-ary minimal clones of operations on the n-element set was proved by P. P. PÁLFY [1] who exhibited concrete examples. Here we give a very simple nonconstructive proof of this theorem.

First we prove the following claim:

Let $(A, \leqq)$ be a partially ordered set and k a natural number such that the cardinality of an arbitrary antichain in $(A, \leqq)$ is at most $k-1$. Then the arity of any nontrivial monotone semiprojection on $(A, \leqq)$ does not exceed k.

Indeed, let f be a monotone semiprojection on $(A, \leqq)$ with arity $m \geqq k+1$. Without loss of generality we may assume that f is a semiprojection to the first variable x_1. Let $a_1, \ldots, a_m$ be arbitrary elements of A. By assumptions for some i and j, $2 \leqq i \neq j \leqq m$, $a_i \leqq a_j$ holds. For $1 \leqq l \leqq m$ we define the elements b_l and c_l by

$$b_l = \begin{cases} a_i & \text{if } l = i, j, \\ a_l & \text{if } l \neq i, j, \end{cases} \quad c_l = \begin{cases} a_j & \text{if } l = i, j, \\ a_l & \text{if } l \neq i, j. \end{cases}$$

Since f is monotone,

$$a_1 = b_1 = f(b_1, \ldots, b_m) \leqq f(a_1, \ldots, a_m) \leqq f(c_1, \ldots, c_m) = c_1 = a_1,$$

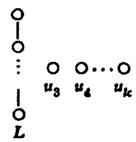
i.e. f is trivial.

In order to prove Pálfy's theorem, let k and n be natural numbers such that $3 \leqq k \leqq n$. Suppose we have an n-element poset $(A, \leqq)$ such that the cardinality of an arbitrary antichain is at most $k-1$ and f is a nontrivial, monotone, k-ary semiprojection on $(A, \leqq)$. Since A is finite, there exists a minimal clone C contained in the clone generated by f. Let g be a nontrivial function of minimal arity from C. Then g is a semiprojection (see [2]) with arity m. Clearly $m \geqq k$; on the other hand g is also monotone, hence $m \leqq k$ by our previous claim, i.e. $m = k$.

We will be done if for all k and n, $3 \leqq k \leqq n$, we give an n-element poset $(A, \leqq)$ and a nontrivial, monotone, k-ary semiprojection f on it. For this aim let A be an

Received August 29, 1985.

n-element set and $u_3, \ldots, u_k$ distinct fixed elements in A, $L=A\setminus\{u_3, \ldots, u_k\}$. Let $\leqq$ be a parial order on A such that the distinct elements u and v are comparable if and only if $u, v \in L$ (see the diagram).



Then any antichain of $(A, \leqq)$ has at most $k-1$ elements. Define a k-ary operation f by

$$f(a_1, \ldots, a_k) = \begin{cases} a_2 & \text{if } \ a_1, a_2 \in L \ \text{ and } \ a_3 = u_3, \ldots, a_k = u_k \\ a_1 & \text{otherwise.} \end{cases}$$

Since $|L| \geqq 2$, f is a nontrivial semiprojection to the first variable. Suppose that $a_1 \leqq b_1, \ldots, a_k \leqq b_k$. If $a_1, a_2 \in L$ and $a_3=u_3, \ldots, a_k=u_k$, then $b_1, b_2 \in L$ and $b_3=u_3, \ldots, b_k=u_k$, hence $f(a_1, \ldots, a_k)=a_2 \leqq b_2=f(b_1, \ldots, b_k)$. If either $a_1, a_2 \in L$ or $a_3=u_3, \ldots, a_k=u_k$ does not hold then either $b_1, b_2 \in L$ or $b_3=u_3, \ldots, b_k=u_k$ does not hold. Thus, $f(a_1, \ldots, a_k)=a_1 \leqq b_1=f(b_1, \ldots, b_k)$, i.e. f is monotone, completing the proof.

References

[1] P. P. Pálfy, The arity of minimal clones, *Acta Sci. Math.*, **50** (1986), 000—000.
[2] I. G. Rosenberg, Minimal clones I: The five types, in: *Lectures in Universal Algebra* (Proc. Conf. Szeged, 1983), Coll. Math. Soc. János Bolyai, Vol. 43, North-Holland (Amsterdam, 1986); pp. 405—427.

BOLYAI INSTITUTE
ARADI VÉRTANÚK TERE 1
6720 SZEGED, HUNGARY

Acta Sci. Math., 50 (1986), 337—350

Intervallfüllende Folgen und volladditive Funktionen

Z. DARÓCZY, A. JÁRAI und I. KÁTAI

1. Einführung

Es sei $\lambda_n > \lambda_{n+1} > 0$ $(n \in \mathbf{N})$ und $L := \sum_{n=1}^{\infty} \lambda_n < \infty$ eine Folge mit der folgenden Eigenschaft: für beliebiges $x \in [0, L]$ gibt es eine Folge $\varepsilon_n \in \{0, 1\}$ $(n \in \mathbf{N})$ derart, dass $x = \sum_{n=1}^{\infty} \varepsilon_n \lambda_n$ ist. Die Folge $\{\lambda_n\}$ wird dann intervallfüllend genannt. Z. B. ist $\{1/2^n\}$ intervallfüllend mit $L = 1$.

Ist $\{\lambda_n\}$ eine intervallfüllende Folge, so nennen wir die unbekannte Funktion $F\colon [0, L] \to \mathbf{R}$ volladditiv, falls

$$F\Big(\sum_{n=1}^{\infty} \varepsilon_n \lambda_n\Big) = \sum_{n=1}^{\infty} \varepsilon_n F(\lambda_n)$$

für jede Folge $\varepsilon_n \in \{0, 1\}$ $(n \in \mathbf{N})$ gilt. Unser Hauptziel in dieser Arbeit ist es, für geeignete intervallfüllende Folgen $\{\lambda_n\}$ die volladditive Funktionen zu bestimmen.

Ähnliche Untersuchungen in dieser Richtung kann man in der Arbeit [1] finden. Z. B. ist in [1] der Fall $\{\lambda_n = 1/2^n\}$ betrachtet.

2. Intervallfüllende Folgen

Es bezeichne Λ die Menge der reellen Folgen $\{\lambda_n\}$ mit $\lambda_n > \lambda_{n+1} > 0$ $(n \in \mathbf{N})$ und es sei $L := \sum_{n=1}^{\infty} \lambda_n < \infty$.

Definition 1. Wir nennen die Folge $\{\lambda_n\} \in \Lambda$ *intervallfüllend,* falls es für beliebiges $x \in [0, L]$ eine Folge $\varepsilon_n \in \{0, 1\}$ $(n \in \mathbf{N})$ gibt, für welche

(2.1) $$x = \sum_{n=1}^{\infty} \varepsilon_n \lambda_n$$

Eingegangen am 24 Mai, 1984.

ist.

Satz 2.1. *Die Folge* $\{\lambda_n\}\in\Lambda$ *ist genau dann intervallfüllend, falls*

$$\lambda_n \leqq \sum_{i=n+1}^{\infty} \lambda_i \tag{2.2}$$

für jedes $n\in\mathbf{N}$ *gilt.*

Beweis. (i) Nehmen wir an, dass $\lambda_n > \sum_{i=n+1}^{\infty} \lambda_i$ für irgendein $n\in\mathbf{N}$, und es sei $\lambda_n > y > \sum_{i=n+1}^{\infty} \lambda_i$. Wir zeigen, dass dann die Zahl $x := \sum_{i=1}^{n-1} \lambda_i + y \in [0, L]$ sich nicht in der Form (2.1) darstellen lässt, d.h. dass die Bedingung (2.2) notwendig ist. Gilt $\varepsilon_i = 0$ für irgendein $i \leqq n$, so ist

$$\sum_{i=1}^{\infty} \varepsilon_i \lambda_i \leqq \sum_{i=1}^{n-1} \lambda_i + \sum_{i=n+1}^{\infty} \lambda_i < x,$$

gilt hingegen $\varepsilon_i = 1$ für alle $i \leqq n$, so ist

$$\sum_{i=1}^{\infty} \varepsilon_i \lambda_i \geqq \sum_{i=1}^{n} \lambda_i > x,$$

d.h. x kann nicht in der Form (2.1) dargestellt werden.

(ii) Es sei $x\in[0, L]$ und wir setzen induktiv $\varepsilon_n = 1$ für $\sum_{i=1}^{n-1} \varepsilon_i \lambda_i + \lambda_n \leqq x$ und $\varepsilon_n = 0$ andernfalls. Wir zeigen, dass $\sum_{i=1}^{\infty} \varepsilon_i \lambda_i < x$ unmöglich ist, d.h. dass x in der Gestalt (2.1) darstellbar ist. Gilt $\varepsilon_n = 0$ für unendlich viele Werte n, dann ist für diese Werte n

$$x - \sum_{i=1}^{\infty} \varepsilon_i \lambda_i \leqq x - \sum_{i=1}^{n-1} \varepsilon_i \lambda_i < \lambda_n,$$

woraus wegen $\lambda_n \to 0$ die Darstellung $x = \sum_{i=1}^{\infty} \varepsilon_i \lambda_i$ folgt. Gilt $\varepsilon_n = 0$ nur für endlich viele Werte n, so sei N der grösste dieser Werte. Wir haben

$$x - \sum_{i=1}^{N-1} \varepsilon_i \lambda_i < \lambda_N \leqq \sum_{i=N+1}^{\infty} \lambda_i = \sum_{i=N+1}^{\infty} \varepsilon_i \lambda_i,$$

woraus

$$x < \sum_{i=1}^{\infty} \varepsilon_i \lambda_i$$

folgt, ein Widerspruch.

Definition 2. Es sei $\{\lambda_n\}\in\Lambda$ eine intervallfüllende Folge. Wir nennen die Zahl $x\in[0, L]$ *eindeutig,* falls es genau eine Folge $\varepsilon_n\in\{0, 1\}$ $(n\in\mathbf{N})$ gibt, für welche (2.1) gilt.

Bemerkung. Offenbar sind 0 und L eindeutige Zahlen.

Definition 3. Wir nennen die intervallfüllende Folge $\{\lambda_n\}\in A$ *locker*, falls für beliebiges $N\in\mathbf{N}$ die Restfolge $\{\lambda_n\}-\{\lambda_N\}$ intervallfüllend ist.

Bemerkung. Im Falle einer lockeren Folge sei

$$L_N := \sum_{\substack{n=1\\ n\neq N}}^{\infty} \lambda_n = L-\lambda_N \quad \text{für beliebiges} \quad N\in\mathbf{N}.$$

Dann ist jedes $x\in[0, L_N]$ darstellbar in der Form

$$x = \sum_{\substack{i=1\\ i\neq N}}^{\infty} \varepsilon_i\lambda_i \quad \text{mit} \quad \varepsilon_i\in\{0, 1\}.$$

Definition 4. Wir nennen die intervallfüllende Folge $\{\lambda_n\}\in A$ *ergiebig*, falls jede Zahl $x\in]0, L[$ nichteindeutig ist.

Satz 2.2. *Ist die intervallfüllende Folge $\{\lambda_n\}\in A$ locker, so ist sie auch ergiebig.*

Beweis. Es sei $x\in[0, L]$. Dann gibt es eine Folge $\varepsilon_n\in\{0, 1\}$ $(n\in\mathbf{N})$ derart, dass

$$x = \sum_{n=1}^{\infty} \varepsilon_n\lambda_n. \tag{2.3}$$

(i) Ist in (2.3) $\varepsilon_n=1$ nur endlich viele n erfüllt, so sei N der grösste dieser Werte. Da die Folge intervallfüllend ist, gilt

$$x = \sum_{n=1}^{\infty} \varepsilon_n\lambda_n = \sum_{n=1}^{N-1} \varepsilon_n\lambda_n+\lambda_N = \sum_{n=1}^{N-1} \varepsilon_n\lambda_n + \sum_{n=N+1}^{\infty} \delta_n\lambda_n$$

mit $\delta_n\in\{0, 1\}$ $(n\geqq N+1)$. Es ist also x nicht eindeutig.

(ii) Ist in (2.3) $\varepsilon_n=1$ für unendlich viele n erfüllt, so gibt es ein $N\in\mathbf{N}$ mit $\varepsilon_N=1$ und $x<L-\lambda_N=L_N$. Darum gibt es eine Folge $\delta_n\in\{0, 1\}$ $(n\in\mathbf{N}, n\neq N)$ für welche

$$x = \sum_{\substack{n=1\\ n\neq N}}^{\infty} \delta_n\lambda_n$$

gilt, d.h. x ist nicht eindeutig.

Es sei $1<q<2$ und $\lambda_n:=1/q^n$ $(n\in\mathbf{N})$. Dann ist $\{1/q^n\}\in A$ und $L:=\sum_{n=1}^{\infty} 1/q^n = 1/(q-1)>1$. Es sei $k\in\mathbf{N}$ festgewählt und $1<q(k)<2$ die Wurzel der Gleichung

$$L-1 = 1/q^k. \tag{2.4}$$

Satz 2.3. *Für $1<q<2$ ist die Folge $\{1/q^n\}\in A$ intervallfüllend. Für $1<q\leqq q(1)$ ist $\{1/q^n\}$ locker, und folglich ergiebig.*

Beweis. (i) Im Falle $1<q<2$ gilt für jedes n

$$1/q^n < (1/q^n)(1/(q-1)) = \sum_{i=n+1}^{\infty} 1/q^i,$$

so dass wegen Satz 2.1. die Folge $\{1/q^n\}$ intervallfüllend ist.

(ii) Für $1<q\leqq q(1)$ hat man $L-1\geqq 1/q$. Dann ist bei beliebigem festgewählten $N\in\mathbf{N}$ für die Restfolge $\{1/q^n\}-\{1/q^N\}$ (2.2) trivialerweise erfüllt, falls nur $n\geqq N+1$ gilt. Ist hingegen $n<N$, so folgt aus

$$q^n/q^N \leqq 1/q \leqq L-1$$

die Ungleichung

$$1/q^n \leqq \sum_{i=n+1}^{\infty} 1/q^i - 1/q^N,$$

d.h. es gilt (2.2). Somit ist die Folge $\{1/q^n\}$ locker, und wegen Satz 2.2. auch ergiebig.

Satz 2.4. *Für $q(1)<q<2$ ist die intervallfüllende Folge $\{1/q^n\}\in\Lambda$ nicht ergiebig, also auch nicht locker.*

Beweis. Der Beweis ergibt sich aus dem folgenden.

Lemma. *Für $q(1)<q<2$ ist die Zahl*

$$x := \sum_{n=1}^{\infty} 1/q^{2n-1} \in]0, L[\tag{2.5}$$

eindeutig.

Beweis des Lemmas. Nehmen wir an, dass die mittels (2.5) definierte Zahl x auch noch eine andere Darstellung der Form (2.1) hat, wobei $\lambda_n := 1/q^n$ ist. Es sei N die erste natürliche Zahl für welche $\varepsilon_N \neq \delta_N$ gilt; hierbei ist $\delta_n = 1$ für ungerades n, und $\delta_n = 0$ für gerades n. Nun gilt für $\delta_N = 0$ (gerades N) $\varepsilon_N = 1$, d.h. wegen

$$x = \sum_{n=1}^{\infty} \delta_n/q^n = \sum_{n=1}^{N-1} \delta_n/q^n + \sum_{n=N+1}^{\infty} \delta_n/q^n = \sum_{n=1}^{N-1} \delta_n/q^n + 1/q^N + \sum_{n=N+1}^{\infty} \varepsilon_n/q^n$$

haben wir

$$\sum_{n=N+1}^{\infty} \delta_n/q^n = 1/q^N + \sum_{n=N+1}^{\infty} \varepsilon_n q^n.$$

Daraus folgt

$$(1/q^N)(q/(q^2-1)) = 1/q^N + \sum_{n=N+1}^{\infty} \varepsilon_n/q^n \geqq 1/q^N,$$

d.h. $L-1\geqq 1/q$, dies ist aber unmöglich, da im Falle $q(1)<q<2$ die Ungleichung $L-1<1/q$ erfüllt ist. Für $\delta_N=1$ (N ungerade) und für $\varepsilon_N=0$ verläuft der Beweis ähnlich.

3. Über volladditive Funktionen

Es sei $\{\lambda_n\} \in \Lambda$ eine festgewählte intervallfüllende Folge.

Definition 5. Wir nennen die Funktion F: $[0, L] \to \mathbf{R}$ *volladditiv,* falls für jede Folge $\varepsilon_n \in \{0, 1\}$ $(n \in \mathbf{N})$ die Beziehung

$$F\Big(\sum_{n=1}^{\infty} \varepsilon_n \lambda_n\Big) = \sum_{n=1}^{\infty} \varepsilon_n F(\lambda_n) \tag{3.1}$$

gilt.

Satz 3.1. *Es sei $\{\lambda_n\} \in \Lambda$ eine intervallfüllende und ergiebige Folge. Ist F: $[0, L] \to \mathbf{R}$ volladditiv, so gibt es ein $c \in \mathbf{R}$ derart, dass*

$$F(x) = cx \tag{3.2}$$

für alle $x \in [0, L]$.

Beweis. Wir setzen

$$\hat{F}(x) := F(x) - F(L)x/L \quad (x \in [0, L]). \tag{3.3}$$

Dann ist $\hat{F}$ volladditiv und es gilt $\hat{F}(0) = \hat{F}(L) = 0$. Es sei $\hat{F}(\lambda_n) =: a_n$ und $P :=$ $:= \{n | n \in \mathbf{N},\ a_n > 0\}$. Es sei noch

$$\xi := \sum_{n \in P} \lambda_n. \tag{3.4}$$

Für $\xi \in]0, L[$ gibt es eine Folge $\varepsilon_n \in \{0, 1\}$ derart, dass

$$\xi = \sum_{n=1}^{\infty} \varepsilon_n \lambda_n \tag{3.5}$$

gilt, und die Darstellung (3.5) von der Darstellung (3.4) verschieden ist. Darum existiert ein $n_0 \in P$ mit $\varepsilon_{n_0} = 0$, woraus wegen (3.1)

$$\hat{F}(\xi) = \hat{F}\Big(\sum_{n \in P} \lambda_n\Big) = \sum_{n \in P} \hat{F}(\lambda_n) = \sum_{n \in P} a_n >$$

$$> \sum_{n=1}^{\infty} \varepsilon_n a_n = \sum_{n=1}^{\infty} \varepsilon_n \hat{F}(\lambda_n) = \hat{F}\Big(\sum_{n=1}^{\infty} \varepsilon_n \lambda_n\Big) = \hat{F}(\xi)$$

folgt, was unmöglich ist. Somit haben wir $\xi = 0$ oder $\xi = L$, d.h. $P = \emptyset$ oder $P = \mathbf{N}$. Der letztere Fall ist unmöglich, weil dann $\hat{F}(\xi) = \hat{F}(L) > 0$ wäre. Ist aber $P = \emptyset$, so gilt $\hat{F}(x) \leqq 0$ für jedes $x \in [0, L]$. Da $-\hat{F}$ ebenfalls volladditiv ist, ergibt sich durch eine Widerholung des vorigen Gedankenganges $-\hat{F}(x) \leqq 0$, woraus $\hat{F}(x) = 0$ für jedes $x \in [0, L]$ folgt. Aus (3.3) folgt jetzt mit $c := F(L)/L$ die Behauptung.

Bemerkung. In Satz 3.1. kann man die Bedingung der Ergiebigkeit durch diejenige der Lockerheit ersetzen.

Korollar 3.1. *Falls* $1<q\leqq q(1)$ *ist und die Funktion* $F\colon [0, L]\to\mathbf{R}$ $(L:=1/(q-1))$ *die Bedingung*

$$F\Big(\sum_{n=1}^{\infty}\varepsilon_n/q^n\Big)=\sum_{n=1}^{\infty}\varepsilon_n F(1/q^n) \tag{3.6}$$

für jede Folge $\varepsilon_n\in\{0, 1\}$ $(n\in\mathrm{N})$ *erfüllt, so gibt es ein* $c\in\mathbf{R}$ *derart, dass* $F(x)=cx$ *für jedes* $x\in[0, L]$ *gilt.*

Beweis. Wegen Satz 2.3. ist jetzt $\{1/q^n\}\in\Lambda$ intervallfüllend und locker (d.h. ergiebig), so dass sich Satz 3.1. anwenden lässt.

Die Beweisidee des Satzes 3.1. ermöglicht es uns, das folgende Resultat auszusprechen:

Satz 3.2. *Es sei* $\{\lambda_n\}\in\Lambda$ *eine intervallfüllende Folge, und* $F\colon [0, L]\to\mathbf{R}$ *eine volladditive Funktion. Ferner sei* $a_n:=F(\lambda_n)$ $(n\in\mathrm{N})$. *Für* $P:=\{n\mid n\in\mathrm{N},\ a_n>0\}$ *und* $\xi:=\sum_{n\in P}\lambda_n$ *ist im Falle* $P\neq\emptyset$ *und* $P\neq\mathrm{N}$ *die Grösse* $\xi\in]0, L[$ *eindeutig.*

Beweis. Wegen der Bedingung $P\neq\emptyset$ und $P\neq\mathrm{N}$ gilt $\xi\in]0, L[$. Ist ξ nicht eindeutig, so gibt es eine Folge $\varepsilon_n\in\{0, 1\}$ und $n_0\in P$ derart, dass $\varepsilon_{n_0}=0$ und

$$\xi=\sum_{n=1}^{\infty}\varepsilon_n\lambda_n$$

ist. Daraus folgt auf Grund der Volladditivät

$$F(\xi)=F\Big(\sum_{n\in P}\lambda_n\Big)=\sum_{n\in P}a_n>\sum_{n=1}^{\infty}\varepsilon_n a_n=F\Big(\sum_{n=1}^{\infty}\varepsilon_n\lambda_n\Big)=F(\xi),$$

was einen Widerspruch bedeutet. Folglich ist ξ eindeutig. ∎

Definition 5. Es sei $\{\lambda_n\}\in\Lambda$ eine intervallfüllende Folge. Für $x\in[0, L]$ sei induktiv nach n

$$\varepsilon_n(x):=\begin{cases}1, & \text{für } \sum_{i=1}^{n-1}\varepsilon_i(x)\lambda_i+\lambda_n\leqq x,\\ 0, & \text{für } \sum_{i=1}^{n-1}\varepsilon_i(x)\lambda_i+\lambda_n> x.\end{cases} \tag{3.7}$$

Sodann gilt wegen Satz 2.1.

$$x=\sum_{n=1}^{\infty}\varepsilon_n(x)\lambda_n. \tag{3.8}$$

Die Darstellung (3.8) nennen wir die *reguläre* Darstellung von x.

Satz 3.3. *Es sei* $\{\lambda_n\}\in\Lambda$ *eine intervallfüllende Folge. Bei beliebigem* $x\in[0, L]$ *gilt* $\varepsilon_n(x)=0$ *für unendlich viele Werte von n.*

Beweis. Für $x=0$ ist die Behauptung trivial. Es sei $0<x<L$. Dann gibt es in (3.8) ein n mit $\varepsilon_n(x)=0$. Gilt entgegen unserer Behauptung $\varepsilon_n(x)=0$ in (3.8) nur für endlich viele n, so sei N der grösste dieser Werte. Wegen (3.7) ist nun

$$\sum_{i=1}^{N-1} \varepsilon_i(x)\lambda_i+\lambda_N > x = \sum_{i=1}^{N-1} \varepsilon_i(x)\lambda_i + \sum_{i=N+1}^{\infty} \lambda_i$$

in Widerspruch zu (2.2).

Satz 3.4. *Ist* $\{\lambda_n\}\in\Lambda$ *eine intervallfüllende Folge und* F: $[0, L]\to\mathbf{R}$ *volladditiv, so gilt für* $a_n:=F(\lambda_n)$ $(n\in\mathbf{N})$ *die Beziehung*

$$\text{(3.9)} \qquad \sum_{n=1}^{\infty} |a_n| < \infty.$$

Beweis. Es sei $P:=\{n\,|\,n\in\mathbf{N},\ a_n>0\}$ und $M:=\mathbf{N}-P$. Dann gilt für

$$\xi := \sum_{n\in P} \lambda_n$$

wegen der Volladditivität

$$F(\xi) = F\Big(\sum_{n\in P}\lambda_n\Big) = \sum_{n\in P} F(\lambda_n) = \sum_{n\in P} |a_n|$$

und

$$F(L-\xi) = F\Big(\sum_{n\in M}\lambda_n\Big) = \sum_{n\in M} F(\lambda_n) = -\sum_{n\in M} |a_n|$$

woraus

$$\sum_{n=1}^{\infty} |a_n| = F(\xi)-F(L-\xi) < \infty$$

folgt.

Satz 3.5. *Ist* $\{\lambda_n\}\in\Lambda$ *eine intervallfüllende Folge und* F: $[0, L]\to\mathbf{R}$ *volladditiv, so ist* F *für beliebiges* $x\in[0, L[$ *rechtsstetig.*

Beweis. Für beliebiges $\varepsilon>0$ gibt es wegen Satz 3.4. ein N derart, dass

$$\text{(3.10)} \qquad \sum_{i=N+1}^{\infty} |F(\lambda_i)| < \varepsilon/2.$$

Es sei

$$\delta_N := \sum_{n=N+1}^{\infty} \lambda_n - \sum_{n=N+1}^{\infty} \varepsilon_n(x)\lambda_n,$$

wobei $x=\sum_{n=1}^{\infty} \varepsilon_n(x)\lambda_n$ eine reguläre Darstellung ist. Wegen Satz 3.3. ist $\delta_N>0$. Falls

$$x < y < x+\delta_N = \sum_{n=1}^{N} \varepsilon_n(x)\lambda_n + \sum_{n=N+1}^{\infty} \lambda_n,$$

so gibt es wegen $y-\sum_{n=1}^{N}\varepsilon_n(x)\lambda_n<\sum_{n=N+1}^{\infty}\lambda_n$ eine Folge $\varepsilon_n^*\in\{0, 1\}$ $(n\geqq N+1)$ derart, dass

$$y-\sum_{n=1}^{N}\varepsilon_n(x)\lambda_n=\sum_{n=N+1}^{\infty}\varepsilon_n^*\lambda_n$$

ist, und daraus folgt wegen der Volladditivität von F und wegen (3.10)

$$|F(y)-F(x)|=\Big|\sum_{n=N+1}^{\infty}\varepsilon_n^*F(\lambda_n)-\sum_{n=N+1}^{\infty}\varepsilon_n(x)F(\lambda_n)\Big|\leqq 2\sum_{n=N+1}^{\infty}|F(\lambda_n)|<\varepsilon.$$

Satz 3.6. *Ist* $\{\lambda_n\}\in\Lambda$ *eine intervallfüllende Folge und* $F\colon[0, L]\to\mathbf{R}$ *volladditiv, so ist F im abgeschlossenen Intervall* $[0, L]$ *stetig.*

Beweis. Für beliebiges $x\in[0, L]$ hat man wegen der Volladditivität von F

$$F(x)+F(L-x)=F(L). \tag{3.11}$$

Wegen Satz 3.5. ist F für alle $x\in[0, L[$ rechtsstetig, also auf Grund von (3.11) für alle $y\in]0, L]$ linksstetig, und somit stetig auf $[0, L]$.

4. Volladditive Funktionen im Falle spezieller intervallfüllender Folgen

Es sei $1<q<2$ und $\{1/q^n\}\in\Lambda$ eine intervallfüllende Folge. Ist $F\colon[0, L]\to\mathbf{R}$ $(L:=1/(q-1))$ volladditiv (d.h. gilt (3.1) für die Folge $\lambda_n:=1/q^n$), so gilt nach Korollar 3.1. für $1<q\leqq q(1)$ die Beziehung $F(x)=cx$ mit c konstant. Es ist natürlich danach zu fragen, was sich im Falle $q(1)<q<2$ sagen lässt, wenn also wegen Satz 2.4. die Folge $\{1/q^n\}$ nicht ergiebig (nicht locker) ist.

Satz 4.1. *Für* $q=q(k)$ $(k\in\mathbf{N})$ *und volladditives F gibt es ein* $c\in\mathbf{R}$ *derart, dass* $F(x)=cx$ *für alle* $x\in[0, 1/(q(k)-1)]$ *gilt.*

Beweis. Es sei $k\in\mathbf{N}$ festgewählt und $F\colon[0, L]\to\mathbf{R}$ $(L:=1/(q(k)-1)$ volladditiv. Dann ist auch die Funktion $\hat{F}(x):=F(x)-F(L)x/L$ $(x\in[0, L])$ volladditiv und es gilt $\hat{F}(0)=\hat{F}(L)=0$. Es sei $a_n:=\hat{F}(1/q^n)$ $(n\in\mathbf{N})$ mit $q:=q(k)$. Wegen der Volladditivität gilt

$$0=\hat{F}(L)=\hat{F}\Big(\sum_{n=1}^{\infty}1/q^n\Big)=\sum_{n=1}^{\infty}\hat{F}(1/q^n)=\sum_{n=1}^{\infty}a_n. \tag{4.1}$$

Auf Grund der Voraussetzung ist

$$1=L-1/q^k=\sum_{\substack{n=1\\ n\neq k}}^{\infty}1/q^n$$

woraus für beliebiges $N \in \mathbf{N}$

$$1/q^N = \sum_{\substack{n=1 \\ n \neq k}} 1/q^{N+n} \tag{4.2}$$

folgt. Aus (4.2) ergibt sich der Volladditivität von $\hat{F}$

$$a_N = \sum_{\substack{n=1 \\ n \neq k}}^{\infty} a_{N+n} \tag{4.3}$$

und

$$a_{N+1} = \sum_{\substack{n=1 \\ n \neq k}}^{\infty} a_{N+n+1} \tag{4.4}$$

für alle $N \in \mathbf{N}$. Aus (4.3) und (4.4) folgt nun $a_N - a_{N+1} = a_{N+1} + a_{N+k+1} - a_{N+k}$ d.h.

$$a_{N+k+1} - a_{N+k} + 2a_{N+1} - a_N = 0 \tag{4.5}$$

für alle $N \in \mathbf{N}$.

Wegen (4.1) ist die Potenzreihe

$$f(z) := \sum_{n=1}^{\infty} a_n z^n \tag{4.6}$$

konvergent für $|z| < 1$ und für $z = 1$. Indem wir jetzt die Gleichung (4.5) mit der Zahl z^{N+k+1} multiplizieren und für N summieren, erhalten wir unter Berücksichtigung von (4.6) für $|z| < 1$ und für $z = 1$

$$f(z) - \sum_{i=1}^{k+1} a_i z^i - z\left[f(z) - \sum_{i=1}^{k} a_i z^i\right] + 2^i z^k [f(z) - a_1 z] - z^{k+1} f(z) = 0$$

und daraus folgt

$$f(z)[z^{k+1} - 2z^k + z - 1] = z(z-1) \sum_{i=1}^{k} a_i z^{i-1} + z^{k+1}(-a_{k+1} - 2a_1).$$

Aus der letzteren Gleichung erhalten wir für $z = 1$ und unter Berücksichtigung von $f(1) = 0$ die Beziehung $-a_{k+1} - 2a_1 = 0$, d.h.

$$f(z)[z^{k+1} - 2z^k + z - 1] = z(z-1) \sum_{i=1}^{k} a_i z^{i-1} = z(z-1) Q_{k-1}(z) \tag{4.7}$$

für alle $|z| < 1$, wobei $Q_{k-1}(z)$ ein Polynom von z höchstens $(k-1)$-ten Grades ist.

Wir betrachten jetzt das Polynom

$$P(z) := P_{k+1}(z) := z^{k+1} - 2z^k + z - 1 \tag{4.8}$$

für welches $1 < z := q(k) < 2$ wegen $1/(q(k)-1) - 1 = 1/q(k)^k$ eine reelle Wurzel ist. Es sei

$$A(z) := z^{k+1} + z \quad \text{und} \quad B(z) := 2z^k + 1. \tag{4.9}$$

Es ist $A(z)=P(z)+B(z)$ wobei P, B holomorph im abgeschlossenen Einheitskreis $|z|\leqq 1$ sind, ferner ist

$$|A(z)| = |P(z)+B(z)| < |P(z)|+|B(z)| \tag{4.10}$$

für $|z|=1$. Die Ungleichung (4.10) ergibt sich daraus, dass für $|z|=1$

$$|A(z)| = |z|\,|z^k+1| = |z^k+1| < |2z^k+1| = |B(z)|$$

gilt. Darum haben nach dem Satz von Rouché P und B mit Multiplizität gerechnet dieselbe Anzahl von Wurzeln im offenen Einheitskreis $|z|<1$. Da für die Wurzeln von B die Ungleichung $|z|=|\sqrt[k]{-1/2}|<1$ gilt, haben sowohl B als auch P im offenen Einheitskreis genau k Wurzeln. Da $z=0$ und $z=1$ keine Wurzeln von P sind, folgt auf Grund von (4.7), dass sämtliche sich im offenen Einheitskreis befindenden Wurzeln von P auch Wurzeln von $Q_{k-1}(z)$ sind, so dass Q_{k-1} ebenfalls k Wurzeln hat. Dies ist nur möglich falls $Q_{k-1}(z)=0$ für alle z, und so folgt aus (4.7) $f(z)=\sum_{n=1}^{\infty} a_n z^n=0$ für $|z|<1$. Somit ergibt sich $a_k=0$ $(n\in\mathbb{N})$. Da nun jedes $x\in[0, L]$ eine Darstellung $x=\sum_{n=1}^{\infty} \varepsilon_n/q^n$ $(\varepsilon_n\in\{0, 1\})$ zulässt, erhalten wir auf Grund der Volladditivität von $\hat{F}$

$$\hat{F}(x) = \hat{F}\Big(\sum_{n=1}^{\infty} \varepsilon_n/q^n\Big) = \sum_{n=1}^{\infty} \varepsilon_n a_n = 0,$$

woraus $F(x)=cx$ $\big(c:=F(L)/L\big)$ folgt.

Bemerkung. Die Behauptung des Satzes gilt auch für $q=q(1)$. Dies bedeutet einen neuen, von der Beweismethode des Korollars 3.1. verschiedenen Beweis für das vorige $q=q(1)$.

5. Eindeutige Zahlen

Gemäss Satz 2.4. gibt es eindeutige Zahlen für die intervallfüllende Folge $\{1/q^n\}\in\Lambda$, falls $q(1)<q<2$.

Satz 5.1. *Es sei* $q(1)<q<2$. *Falls* $x\in]0, 1[$ *für die intervallfüllende Folge* $\{1/q^n\}\in\Lambda$ *eine eindeutige Zahl ist, gilt*

$$x\in \bigcup_{n=1}^{\infty} [L/q^n, 1/q^{n-1}). \tag{5.1}$$

Beweis. Für $x\in]0, 1[$ gibt es ein n derart, dass $x\in A_n:=[1/q^n, 1/q^{n-1})$ ist. Da für $q(1)<q<2$ die Ungleichungen $1/q^n<L/q^n<1/q^{n-1}$ gelten, zeigen wir, dass im Falle $x\in B_n:=[1/q^n, L/q^n)\subset A_n$ die Zahl x nicht eindeutig ist, also für eindeutiges x die Beziehung $x\in[L/q^n, 1/q^{n-1})$ gilt, d.h. (5.1) erfüllt ist.

Dann lässt sich nämlich im Falle $x\in B_n$ wegen

$$1/q^n < \sum_{i=n+1}^{\infty} 1/q^i = L/q^n$$

jedes Element von $[0, L/q^n[$, also auch x, in der Gestalt

$$x = \sum_{i=1}^{\infty} \varepsilon_i/q^{n+i} \tag{5.2}$$

schreiben, mit $\varepsilon_i\in\{0, 1\}$ $(i\in\mathrm{N})$. Anderseits hat x die Gestalt $x=1/q^n+\vartheta$, wobei wegen $0\leqq\vartheta=x-1/q^n<L/q^n$ auch ϑ in der Form $\vartheta=\sum_{i=1}^{\infty}\delta_i/q^{n+i}$, mit $\delta_i\in\{0, 1\}$ $(i\in\mathrm{N})$ geschrieben werden kann. Darum gilt

$$x = 1/q^n + \sum_{i=1}^{\infty} \delta_i/q^{n+i}. \tag{5.3}$$

Offenbar ist wegen (5.2) und (5.3) x nicht eindeutig.

Satz 5.2. *Gilt* $q(1)<q\leqq q(2)$ *und ist* $x\in]0, 1[$ *eindeutig in Bezug auf die intervallfüllende Folge* $\{1/q^n\}\in\Lambda$, *so gibt es ein* $N\in\mathrm{N}$ *derart, dass*

$$x = (1/q^{N-1}) \sum_{k=1}^{\infty} 1/q^{2k-1} \tag{5.4}$$

gültig ist.

Beweis. (i) Es sei $x\in[1/q, 1)$ eindeutig. Dann gilt wegen Satz 5.1. $x\in[L/q, 1)$. Da $x=1/q+Tx/q$ gilt, ist $Tx\in]0, 1[$ eindeutig, weil andernfalls x nicht eindeutig wäre. Anderseits haben wir $Tx\in[L-1, q-1)$, woraus wegen $1/q^2\leqq L-1<q-1\leqq L/q$ (diese Ungleichungen sind für $q(1)<q\leqq q(2)$ richtig) unter Berücksichtigung von Satz 5.1.

$$Tx\in[L/q^2, 1/q)$$

folgt. Daraus ergibt sich, dass

$$Sx:= qTx\in[L/q, 1)\subset[1/q, 1)$$

und Sx eindeutig ist, weil Tx eindeutig war. Nun folgt

$$x = 1/q+Sx/q^2, \tag{5.5}$$

wobei $Sx\in[L/q, 1)\subset[1/q, 1)$ eindeutig ist. Wir zeigen mittels Induktion nach n, dass

$$x = \sum_{k=1}^{2n-1} 1/q^{2k-1}+S^n x/q^{2n} \tag{5.6}$$

gilt, wobei $S^n x := S(S^{n-1}x) \in [1/q, 1)$ eindeutig ist. Für $n=1$ ist (5.6) wegen (5.5) erfüllt. Gilt (5.6), so haben wir wegen (5.5)

$$S^n x = 1/q + S^{n+1}x/q^2,$$

wobei $S^{n+1}x \in [1/q, 1)$ eindeutig ist, also gilt

$$x = \sum_{k=1}^{2n-1} 1/q^{2k-1} + (1/q + S^{n+1}x/q^2)/q^{2n} = \tag{5.7}$$

$$= \sum_{k=1}^{2n-1} 1/q^{2k-1} + 1/q^{2n+1} + S^{n+1}x/q^{2(n+1)},$$

d.h. (5.6) ist auch für $n+1$ richtig. Aus (5.6) folgt wegen $\lim_{n\to\infty} S^n x/q^{2n} = 0$

$$x = \sum_{k=1}^{\infty} 1/q^{2k-1} \tag{5.8}$$

und zwar ist auf Grund des im Beweis von Satz 2.4. auftretenden Lemmas diese Darstellung tatsächlich eindeutig.

(ii) Falls x in $]0, 1[$ enthalten und eindeutig ist, so gibt es ein $N \in \mathbf{N}$ derart, dass $x \in [1/q^N, 1/q^{N-1})$ gilt. Daraus ergibt sich, dass $q^{N-1}x \in [1/q, 1)$ eindeutig ist, d.h. es gilt wegen (i) notwendigerweise (5.8). Also ist x in der Tat von der Gestalt (5.4).

Bemerkung. Auf Grund der Definition sieht man leicht ein, dass für eindeutiges $x \in]0, L[$ auch $L-x$ eindeutig ist.

6. Volladditive Funktionen im Falle $q(1) < q \leqq q(2)$

Satz 6.1. *Ist $q(1) < q \leqq q(2)$ und $F\colon [0, L] \to \mathbf{R}$ volladditiv bezüglich der intervallfüllenden Folge $\{1/q^n\} \in \Lambda$ $(L := 1/(q-1))$, so gibt es ein $c \in \mathbf{R}$ derart, dass $F(x) = cx$ für alle $x \in [0, L]$ gilt.*

Beweis. Setzen wir

$$\hat{F}(x) := F(x) - (F(L)/L)x \quad (x \in [0, L]), \tag{6.1}$$

so ist $\hat{F}$ volladditiv und es gilt $\hat{F}(0) = \hat{F}(L) = 0$. Es sei $a_n := \hat{F}(1/q^n)$ $(n \in \mathbf{N})$ und

$$P := \{n \mid n \in \mathbf{N},\ a_n > 0\}.$$

Ferner sei

$$\xi := \sum_{n \in P} 1/q^n.$$

Wir zeigen dass $P \neq \emptyset$ ist. Andernfalls ist $P \neq \emptyset$ und folglich $\xi \in]0, L[$, weil aus $\xi = L$ wegen der Volladditivität von $\tilde{F}$ folgen würde, dass $\hat{F}(\xi) = \hat{F}(L) > 0$ ist, also ein Widerspruch. Somit gilt $P \neq \emptyset$ und $P \neq \mathbf{N}$, also ist auf Grund von Satz 3.2. ξ *eindeutig*. Ist nun $x \in]0, L[$ beliebig, so hat man wegen der Volladditivität von $\hat{F}$

$$(6.2) \qquad \hat{F}(x)+\hat{F}(L-x) = \hat{F}(L) = 0,$$

woraus $\hat{F}(L/2)=0$ folgt. Daraus ergibt sich $\xi \neq L/2$, d.h. $\xi \in]0, L/2[\cup]L/2, L[$. Auf Grund der Identität (6.2) kann man ohne Beschränkung der Allgemeinheit $\xi \in]0, L/2[$ voraussetzen. Wegen $q > q(1)$ gilt $L/2 < 1$, d.h. $\xi \in]0, L/2[\subset]0, 1[$, und auf Grund der Eindeutigkeit von ξ folgt aus Satz 5.2.

$$(6.3) \qquad \xi = 1/q^{N-1} \sum_{k=1}^{\infty} 1/q^{2k-1} = \sum_{k=1}^{\infty} 1/q^{N+2(k-1)}$$

für irgendein $N \in \mathbf{N}$. Es sei

$$(6.4) \qquad \alpha := \sum_{k=1}^{\infty} 2/q^{N+4(k-1)}$$

und

$$(6.5) \qquad \beta := \sum_{k=1}^{\infty} 2/q^{N+4(k-1)+2}.$$

Dann gilt $\beta < \xi < \alpha$ und

$$(6.6) \qquad \alpha+\beta = 2\xi.$$

Lemma. $\hat{F}(\alpha)=2\hat{F}(\alpha/2)$, $\hat{F}(\beta)=2\hat{F}(\beta/2)$.

Beweis des Lemmas. Es sei

$$(6.7) \qquad \alpha_i := \sum_{k=i}^{\infty} 2/q^{N+4(k-1)} \quad (i \in \mathbf{N}).$$

Wegen $q \leqq q(2) < q$ hat man

$$q^3-q^2-q-1 < q^3-2q^2+q-1 \leqq 0,$$

woraus $2q^3/(q^4-1) < L$ folgt. Aus (6.7) ergibt sich nun

$$(6.8) \qquad \alpha_i = 2q^3/q^{N+4(i-1)-1}(q^4-1) < L/q^{N+4(i-1)-1} \quad (i \in \mathbf{N}).$$

Definitionsgemäss gilt

$$(6.9) \qquad \alpha_i = 2/q^{N+4(i-1)}+\alpha_{i+1} \quad (i \in \mathbf{N})$$

und wegen (6.8)

$$\alpha_i^* := 1/q^{N+4(i-1)}+\alpha_{i+1} = \alpha_i - 1/q^{N+4(i-1)} <$$

$$< L/q^{N+4(i-1)-1} - 1/q^{N+4(i-1)} = (Lq-1)/q^{N+4(i-1)} = L/q^{N+4(i-1)},$$

woraus wir wegen Satz 5.1. die Darstellung

$$\alpha_i^* = \sum_{k=N+4(i-1)+1} \varepsilon_k/q^k \quad (\varepsilon_k \in \{0, 1\})$$

entnehmen, d.h. wegen der Volladditivität von $\hat{F}$ und wiederum wegen Satz 5.1. gilt

$$\hat{F}(\alpha_i) = \hat{F}(1/q^{N+4(i-1)}+\alpha_i^*) = \hat{F}(1/q^{N+4(i-1)})+\hat{F}(\alpha_i^*) =$$
$$= \hat{F}(1/q^{N+4(i-1)})+\hat{F}(1/q^{N+4(i-1)}+\alpha_{i+1}) = 2\hat{F}(1/q^{N+4(i-1)})+\hat{F}(\alpha_{i+1}).$$

Aus der vorigen Gleichung erhalten wir

$$\hat{F}(\alpha_i) = 2a_{N+4(i-1)}+\hat{F}(\alpha_{i+1}) \quad (i\in\mathrm{N}). \tag{6.10}$$

Aus (6.10) erhalten wir mittels Induktion ($\alpha_1=\alpha$) für beliebiges $K\in\mathrm{N}$

$$\hat{F}(\alpha) = 2\sum_{i=1}^{k} a_{N+4(i-1)}+\hat{F}(\alpha_{K+1}),$$

woraus für $K\to\infty$ wegen der Stetigkeit von $\hat{F}$ im Nullpunkt

$$\hat{F}(\alpha) = 2\sum_{i=1}^{\infty} a_{N+4(i-1)} = 2\hat{F}(\alpha/2)$$

folgt. Für β verläuft der Beweis ganz ähnlich.

Fortsetzung des Beweises des Satzes. Mit Rücksicht auf das Lemma folgt aus (6.6)

$$\hat{F}(\alpha)+\hat{F}(\beta) = 2\hat{F}(\alpha/2)+2\hat{F}(\beta/2) = 2\hat{F}(\xi).$$

Anderseits gelten nach der Definition von ξ die Ungleichungen $\hat{F}(\alpha)<\hat{F}(\xi)$ und $\hat{F}(\beta)<\hat{F}(\xi)$, womit wir auf einen Widerspruch gestossen sind. Es gilt also $P=\emptyset$, und daraus folgt $\hat{F}(x)\leqq 0$ für alle $x\in[0, L]$. Indem wir diesen Gedankengang für $-\hat{F}$ wiederholen, erhalten wir $-\hat{F}(x)\leqq 0$ und somit gilt $\hat{F}(x)=0$ für jedes $x\in[0, L]$. Hieraus folgt nun wegen (6.1) die Behauptung des Satzes.

Literatur

[1] Z. Daróczy, A. Járai, I. Kátai, On functions defined by digits of real numbers, *Acta Math. Hung.*, in print.

(Z. D. und A. J.)
MATHEMATISCHES INSTITUT
L. KOSSUTH UNIVERSITÄT
PF. 12
4010 DEBRECEN, UNGARN

(I. K.)
MATHEMATISCHES INSTITUT
L. EÖTVÖS UNIVERSITÄT
MÚZEUM KRT. 6—8
1088 BUDAPEST, UNGARN

Canonical number systems in $Q(\sqrt[3]{2})$

S. KÖRMENDI

1. Let us given an algebraic number field $Q(\gamma)$ defined as a simple extension of the rational number field determined by γ. Let $S[\gamma]$ denote the ring of the integers in $Q(\gamma)$.

We shall say that an algebraic integer $\varrho \in S[\gamma]$ is the base of a full radix representation in $S[\gamma]$, if every $\alpha \in S[\gamma]$ can be written in the form

$$\alpha = \sum_{k=0}^{m} a_k \varrho^k, \tag{1.1}$$

where the digits a_k are nonnegative integers such that $0 \leqq a_k < N = |\mathrm{Norm}\,(\varrho)|$.

The largest set that we could hope to represent in the form (1.1) is the ring $Z[\varrho]$, i.e. the polynomials in ϱ with rational integer coefficients. The reason that the norm N yields the correct number of digits is due to the fact that the quotient ring $Z[\varrho]/\varrho$ is isomorphic to Z_N by the map which takes a polynomial in ϱ to its constant term modulo N.

Any such radix representation is unique. Let $P(X)$ denote the minimum polynomial of ϱ. Since ϱ is an integer in $S[\gamma]$, therefore the coefficients of $P(X)$ are rational integers, the constant term of $P(X)$ is $\pm N$. Suppose $A(X), B(X) \in Z[X]$ are polynomials whose coefficients are integers in the range from 0 to $N-1$. If $A(\varrho)$ and $B(\varrho)$ represent the same element of $Z[\varrho]$, then $A(X)-B(X)$ is in the ideal generated by $P(X)$ in $Z[X]$. Since the coefficients of $A(X)-B(X)$ are in the interval $[-N+1, N-1]$ and the constant term of $P(X)$ is $\pm N$, therefore $A(X)-B(X)$ must be the zero polynomial, i.e. $A(X)$ and $B(X)$ have the same coefficients.

I. KÁTAI and J. SZABÓ [1] proved that the only numbers which are suitable bases for all the Gaussian integers, using $0, 1, \ldots, N-1$ as digits, are $-n \pm i$ where n is a positive integer, $N = n^2+1$ is the norm of $-n \pm i$. Their work was generalized by I. KÁTAI and B. KOVÁCS [2], [3], namely they determined all the bases for quad-

Received April 20, 1984.

ratic number fields, using natural numbers as digits. Similar results have been achieved by W. GILBERT [4], independently.

B. KOVÁCS [5] gave a necessary and sufficient condition for the existence of number base in algebraic number fields. Namely he proved: If $Q(\gamma)$ is an extension of degree n of Q, then there exists a number base in $S[\gamma]$ if and only if there exists a $\vartheta\in S[\gamma]$ such that $\{1, \vartheta, \dots, \vartheta^{n-1}\}$ is an integer-base in $S[\gamma]$.

However, the determination of all the number bases in algebraic number fields seems to be a quite hard problem. Our purpose in this paper is to determine all the number bases in $Q[\sqrt[3]{2}]$. This is the simplest case that has not been considered until now. We hope to extend our investigation for all cubic fields.

2. Let $\sigma=\sqrt[3]{2}$, and let $K(X)=X^3-2$ be the minimum polynomial of σ. We shall use some lemmas.

Lemma 1. *Let $\alpha=a+b\sigma+c\sigma^2$ with $a, b, c\in Q$, and let $E_1=-3a$, $E_2=3(a^2-2bc)$, $E_3=-(a^3+2b^3+4c^3-6abc)$. Then α is a root of the polynomial $T(X)=X^3+E_1X^2+E_2X+E_3$.*

Proof. Let $\xi=\exp(2\pi i/3)$ be one of the cubic roots of unity, and let $\alpha_1=\alpha$, $\alpha_2=a+b\xi\sigma+c\xi^2\sigma^2$, $\alpha_3=a+b\xi^2\sigma+c(\xi^2\sigma)^2$ be the conjugates of α. Expanding the product $(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ we get immediately that this is $T(X)$.

Lemma 2. *$\{1, \sigma, \sigma^2\}$ is an integer base, i.e. $\alpha=a+b\sigma+c\sigma^2$ is an integer in $Q(\sigma)$ if and only if a, b, c are rational integers.*

Proof. This is well known.

Lemma 3. *Let $\alpha\in S[\sigma]$ $\{1, \alpha, \alpha^2\}$ is an integer basis if and only if $\alpha=M\pm\sigma$, or $\alpha=M\pm(\sigma+\sigma^2)$ with a rational integer M.*

Proof. Let $\alpha=a+b\sigma+c\sigma^2$. Then $\alpha^2=(a^2+4bc)+(2ab+2c^2)\sigma+(2ac+b^2)\sigma^2$. The matrix A of the basis transformation $[1, \sigma, \sigma^2]\to[1, \alpha, \alpha^2]$ has the form

$$A=\begin{bmatrix} 1 & 0 & 0 \\ a & b & c \\ a^2+4bc & 2ab+2c^2 & 2ac+b^2 \end{bmatrix}.$$

det $A=\pm 1$ if and only $b^3-2c^3=\pm 1$. It is well known, see e.g. [6], that all the solutions of this Diophantine equation are:

$$(b,\ c)=(1,0),\ (-1,0),\ (1,1),\ (-1,1). \tag{2.1}$$

Let B denote the set of the number bases in $Q(\sigma)$.

Lemma 4. *If $\alpha\in B$, then $\{1, \alpha, \alpha^2\}$ is an integer base.*

Proof. Obvious.

Lemma 5. *Let $\vartheta \in S[\sigma]$ be such that $\{1, \vartheta, \vartheta^2\}$ is an integer basis. Let the minimum polynomial $T(X)=X^3+E_1X^2+E_2X+E_3$ of ϑ satisfy the conditions $1 \leqq E_1 \leqq E_2 \leqq E_3$, $E_3 \geqq 2$. Then $\vartheta \in B$.*

Proof. See [4].

Lemma 6. *If $\vartheta \geqq -1$, $\vartheta \in S[\sigma]$, then $\vartheta \notin B$.*

Proof. Let H_ϑ denote the set of those numbers α that can be written in the form

$$\alpha = a_0+a_1\vartheta+\ldots+a_k\vartheta^k$$

with suitable digits $a_j \in [0, |N(\vartheta)|-1]$. If $\vartheta \geqq 0$, then $H_\vartheta \subseteqq [0, \infty)$, and so -1 cannot be represented. If $\vartheta=-1$, then $|N(\vartheta)|=1$, $a_j=0$, and so $H_\vartheta=\{0\}$. If $|\vartheta|<1$ and $\alpha \in H_\vartheta$, then

$$|\alpha| \leqq a_0+a_1|\vartheta|+\ldots+a_k|\vartheta|^k \leqq (|N(\vartheta)|-1)|\vartheta|/(|\vartheta|-1),$$

consequently H_ϑ is a bounded subset of the real numbers. Since $Z[\vartheta]$ is not bounded, the proof is finished.

Lemma 7. *Let $T(X)=X^3+E_1X^2E_2X+E_3$ be the minimum polinomial of α, and let $\gamma=(E_2+E_1+1)+(E_1+1)+\alpha^2$. Then $(1-\alpha)\gamma=T(1)$. Consequently, if $|T(1)|<$ <1, then γ or $-\gamma$ cannot be represented in the form $r_0+r_1\alpha+\ldots+r_k\alpha^k$, $r_i \in \{0, 1, \ldots,$ $\ldots, |N(\alpha)|-1\}$, i.e. $\alpha \notin B$.*

Proof. The assertion $T(1)=(1-\alpha)\gamma$ is obvious. Let $c=\operatorname{sgn} T(1)$. Then

$$c\gamma = cT(1)+(c\gamma)\alpha, \quad cT(1) \in \{0, \ldots, |N(\alpha)|-1\}.$$

Let us assume in contrary that c has a representation in the form

$$c\gamma = r_0+r_1\alpha+\ldots+r_k\alpha^k.$$

Then $r_0=cT(1)$, $c\gamma=r_1+r_2\alpha+\ldots+r_k\alpha^{k-1}$. Repeating this procedure we get that $cT(1)=r_0=r_1\ldots=r_k$, $c\gamma=0$, which does not hold.

3. From Lemmas 3 and 4 it follows that if $\alpha \in B$, then $\alpha=M\pm\sigma$ or $\alpha=$ $=M\pm(\sigma+\sigma^2)$. Let $T(X)=X^3+E_1X^2+E_2X+E_3$ be the minimum polynomial of α. Let us consider the table below.

α	E_1	E_2	E_3	Conditions of Lemma 5 are satisfied if
$M+\sigma$	$-3M$	$3M^2$	M^3+2	$M \leqq -4$
$M-\sigma$	$-3M$	$3M^2$	M^3-2	$M \leqq -3$ or $M=-1$
$M+\sigma+\sigma^2$	$-3M$	$3(M^2-2)$	M^3-6M+6	$M \leqq -5$
$M-\sigma-\sigma^2$	$-3M$	$3(M^2-2)$	M^3-6M-6	$M \leqq -4$

The numbers α satisfying the conditions stated in the last column belong to B.

From Lemma 7 we get that $\alpha\notin B$ if $\alpha\geqq -1$, i.e. if

$$\begin{aligned}
\alpha &= M+\sigma && \text{and } M\geqq -2,\\
\alpha &= M-\sigma && \text{and } M\geqq 1,\\
\alpha &= M+\sigma+\sigma^2 && \text{and } M\geqq -3,\\
\alpha &= M-\sigma-\sigma^2 && \text{and } M\geqq 2.
\end{aligned}$$

It remains to consider the following set of integers $\alpha_1, \dots, \alpha_9$, the minimum polynomials of which are denoted by $T_1(X), \dots, T_9(X)$, resp.

	α	$T(X)$	$N(\alpha)$
1	$-3+\sigma$	$X^3+9X^2+27X+25$	25
2	$-2-\sigma$	$X^3+6X^2+12X+10$	10
3	$-\sigma$	X^3+2	2
4	$-4+\sigma+\sigma^2$	$X^3+12X^2+42X+34$	34
5	$-3-\sigma-\sigma^2$	$X^3+9X^2+21X+15$	15
6	$-2-\sigma-\sigma^2$	X^3+6X^2-6X+2	2
7	$-1-\sigma-\sigma^2$	X^3+3X^2-3X+1	1
8	$-\sigma-\sigma^2$	X^3-6X+6	6
9	$1-\sigma-\sigma^2$	$X^3-3X^2-3X+11$	11

Lemma 8. *We have* $\alpha_6, \alpha_7, \alpha_8, \alpha_9\notin B$.

Proof. The conditions of Lemma 7 hold for $\alpha_6, \alpha_8, \alpha_9$. α_7 is a unit, the set of the digits contains only one element, the zero, so $\alpha_7\notin B$.

Lemma 9. $\alpha_3=-\sigma\in B$.

Proof. The set of the allowable digits are $\{0, 1\}$. Let $\alpha_3=\alpha$. First we observe that $-1=1+\alpha^3$, $2=\alpha^3+\alpha^6$. The general form of the integers in $Q(\sigma)$ is $Z= =X_0+X_1\alpha+X_2\alpha^2$, $X_i\in Z$. By the relation $-1=1+\alpha^3$, each Z can be written in the form

$$Z=Y_0+Y_1\alpha+\dots+Y_5\alpha^5 \tag{3.1}$$

with nonnegative integers $Y_0, \dots, Y_5$.

Let now $Z^0\neq 0$ be an arbitrary integer, written in the form (3.1). We shall define the following algorithm:

$$t(Z^0):=Y_0+Y_1+\dots+Y_5;\quad h=[Y_0/2],\quad l=Y_0-2[Y_0/2]\in\{0, 1\}.$$
$$Z^{(1)}=Y_1+Y_2\alpha+(Y_3+h)\alpha^2+Y_4\alpha^3+Y_5\alpha^4+h\alpha^5.$$

Then $Z^{(0)}=l+\alpha Z^{(1)}$, furthermore

$$t(Z^{(1)})=Y_1+Y_2+(Y_3+h)+Y_4+Y_5+h=t(Z^{(0)})-l. \tag{3.2}$$

Let us continue this procedure with $Z^{(1)}$ instead of $Z^{(0)}$, and so on. We get a sequence $Z^{(1)}, Z^{(2)}, \dots$. We say that the procedure *terminates* if $Z^{(N)}=0$ for a suitable N. It is obvious that $\alpha\in B$, if the procedure terminates for every Z. Let us assume in contrary that there exists a Z for which it does not terminate. Since the sequence $t(Z^{(\nu)})$ the values of the members of which are positive integers, is monotonically decreasing, we get that $t(Z^{(N)})=t(Z^{(N+1)})=\dots=m>0$. From (3.2) we get that $\alpha Z^{(N+j+1)}= =Z^{(N+j)}$ $(j=0, 1, 2, \dots)$, i.e. α^k divides $Z^{(N)}$ for every positive integer k, which implies that $Z^{(N)}=0$, contrary to our assumption.

4. It remains to consider the cases $\alpha_1, \alpha_2, \alpha_4, \alpha_5$. We shall prove that the question whether they belong to B can be decided by a finite amount of computations.

Let $\alpha\in Q[\sigma]$, $\alpha=a+b\sigma+c\sigma^2$, $A=\{0, 1, \dots, |N(\alpha)|-1\}$. For $\gamma\in Q[\sigma]$ the algorithm

$$\gamma_i=\alpha\gamma_{i+1}+r_i, \quad r_i\in A, \quad \gamma_0=\gamma \tag{4.1}$$

is well defined. Let

$$\gamma_i=\xi^{(i)}+\eta^{(i)}\sigma+\zeta^{(i)}\sigma^2, \quad \Gamma_i=\begin{bmatrix}\xi^{(i)}\\ \eta^{(i)}\\ \zeta^{(i)}\end{bmatrix}, \quad \mathbf{e}=\begin{bmatrix}1\\0\\0\end{bmatrix}.$$

Let A denote the matrix that describes the multiplication by α in the base $1, \sigma, \sigma^2$, i.e. for which

$$\Gamma_i=A\Gamma_{i+1}+r_i\mathbf{e} \tag{4.2}$$

holds.

From (4.2) we get that

$$\Gamma_{i+1}=A^{-1}\Gamma_i-r_iA^{-1}\mathbf{e} \quad (i=0, 1, 2, \dots), \tag{4.3}$$

where A^{-1} has the following explicit form:

$$A^{-1}=\frac{1}{N(\alpha)}\begin{bmatrix}a^2-2bc & 2b^2-2ac & 4c^2-2ab\\ 2c^2-ab & a^2-2bc & 2b^2-2ac\\ b^2-ac & 2c^2-ab & a^2-2bc\end{bmatrix}. \tag{4.4}$$

The algorithm $\gamma_i\to\gamma_{i+1}$ terminates if $\gamma_N=0$ for a suitable N, i.e. if $\Gamma_N=0$ in (4.3). Let $\|\cdot\|$ be a vector norm for which, with the corresponding matrix norm,

$$\|A^{-1}\|=\varkappa<1 \tag{4.5}$$

is satisfied. From (4.3) we get that

$$\Gamma_{i+N}=(A^{-1})^N\Gamma_i-\sum_{k=0}^{N-1} r_{i+k}(A^{-1})^{N-k+1}(A^{-1}\mathbf{e}), \tag{4.6}$$

and hence that

(4.7) $$\|\Gamma_{i+N}\| \leqq \varkappa^N \|\Gamma_i\| + (|N(\alpha)|-1)\|A^{-1}e\|(\varkappa/(1-\varkappa)).$$

From (4.7) we get immediately that the sequence $\Gamma_0, \Gamma_1, \dots$ is bounded for every Γ_0.

Let us assume that there exists a γ which cannot be represented in the base α. Then (4.3) does not terminate. Since any bounded domain contains only a finite number of vectors with integer entries, we get that (4.3) is cyclic. From (4.7) we get that

(4.8) $$\limsup_N \|\Gamma_N\| \leqq (|N(\alpha)|-1)\|A^{-1}e\|(\varkappa/(1-\varkappa)).$$

Furthermore, the integer γ_N corresponding to Γ_N cannot be represented in the base α.

So we have proved the following assertion. Let $\varepsilon>0$, and let S_ε be the set of those γ for which

$$\|\Gamma\| \leqq (|N(\alpha)|-1)\|A^{-1}e\|(\varkappa/(1-\varkappa))+\varepsilon =: L+\varepsilon,$$

$\Gamma=\Gamma(\gamma)$ holds. If $\alpha\notin B$, then there exists a $\gamma\in K_\varepsilon$ which cannot be written in the base α.

Furthermore, if $\|\Gamma_i\| \leqq L/(1-\varkappa)$, then $\|\Gamma_{i+1}\| \leqq L/(1-\varkappa)$, which is an obvious consequence of (4.7). This implies that the number of arithmetical operations that needs to be executed to determine the whole periodic sequence $\Gamma_0, \Gamma_1, \dots$ is finite.

By using the spectral norm for the matrices A_i corresponding to α_i, we get by an easy computation that

$$\|A_1^{-1}\|_S \approx 0{,}63, \quad \|A_2^{-1}\|_S \approx 0{,}75, \quad \|A_4^{-1}\|_S \approx 0{,}97, \quad \|A_5^{-1}\|_S \approx 0{,}75,$$

i.e. the condition (4.5) holds.

5. So we have proved the following

Theorem. *The question whether the integers* $\alpha_1=-3\sigma$, $\alpha_2=-2-\sigma$, $\alpha_4=-4+\sigma+\sigma^2$, $\alpha_5=-3-\sigma-\sigma^2$ *do or do not belong to B can be decided by executing a finite number of arithmetical operations. All the remaining elements of B are the following integers:*

(a) $\alpha = M+\sigma,\quad M\leqq -4,$

(b) $\alpha = M-\sigma,\quad M\leqq -3$ *or* $M=-1$ *or* $M=0,$

(c) $\alpha = M+\sigma+\sigma^2,\quad M\leqq -5,$

(d) $\alpha = M-\sigma-\sigma^2,\quad M\leqq -4.$

References

[1] I. KÁTAI, J. SZABÓ, Canonical number systems for complex integers, *Acta Sci. Math.*, **37** (1975), 255—260.

[2] I. KÁTAI, B. KOVÁCS, Canonical number systems in imaginary quadratic fields, *Acta Math. Hung.*, **37** (1981), 159—164.

[3] I. KÁTAI, B. KOVÁCS, Kanonische Zahlensysteme in der Theorie der quadratischen algebrischen Zahlen, *Acta Sci. Math.*, **42** (1980), 99—107.

[4] B. KOVÁCS, Canonical number systems in algebraic number fields, *Acta Math. Hung.*, **37** (1981), 405—407.

[5] W. GILBERT, Radix representations of quadratic fields, *J. Math. Anal. Appl.*, **83** (1981), 264—274.

[6] W. SIERPINSKI, *Elementary theory of numbers* (Warsawa, 1964).

DEPARTMENT OF COMPUTER SCIENCE
EÖTVÖS LORÁND UNIVERSITY
BOGDÁNFY ÚT 10/B
1117 BUDAPEST, HUNGARY

Acta Sci. Math., 50 (1986), 359—363

On measurable functions with a finite number of negative squares

Z. SASVÁRI

To Professor Heinz Langer on the occassion of his 50th birthday

1. Introduction

The complex-valued function f defined on the interval $(-2a, 2a)$, $0<a\leqq\infty$, is called Hermitian if $f(-x)=\overline{f(x)}$ for every $x\in(-2a, 2a)$. Let $\varkappa$ be a nonnegative integer. The Hermitian function f is said to have $\varkappa$ negative squares if the matrix

(1) $$\left(f(x_i-x_j)\right)_{i,j=1}^{n}$$

has at most $\varkappa$ negative eigenvalues for any choice of n and $x_1, \ldots, x_n\in(-a, a)$, and for some choice of n and $x_1, \ldots, x_n$ the matrix (1) has exactly $\varkappa$ negative eigenvalues. Denote by $\mathfrak{P}^c_{\varkappa;a}$ ($\mathfrak{P}^m_{\varkappa;a}$) the class of all Hermitian functions defined on $(-2a, 2a)$ which are continuous (measurable, respectively) and which have $\varkappa$ negative squares.

In [1] the question was raised if $f\in\mathfrak{P}^m_{\varkappa;a}$ implies that f is locally bounded on $(-2a, 2a)$. The aim of this note is to answer this question in the affirmative (Theorem 1). Therefore in [1] in the definition of $\mathfrak{P}^m_{\varkappa;a}$ the condition of local boundednes of f can be dropped. We mention that an arbitrary positive definite function f (that is $\varkappa=0$) is bounded. If, however, $\varkappa>0$, then there exist nonmeasurable functions with $\varkappa$ negative sguares which are unbounded on each subinterval of $(-2a, 2a)$, see [1].

As a consequence of Theorem 1, of the decomposition result in [1] and of [3, Theorem 2] we show that an arbitrary function $f\in\mathfrak{P}^m_{\varkappa;a}$ has at least one continuation in $\mathfrak{P}^m_{\varkappa;\infty}$ (Theorem 3). An extension of Theorem 1 to locally compact groups is given in Section 3. A survey and a bibliography on functions with a finite number of negative squares can be found in [4].

Received April 28, 1984.

2. The main result

Theorem 1. *If $f\in\mathfrak{P}^m_{\varkappa;a}$ then f is locally bounded on $(-2a, 2a)$.*

Proof. We show that f is bounded on every interval $I_\delta=[-2a+\delta, 2a-\delta]$, $0<\delta<a$. For $c>0$ the function $f+c$ has at most $\varkappa$ negative squares. Therefore we can suppose that $f(0)>0$. If $K>0$, define

$$S_K f=\{t\in I\colon\ |f(t)|<K\}.$$

The sets $S_K f$ are measurable and we have

$$\lim_{K\to\infty}\lambda(S_K f)=4a$$

where λ denotes the Lebesgue measure. If f is not bounded on I_δ then there exists a sequence $\{t_n\}_1^\infty\subset I_\delta$ with $|f(t_n)|\to\infty$. Let $K>0$ be such that

(2) $$\lambda(S_K f)>4a-\delta/\varkappa^3 \quad\text{and}\quad 0\in S_K f.$$

We show that for every $n=1,2,\ldots$ there exist elements $x_1^{(n)},\ldots,x_{\varkappa+1}^{(n)}$ with the following properties:

(3) $$x_i^{(n)}\in[-\delta/2,\delta/2]=J_\delta \quad\text{for}\quad i=1,\ldots,\varkappa+1 \quad\text{and}\quad x_1^{(n)}=0,$$

(4) $$x_i^{(n)}-x_j^{(n)}\in S_K f \quad\text{for}\quad i,j=1,\ldots,\varkappa+1,$$

(5) $$x_i^{(n)}-x_j^{(n)}+t_n\in S_K f \quad\text{for}\quad i,j=1,\ldots,\varkappa+1,\quad i\neq j.$$

Let $x_1^{(n)}=0$, and suppose that $x_1^{(n)},\ldots,x_l^{(n)}$, $1\leqq l<\varkappa+1$, have been found such that (3), (4) and (5) hold with $k+1$ replaced by l. For each $i=1,\ldots,l$ we define

$$M_i=(S_K f+x_i^{(n)})\cap J_\delta,\quad N_i=(S_K f+x_i^{(n)}-t_n)\cap J_\delta,\quad Q_i=(S_K f+x_i^{(n)}+t_n)\cap J_\delta.$$

From $|x_i^{(n)}|<\delta/2$, $|x_i^{(n)}\pm t_n|<2a-\delta/2$ and (2) it follows that

$$\Big(\bigcap_{i,j,m=1}^{l}\{(J_\delta\setminus M_i)\cup(J_\delta\setminus N_j)\cup(J_\delta\setminus Q_m)\}\Big)<l^3\delta/\varkappa^3\leqq\delta=\lambda(J_\delta)$$

and so

$$\lambda\Big(\bigcap_{i,j,m=1}^{l}(M_i\cap N_j\cap Q_m)\Big)>0.$$

Let $x_{l+1}^{(n)}$ be an arbitrary element of the set $\bigcap_{i,j,m=1}^{l}(M_i\cap N_j\cap Q_m)$. Then (3), (4) and (5) hold with $\varkappa+1$ replaced by $l+1$. Therefore, for every $n=1,2,\ldots$ we can choose $x_1^{(n)},\ldots,x_{\varkappa+1}^{(n)}$ so that (3), (4) and (5) are satisfied. Now let $z_1^{(n)},\ldots,z_{2\varkappa+2}^{(n)}$ be defined by

$$z_1^{(n)}=x_1^{(n)},\quad z_2^{(n)}=x_1^{(n)}+t_n,\quad z_3^{(n)}=x_2^{(n)},$$

$$z_4^{(n)}=x_2^{(n)}+t_n,\ \ldots,\ z_{2\varkappa+1}^{(n)}=x_{\varkappa+1}^{(n)},\quad z_{2\varkappa+2}^{(n)}=x_{\varkappa+1}^{(n)}+t_n.$$

We consider the matrix

$$A^{(n)} = (a_{ij}^{(n)})_{i,j=1}^{2\varkappa+2} = \big(f(z_i^{(n)} - z_j^{(n)})\big)_{i,j=1}^{2\varkappa+2}.$$

The relations (3), (4) and (5) imply $|a_{2i-1,2i}^{(n)}|=|a_{2i,2i-1}^{(n)}|=|f(t_n)|$, $i=1, \ldots, \varkappa+1$ and $|a_{ij}^{(n)}|<K$ for the other entries of $A^{(n)}$. Using these facts it is easy to see that by setting $D_r^{(n)}=\det (a_{ij}^{(n)})_{i,j=1}^r$, $r=1, \ldots, 2\varkappa+2$, we have

$$\lim_{n\to\infty} D_{2r}^{(n)}/|f(t_n)|^{2r} = (-1)^r, \quad r = 1, \ldots, \varkappa+1,$$

$$\lim_{n\to\infty} D_{2r+1}^{(n)}/|f(t_n)|^{2r} = (-1)^r, \quad r = 1, \ldots, \varkappa,$$

$$D_1^{(n)} > 0.$$

It follows that for n sufficiently large, the signs in the sequence

$$1, D_1^{(n)}, D_2^{(n)}, \ldots, D_{2\varkappa+2}^{(n)}$$

change exactly $\varkappa+1$ times. Consequently, by Frobenius's rule the matrix $A^{(n)}$ has $\varkappa+1$ negative eigenvalues. This is a contradiction to the assumption that f has exactly $\varkappa$ negative squares. The theorem is proved.

Combining Theorem 1 and the decomposition theorem in [1] we have the following

Theorem 2. *Every function $f\in\mathfrak{P}_{\varkappa;a}^m$ admits a unique decomposition*

$$f(t) = f_c(t)+f_s(t) \quad (-2a < t < 2a) \tag{7}$$

such that $f_c\in\mathfrak{P}_{\varkappa;a}^{c}$, $f_s\in\mathfrak{P}_{0;a}^m$ and $f_s(t)=0$ a.e. on $(-2a, 2a)$.

Corollary 1. *If* a *is finite then $f\in\mathfrak{P}_{\varkappa;a}^m$ is bounded on* $(-2a, 2a)$.

Indeed, in the decomposition (7) the function f_c is bounded on $(-2a, 2a)$ according to [2] and f_s is bounded as it is a positive definite function.

Theorem 3. *Let $f\in\mathfrak{P}_{\varkappa;a}^m$ where $0<a<\infty$ and $\varkappa$ is a nonnegative integer. Then there exists a function $\tilde{f}\in\mathfrak{P}_{\varkappa;\infty}^m$ such that*

$$f(t) = \tilde{f}(t) \quad (-2a < t < 2a).$$

Proof. By Theorem 2 the function f admits a decomposition

$$f(t) = f_c(t)+f_s(t) \quad (-2a < t < 2a)$$

such that $f_c\in\mathfrak{P}_{\varkappa;a}^c$, $f_s\in\mathfrak{P}_{0;a}^m$ and $f_s(t)=0$ a.e. on $(-2a, 2a)$. In [2] it was shown that f_c has an extension $\tilde{f}_c\in\mathfrak{P}_{\varkappa;\infty}^c$, and by Theorem 2 in [3] f_s has an extension $\tilde{f}_s\in\mathfrak{P}_{\varkappa;\infty}^m$. If we set $\tilde{f}=\tilde{f}_c+\tilde{f}_s$ we have $\tilde{f}\in\mathfrak{P}_{\varkappa;\infty}^m$ and $f(t)=\tilde{f}(t)$ $(-2a<t<2a)$.

3. Some remarks

1. Let $\varkappa$ again be a nonnegative integer. The definition of a function with $\varkappa$ negative squares can be formulated on a group G as follows. Suppose that f is a complex-valued function defined on a symmetric set $V \subset G$ which contains the unit of G and has the property that $f(g^{-1}) = \overline{f(g)}$ for every $g \in V$. The function f is said to have $\varkappa$ negative squares if the matrix

$$(f(g_i g_j^{-1}))_{i,j=1}^{n} \tag{8}$$

has at most $\varkappa$ negative eigenvalues for any choice of n and $g_1, \ldots, g_n \in V$ for which $g_i g_j^{-1} \in V$ $(i, j = 1, \ldots, n)$, and if for some choice of n and $g_1, \ldots, g_n$ the matrix (8) has exactly $\varkappa$ negative eigenvalues. We denote by $\mathfrak{P}_{\varkappa; V}$ the set of functions on V which have $\varkappa$ negative squares. If G is a locally compact group with Haar measure λ and V is λ-measurable we set

$$\mathfrak{P}_{\varkappa; V}^{m} = \{f \in \mathfrak{P}_{\varkappa; V} \colon f \text{ is } \lambda\text{-measurable on } V\}.$$

It is not hard to see that the arguments in the proof of Theorem 1 can be used in order to show the following result.

Theorem 1′. *Let G be a locally compact group and $f \in \mathfrak{P}_{\varkappa; V}^{m}$ where V is an open symmetric subset of G. Then f is locally bounded, that is, f is bounded on every compact set $K \subset V$.*

2. It follows immediately from Theorem 2 that a function $f \in \mathfrak{P}_{\varkappa; a}^{m}$ with $\varkappa \geqq 1$ cannot vanish almost everywhere on $(-2a, 2a)$. This fact remains valid for functions on a locally compact group. In order to see this we need the following.

Lemma 1. *Let G be an arbitrary group and $f \in \mathfrak{P}_{\varkappa; V}$. If $\varkappa \geqq 1$ then V can be covered with finitely many translates of the support of f.*

Proof. Let $g_1, \ldots, g_n \in V$ be such that the matrix $A = (f(g_i g_j^{-1}))_{i,j=1}^{n}$ has $\varkappa$ negative eigenvalues. Suppose that V cannot be covered with finitely many translates of $\operatorname{Supp} f = \{g \in V \colon f(g) \neq 0\}$. Then there exists a $g \in V$ for which $g \notin g_i (\operatorname{Supp} f) g_j^{-1}$, $i, j = 1, \ldots, n$. Let $t_1, \ldots, t_{2n}$ be defined by

$$t_1 = g_1, \ldots, t_n = g_n, \quad t_{n+1} = g_1 g, \ldots, t_{2n} = g_n g.$$

Then we have

$$B = (f(t_i t_j^{-1}))_{i,j=1}^{2n} = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}.$$

Thus B has $2\varkappa$ negative eigenvalues, a contradiction.

Corollary 2. *Let G be a locally compact group and let* $f\in\mathfrak{P}^m_{\varkappa;V}$ *where* $\lambda(V)>0$. *If* $\varkappa\geqq 1$ *then* f *cannot vanish almost everywhere on* V.

The author is indebted to Professor Heinz Langer for suggesting the problem discussed in this paper and for several helpful discussions.

References

[1] H. Langer, On measurable Hermitian indefinite functions with a finite number of negative squares, *Acta Sci. Math.*, **45** (1983), 281—292.

[2] V. I. Plusčeva, The integral representation of continuous Hermitian-indefinite kernels, *Dokl. Akad. Nauk SSSR*, **145** (1962), 534—537. (Russian)

[3] Z. Sasvári, The extension problem for measurable positive definite functions, *Math. Z.*, **191** (1986), 475—478.

[4] J. Stewart, Positive definite functions and generalizations, an historical survey, *Rocky Mountain J. Math.*, **6** (1976), 409—434.

SEKTION MATHEMATIK
TECHNISCHE UNIVERSITÄT
MOMMSENSTR. 13
8027 DRESDEN, G.D.R.

Acta Sci. Math., 50 (1986), 365—366

Представление полиномов Лагерра

О. В. ВИСКОВ

Пусть $D = d/dx$ — оператор дифференцирования и

(1) $$L_n^\alpha(x) = (1/n!)e^x x^{-\alpha} D^n[e^{-x}x^{n+\alpha}], \quad n = 0, 1, 2, \dots,$$

— обобщенные полиномы Лагерра (см. [1], 10.12). В настоящей заметке устанавливается справедливость следующего представления для полиномов $L_n^\alpha(x)$:

(2) $$L_n^\alpha(x) = (1/n!)x^{-n}e^x(x^2D+\alpha x+x)^n[e^{-x}].$$

Это соотношение является в известном смысле двойственным к формуле Родрига (1) и установленному в [2] представлению

(3) $$L_n^\alpha(x) = ((-1)^n/n!)e^x(xD^2+\alpha D+D)^n[e^{-x}].$$

Отметим, что представление (3) в частном случае $\alpha = 0$ было доказано Л. Б. Редеи [3].

Доказательство (2) можно было бы провести, опираясь на установленную в [2] операционную лемму и почти дословно следуя использованному там ходу рассуждений (с заменой оператора D оператором умножения на независимую переменную, и наоборот). Однако в настоящей заметке предлагается иное доказательство, основанное на единственности решения задачи Коши, для подходящего уравнения в частных производных.

В самом деле, хорошо известно [1], что

(4) $$\sum_{n \geqq 0} L_n^\alpha(x)t^n = (1-t)^{-\alpha-1}\exp\{xt/(t-1)\}.$$

Кроме того, ясно, что функция

$$u(t, x) = \sum_{n \geqq 0} (t^n/n!)(x^2D+\alpha x+x)^n[e^{-x}]$$

Поступило 5-ого февраля 1984.

дает решение задачи Коши

$$(5)\qquad \frac{\partial u}{\partial t} = x^2\frac{\partial u}{\partial x} + (\alpha+1)xu, \quad u|_{t=0} = e^{-x}.$$

С другой стороны, легко проверяется, что функция

$$u(t, x) = (1-xt)^{-\alpha-1}\exp\{x/(xt-1)\}$$

тоже является решением задачи Коши (5). Поэтому

$$(6)\qquad \sum_{n\geqq 0}(t^n/n!)e^x(x^2D+\alpha x+x)^n[e^{-x}] = (1-xt)^{-\alpha-1}\exp\{x^2t/(xt-1)\}.$$

Сравнение (6) и (4) с учетом (2) завершает доказательство.

Литература

[1] Bateman Manuscript Project, *Higher Transcendental Functions*, vol. 2, McGraw-Hill (New York, 1953).

[2] О. В. Висков, О тождестве Л. Б. Редеи для полиномов Лагерра, *Acta Sci. Math.*, 39 (1977), 27—28.

[3] L. B. Rédei, An identity for Laguerre polynomials, *Acta Sci. Math.*, 37 (1975), 115—116.

МАТЕМАТИЧЕСКИЙ ИНСТИТУТ ИМ. В. А. СТЕКЛОВА АН СССР
УЛ. ВАВИЛОВА 42
МОСКВА 117333, СССР

Acta Sci. Math., 50 (1986), 367—380

Orthonormal systems of polynomials in the divergence theorems for double orthogonal series

F. MÓRICZ*

1. Introduction. Let $(X, \mathscr{F}, \mu)$ be a positive measure space and $\{\varphi_{ik}(x): i, k = 0, 1, \ldots\}$ an orthonormal system (in abbreviation: ONS) defined on X. We will consider the double orthogonal series

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} a_{ik}\varphi_{ik}(x) \tag{1.1}$$

where $\{a_{ik}\}$ is a double sequence of real numbers for which

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} a_{ik}^2 < \infty. \tag{1.2}$$

The rectangular partial sums and (C, α, β)-means of series (1.1) are defined by

$$s_{mn}(x) = \sum_{i=0}^{m}\sum_{k=0}^{n} a_{ik}\varphi_{ik}(x)$$

and

$$\sigma_{mn}^{\alpha\beta}(x) = (1/A_m^\alpha A_n^\beta)\sum_{i=0}^{m}\sum_{k=0}^{n} A_{m-i}^{\alpha-1}A_{n-k}^{\beta-1}s_{ik}(x),$$

respectively, where

$$A_m^\alpha = \binom{m+\alpha}{m} \quad (\alpha > -1, \beta > -1;\ m, n = 0, 1, \ldots).$$

2. Preliminary results: Convergence theorems. The extension of the Rademacher—Menšov theorem proved by a number of authors (see, e.g. [1], [5, Corollary 2], etc.) reads as follows.

Received May 15, 1984.

* This research was conducted while the author was a visiting professor at the Indiana University, Bloomington, Indiana, U.S.A., during the academic year 1983/84, on leave from the University of Szeged, Hungary.

Theorem A. *If*

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} a_{ik}^2[\log(i+2)]^2[\log(k+2)]^2<\infty, \tag{2.1}$$

then series (1.1) *regularly converges a.e.*

In this paper the logarithms are to the base 2.

The convergence behavior improves when considering $\sigma_{mn}^{\alpha\beta}(x)$ with $\alpha\geqq 0$ and $\beta\geqq 0$ instead of $s_{mn}(x)$. The following two extensions of the Menšov—Kaczmarz $(\alpha=1)$ and Zygmund $(\alpha>0)$ theorems were proved in [7].

Theorem *B. If* $\alpha>0$ *and*

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} a_{ik}^2[\log\log(i+4)]^2[\log(k+2)]^2<\infty, \tag{2.2}$$

then series (1.1) *is regularly* $(C, \alpha, 0)$*-summable a.e.*

Theorem C. *If* $\alpha>0$, $\beta>0$, *and*

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} a_{ik}^2[\log\log(i+4)]^2[\log\log(k+4)]^2<\infty, \tag{2.3}$$

then series (1.1) *is regularly* (C, α, β)*-summable a.e.*

The next three theorems give information on the order of magnitude of $s_{mn}(x)$ and $\sigma_{mn}^{\alpha\beta}(x)$, respectively, in the more general setting of (1.2).

Theorem D [6, Corollary 2]. *If condition* (1.2) *is satisfied, then*

$$s_{mn}(x)=o_x\{\log(m+2)\log(n+2)\} \quad \textit{a.e. as} \quad \max(m,n)\to\infty. \tag{2.4}$$

Theorem E [9, Theorem 1]. *If* $\alpha>0$ *and condition* (1.2) *is satisfied, then*

$$\sigma_{mn}^{\alpha 0}(x)=o_x\{\log\log(m+4)\log(n+2)\} \quad \textit{a.e. as} \quad \max(m,n)\to\infty. \tag{2.5}$$

Theorem F [9, Theorem 2]. *If* $\alpha>0$, $\beta>0$, *and condition* (1.2) *is satisfied, then*

$$\sigma_{mn}^{\alpha\beta}(x)=o_x\{\log\log(m+4)\log\log(n+4)\} \quad \textit{a.e. as} \quad \max(m,n)\to\infty. \tag{2.6}$$

3. Preliminary results: Divergence theorems. The conditions (2.1)—(2.3) and statements (2.4)—(2.6) are the best possible.

To see this, from here on let $(X, \mathscr{F}, \mu)$ be the unit square $X=[0, 1]\times[0, 1]$ in $\mathbf{R}^2$, $\mathscr{F}$ the σ-algebra of the Borel measurable subsets, and μ the Lebesgue measure. In the sequel, the unit interval $[0, 1]$ will be denoted by I, the unit square $I\times I$ by S, and the plane Lebesgue measure by $|\cdot|$.

Theorem A′ [10, Theorem 4]. *If* $\{a_{ik}\}$ *is a double sequence of numbers for which*

$$|a_{ik}| \geqq \max \{|a_{i+1,k}|, |a_{i,k+1}|\} \quad (i, k = 0, 1, \ldots) \tag{3.1}$$

and

$$\sum_{i=0}^{\infty} \sum_{k=0}^{\infty} a_{ik}^2 [\log (i+2)]^2 [\log (k+2)]^2 = \infty, \tag{3.2}$$

then there exists a uniformly bounded double ONS $\{\varphi_{ik}(x_1, x_2)\}$ *of step functions on* S *such that*

$$\limsup |s_{mn}(x_1, x_2)| = \infty \quad \textit{a.e. as} \quad \min (m, n) \to \infty. \tag{3.3}$$

A function φ is said to be a step function on S if S can be represented as a finite union of disjoint rectangles with sides parallel to the coordinate axes, and φ is constant on each of these rectangles.

Remark 1. As a matter of fact, (3.3) was proved in [10] under (3.1) and the stronger condition that for all pairs of i_0 and k_0

$$\sum_{i=i_0}^{\infty} \sum_{k=k_0}^{\infty} a_{ik}^2 [\log (i+2)]^2 [\log (k+2)]^2 = \infty. \tag{3.2′}$$

Assume (3.2′) is not satisfied for a certain pair of i_0 and k_0, but (3.2) is. Then either

$$\sum_{i=0}^{\infty} \sum_{k=0}^{k_0-1} a_{ik}^2 [\log (i+2)]^2 = \infty$$

or

$$\sum_{i=0}^{i_0-1} \sum_{k=0}^{\infty} a_{ik}^2 [\log (k+2)]^2 = \infty.$$

Now, it is a routine to construct an ONS $\{\varphi_{ik}(x_1, x_2)\}$ such that

$$\limsup s_{mn}(x_1, x_2) = \infty \quad \text{a.e. as} \quad m \to \infty \quad \text{and} \quad n = k_0 - 1, \quad \text{or} \\ m = i_0 - 1 \quad \text{and} \quad n \to \infty. \tag{3.3′}$$

On the other hand, since (3.2′) is not satisfied, by Theorem A the truncated series

$$\sum_{i=i_0}^{\infty} \sum_{k=k_0}^{\infty} a_{ik} \varphi_{ik}(x_1, x_2) \tag{1.1′}$$

regularly converges a.e. Consequently, the divergence expressed in (3.3′) cannot be spoilt as $\min (m, n) \to \infty$ and this is (3.3) to be shown.

Remark 2. In particular, it follows from Theorem A′ that $\log (n+2)$ cannot be replaced in condition (2.1) by any sequence $\varrho(n)$ tending to ∞ slower than $\log (n+2)$ as $n \to \infty$. Similar observation pertains to Theorems B′ and C′ below.

Theorem B′ [11, Theorem 2]. *Set*

$$A_{-2,k} = |a_{0k}|, \quad A_{-1,k} = |a_{1k}|, \quad A_{pk} = \Big\{\sum_{i=2^p+1}^{2^{p+1}} a_{ik}^2\Big\}^{1/2} \quad (p, k = 0, 1, \ldots).$$

If

$$A_{pk} \geqq \max\{A_{p+1,k}, A_{p,k+1}\} \quad (p = -2, -1, 0, \ldots; \; k = 0, 1, \ldots)$$

and

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} a_{ik}^2 [\log\log(i+4)]^2 [\log(k+2)]^2 = \infty,$$

then there exists a double ONS $\{\varphi_{ik}(x_1, x_2)\}$ *of step functions on S such that*

$$\limsup |\sigma_{mn}^{10}(x_1, x_2)| = \infty \quad a.e. \text{ as } \quad \min(m, n) \to \infty.$$

Making the convention that for $p=-2$ and -1 by 2^p we mean -1 and 0, respectively, the definition of the A_{pk} can be unified as

$$A_{pk} = \Big\{\sum_{i=2^p+1}^{2^{p+1}} a_{ik}^2\Big\}^{1/2} \quad (p = -2, -1, 0, \ldots; \; k = 0, 1, \ldots).$$

Theorem C′ [12, Theorem 1]. *Set*

$$A_{pq}^* = \Big\{\sum_{i=2^p+1}^{2^{p+1}} \sum_{k=2^q+1}^{2^{q+1}} a_{ik}^2\Big\}^{1/2} \quad (p, q = -2, -1, 0, \ldots).$$

If

$$A_{pk}^* \geqq \max\{A_{p+1,k}^*, A_{p,k+1}^*\} \quad (p = -2, -1, 0, \ldots; \; k = 0, 1, \ldots)$$

and

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} a_{ik}^2 [\log\log(i+4)]^2 [\log\log(k+4)]^2 = \infty,$$

then there exists a double ONS $\{\varphi_{ik}(x_1, x_2)\}$ *of step functions on S such that*

$$\limsup |\sigma_{mn}^{11}(x_1, x_2)| = \infty \quad a.e. \text{ as } \quad \min(m, n) \to \infty.$$

The divergence theorems corresponding to Theorems D, E and F will be stated in Section 5.

4. Main results. Following the arguments due to MENŠOV [4] and LEINDLER [3], we can conclude an approximation theorem for double ONS of L^2-functions by double orthonormal systems of polynomials (in abbreviation: ONSP) in x_1 and x_2. This theorem can be considered an extension of [3, Theorem 1] from single to double ONS.

Theorem 1. *Let* $\{\varphi_{ik}(x_1, x_2)\colon i, k=0, 1, \ldots\}$ *be a double* ONS *on S,* $\{\varepsilon_{rs}\colon r, s=1, 2, \ldots\}$ *a double sequence of positive numbers,* $\{M_r\colon r=1, 2, \ldots\}$ *and* $\{N_s\colon s=1, 2, \ldots\}$ *two strictly increasing sequences of nonnegative integers. Then there exist a double* ONSP $\{P_{ik}(x_1, x_2)\colon i, k=0, 1, \ldots\}$ *on S and a double sequence*

$\{E_{rs}: r, s=1, 2, \ldots\}$ *of measurable subsets of* S *such that the following properties are satisfied:*

(i) $|E_{rs}| \leqq \varepsilon_{rs}$ $(r, s=1, 2, \ldots)$;

(ii) *For every* $(x_1, x_2) \in S \setminus E_{rs}$, *and for every* $M_{r-1} < i \leqq M_r$ *and* $N_{s-1} < k \leqq N_s$,

$$|\varphi_{ik}(x_1, x_2) - (-1)^{j_{rs}(x_1, x_2)} P_{ik}(x_1, x_2)| \leqq \varepsilon_{rs} \tag{4.1}$$
$$(r, s = 1, 2, \ldots;\ M_0 = N_0 = -1).$$

where $j_{rs}(x_1, x_2)$ *equals* 0 *or* 1 *depending on* r, s, x_1, *and* x_2, *but not depending on* i *and* k;

(iii) *If the functions* φ_{ik} *are (not necessarily uniformly) bounded on* S, *then*

$$\max_{(x_1, x_2) \in S} |P_{ik}(x_1, x_2)| \leqq 2\Big\{\sup_{(x_1, x_2) \in S} |\varphi_{ik}(x_1, x_2)| + 1\Big\} \quad (i, k = 0, 1, \ldots).$$

Remark 3. If the φ_{ik} are bounded, in particular, step functions on S, then it suffices to require that the functions φ_{ik} are orthonormal only in each block $M_{r-1} < i \leqq M_r$ and $N_{s-1} < k \leqq N_s$ $(r, s=1, 2, \ldots)$, but not altogether.

Remark 4. If in each block $M_{r-1} < i \leqq M_r$ and $N_{s-1} < k \leqq N_s$ the φ_{ik} can be represented in a product form, i.e.

$$\varphi_{ik}(x_1, x_2) = \varphi_i^{(1,r)}(x_1)\, \varphi_k^{(2,s)}(x_2) \tag{4.2}$$

where both $\{\varphi_i^{(1,r)}(x_1): M_{r-1} < i \leqq M_r\}$ and $\{\varphi_k^{(2,s)}(x_2): N_{s-1} < k \leqq N_s\}$ are bounded orthonormal functions on I $(r, s=1, 2, \ldots)$, then the resulting P_{ik} can also be taken in the product form

$$P_{ik}(x_1, x_2) = P_i^{(1,r)}(x_1)\, P_k^{(2,s)}(x_2) \tag{4.3}$$

in each block $M_{r-1} < i \leqq M_r$ and $N_{s-1} < k \leqq N_s$, where both $\{P_i^{(1,r)}(x_1): M_{r-1} < i \leqq M_r\}$ and $\{P_k^{(2,s)}(x_2): N_{s-1} < k \leqq N_s\}$ are orthonormal polynomials on I $(r, s = 1, 2, \ldots)$.

The above approximation theorem enables us to strengthen Theorems A′, B′, and C′ in the same sense as it was done by Leindler [3, Theorems A and G] in the case of single ONS. Namely, if there exists a double ONS for which such and such a series or sequence diverges a.e., then there exists a double ONSP which exhibits this divergence phenomenon.

Theorem 2. *In each of Theorems* A′, B′ *and* C′ *the double* ONS $\{\varphi_{ik}(x_1, x_2)\}$ *can be replaced by a double* ONSP $\{P_{ik}(x_1, x_2)\}$ *of the form* (4.3).

5. Immediate consequences of Leindler's results. Here we cite the main lemma of Leindler [3, Lemma 3] in the form of the following

Theorem G. *Let* $\{\varepsilon_r: r=1, 2, \ldots\}$ *be a sequence of positive numbers,* $\{M_r: r=1, 2, \ldots\}$ *a strictly increasing sequence of nonnegative integers, and*

$\{\varphi_i(x_1): i=0, 1, \ldots\}$ *a system of bounded functions such that the* φ_i *are orthonormal on* I *in each block* $M_{r-1}<i\leqq M_r$ $(r=1, 2, \ldots;\ M_0=-1)$. *Then there exist an* ONSP $\{P_i(x_1): i=0, 1, \ldots\}$ *on* I *and a sequence* $\{E_r: r=1, 2, \ldots\}$ *of measurable subsets of* I *such that the following properties are satisfied:*

$\overline{\text{(i)}}$ $|E_r|\leqq\varepsilon_r$ $(r=1, 2, \ldots;$ *here* $|\cdot|$ *means the linear Lebesgue measure);*

$\overline{\text{(ii)}}$ *For every* $x_1\in I\setminus E_r$ *and for every* $M_{r-1}<i\leqq M_r$,

$$|\varphi_i(x_1)-(-1)^{j_r(x_1)}P_i(x_1)|\leqq\varepsilon_r \quad (r=1, 2, \ldots),$$

where $j_r(x_1)$ *equals* 0 *or* 1 *depending on* r *and* x_1, *but not on* i;

$$\overline{\text{(iii)}} \qquad \max_{x_1\in I}|P_i(x_1)|\leqq 2\{\sup_{x_1\in I}|\varphi_i(x_1)|+1\} \quad (i=0, 1, \ldots).$$

Assume we have two sequences $\{\varepsilon_r^{(1)}: r=1, 2, \ldots\}$ and $\{\varepsilon_s^{(2)}: s=1, 2, \ldots\}$ of positive numbers, two strictly increasing sequences $\{M_r: r=1, 2, \ldots\}$ and $\{N_s: s=1, 2, \ldots\}$ of nonnegative integers, and two systems $\{\varphi_i^{(1)}(x_1): i=0, 1, \ldots\}$ and $\{\varphi_k^{(2)}(x_2): k=0, 1, \ldots\}$ of bounded functions on I with bounds $B_i^{(1)}$ and $B_k^{(2)}$, respectively, such that the $\varphi_i^{(1)}$ are orthonormal on I in each block $M_{r-1}<i\leqq M_r$ $(r=1, 2, \ldots; M_0=-1)$ and the $\varphi_k^{(2)}$ are orthonormal on I in each block $N_{s-1}<k\leqq N_s$ $(s=1, 2, \ldots;\ N_0=-1)$. Applying Theorem G separately to both cases yields two ONSP $\{P_i^{(1)}(x_1): i=0, 1, \ldots\}$ and $\{P_k^{(2)}(x_2): k=0, 1, \ldots\}$, two sequences $\{E_r^{(1)}: r=1, 2, \ldots\}$ and $\{E_r^{(2)}: s=1, 2, \ldots\}$ of measurable subsets of I so that properties $\overline{\text{(i)}}$—$\overline{\text{(iii)}}$ are satisfied, respectively.

It is not hard to verify that the product ONSP given by

$$P_{ik}(x_1, x_2)=P_i^{(1)}(x_1)P_k^{(2)}(x_2) \quad (i, k=0, 1, \ldots)$$

provides an approximation to the product ONS $\{\varphi_{ik}(x_1, x_2)=\varphi_i^{(1)}(x_1)\varphi_k^{(2)}(x_2): i, k=0, 1, \ldots\}$ with the following properties:

$\overline{\overline{\text{(i)}}}$ Setting $E_{rs}=(E_r^{(1)}\times I)\cup(I\times E_s^{(2)})$,

$$|E_{rs}|\leqq\varepsilon_r^{(1)}+\varepsilon_s^{(2)} \quad (r, s=1, 2, \ldots); \tag{5.1}$$

$\overline{\overline{\text{(ii)}}}$ For every $(x_1, x_2)\in S\setminus E_{rs}$, and for every $M_{r-1}<i\leqq M_r$ and $N_{s-1}<k\leqq N_s$,

$$|\varphi_i^{(1)}(x_1)\varphi_k^{(2)}(x_2)-(-1)^{j_r^{(1)}(x_1)+j_s^{(2)}(x_2)}P_i^{(1)}(x_1)P_k^{(2)}(x_2)|\leqq \tag{5.2}$$

$$\leqq\Big(\max_{N_{s-1}<k\leqq N_r}B_k^{(2)}\Big)\varepsilon_r^{(1)}+\Big(\max_{M_{r-1}<i\leqq M_s}B_i^{(1)}\Big)\varepsilon_s^{(2)}+\varepsilon_r^{(1)}\varepsilon_s^{(2)} \quad (r, s=1, 2, \ldots),$$

where both $j_r^{(1)}(x_1)$ and $j_s^{(2)}(x_2)$ equal 0 or 1;

$$\overline{\overline{\text{(iii)}}} \qquad \max_{(x_1, x_2)\in S}|P_i^{(1)}(x_1)P_k^{(2)}(x_2)|\leqq$$

$$\leqq 4\{\sup_{x_1\in I}|\varphi_i^{(1)}(x_1)|+1\}\{\sup_{x_2\in I}|\varphi_k^{(2)}(x_2)|+1\} \quad (i, k=0, 1, \ldots).$$

Relation (5.2) immediately follows via the identity

$$\varphi^{(1)}\varphi^{(2)}-(-1)^{j^{(1)}+j^{(2)}}P^{(1)}P^{(2)} = \varphi^{(2)}[\varphi^{(1)}-(-1)^{j^{(1)}}P^{(1)}]+\varphi^{(1)}[\varphi^{(2)}-(-1)^{j^{(2)}}P^{(2)}]-$$
$$-[\varphi^{(1)}-(-1)^{j^{(1)}}P^{(1)}][\varphi^{(2)}-(-1)^{j^{(2)}}P^{(2)}].$$

The main trouble is that the right-hand sides in (5.1) and (5.2) are of $O\{\varepsilon_r^{(1)}+\varepsilon_s^{(2)}\}$ and thus do not tend to 0 as $\max(r, s)\to\infty$. In spite of this disadvantage, the approximation result just obtained is enough to state, for instance, that the double ONS can be replaced by double ONSP in the divergence theorems showing the exactness of Theorems D, E, and F. This is due to the fact that in these cases r and s can be chosen so as to depend on a single parameter l, say: $r=r_l$ and $s=s_l$, while both $r_l\to\infty$ and $s_l\to\infty$ as $l\to\infty$.

However, we can proceed another way. Starting with the strengthened versions of [3, Theorems D and E], the following three theorems can be deduced simply by forming the product system of two appropriate single ONSP as well as the product system $\{a_{ik}=a_i^{(1)}a_k^{(2)}\colon i, k=0, 1, \dots\}$ of the corresponding single sequences $\{a_i^{(1)}\}$ and $\{a_k^{(2)}\}$ of coefficients.

Theorems D′. *If $\{\varrho(n)\colon n=0, 1, \dots\}$ is a nondecreasing sequence of positive numbers for which*

(5.3) $$\varrho(n) = o\{\log(n+2)\} \quad as \quad n\to\infty,$$

then there exist a double ONSP $\{P_{ik}(x_1, x_2)=P_i^{(1)}(x_1)P_k^{(2)}(x_2)\colon i, k=0, 1, \dots\}$ *on* S *and a double sequence* $\{a_{ik}\}$ *of coefficients such that condition* (1.2) *is satisfied and*

(5.4) $$\limsup |S_{mn}(x_1, x_2)|/\varrho(m)\varrho(n) = \infty \quad a.e.\ as \quad \min(m, n)\to\infty$$

where

$$S_{mn}(x_1, x_2) = \sum_{i=0}^{m}\sum_{k=0}^{n} a_{ik}P_{ik}(x_1, x_2) \quad (m, n = 0, 1, \dots).$$

Using a double ONS $\{\varphi_{ik}(x_1, x_2)=\varphi_i^{(1)}(x_1)\varphi_k^{(2)}(x_2)\}$ in the counterexample, this theorem was proved in [11, Theorem 2].

Theorem E′. If $\{\varrho(n)\colon n=0, 1, \dots\}$ and $\{\tau(m)\colon m=0, 1, \dots\}$ *are two nondecreasing sequences of positive numbers,* ϱ *satisfying* (5.3) *and* τ *satisfying*

(5.5) $$\tau(m) = o\{\log\log(m+4)\} \quad as \quad m\to\infty,$$

then there exist a double ONSP $\{P_{ik}(x_1, x_2)=P_i^{(1)}(x_1)P_k^{(2)}(x_2)\}$ *on* S *and a double sequence* $\{a_{ik}\}$ *of coefficients such that* (1.2) *is satisfied and for every* $\alpha>0$

$$\limsup |\Sigma_{mn}^{\alpha 0}(x_1, x_2)|/\tau(m)\varrho(m) = \infty \quad a.e.\ as \quad \min(m, n)\to\infty,$$

where

$$\Sigma_{mn}^{\alpha 0}(x_1, x_2) = (1/A_m^\alpha)\sum_{i=0}^{m}\sum_{k=0}^{n} A_{m-i}^{\alpha-1}S_{ik}(x_1, x_2) \quad (m, n = 0, 1, \dots).$$

Theorem F′. *If* $\{\tau(m)\}$ *is a nondecreasing sequence of positive numbers satisfying* (5.5), *then there exist a double* ONSP $\{P_{ik}(x_1, x_2)=P_i^{(1)}(x_1)P_k^{(2)}(x_2)\}$ *and a double sequence* $\{a_{ik}\}$ *of coefficients such that* (1.2) *is satisfied and for every* $\alpha>0$ *and* $\beta>0$

(5.6) $$\limsup |\Sigma_{mn}^{\alpha\beta}(x_1, x_2)|/\tau(m)\tau(n) = \infty \quad \text{a.e. as} \quad \min(m, n) \to \infty$$

where

$$\Sigma_{mn}^{\alpha\beta}(x_1, x_2) = (1/A_m^\alpha A_n^\beta) \sum_{i=0}^{m} \sum_{k=0}^{n} A_{m-i}^{\alpha-1} A_{n-k}^{\beta-1} S_{ik}(x_1, x_2) \quad (m, n = 0, 1, \ldots).$$

Using double ONS $\{\varphi_{ik}(x_1, x_2)=\varphi_i^{(1)}(x_1)\varphi_k^{(2)}(x_2)\}$ in the counterexamples, Theorems E′ and F′ were included in [8, Section 5].

Remark 5. Examining the structure of the counterexamples in Theorems D′ and F′, the following slightly sharper result can be concluded: Estimates (5.4) and (5.6) remain true if $\varrho(m)\varrho(n)$ and $\tau(m)\tau(n)$ in the denominators are replaced by $\varrho^2(\min(m, n))$ and $\tau^2(\min(m, n))$, respectively, provided

$$\varrho(2n) \leqq C\varrho(n) \quad (n = 0, 1, \ldots) \quad \text{and} \quad \tau(m^2) \leqq C\tau(m) \quad (m = 0, 1, \ldots),$$

where C is a positive constant.

Remark 6. A couple of other divergence theorems can be strengthened by inserting double ONSP in the above way. For example, the corresponding two-dimensional versions of [3, Theorems B, C, and F] hold also true.

6. Proof of Theorem 1. It relies on the basic ideas of Menšov [4] and Leindler [3]. Here we reformulate four lemmas of their papers for the two-dimensional case. These lemmas were stated and proved in the one-dimensional case. However, the proofs of the two-dimensional reformulations closely follow the original proofs. Where is needed, we indicate the necessary modifications.

Lemma 1. *Let* $\{f_i(x_1, x_2)\colon 1 \leqq i \leqq N\}$ *be continuous functions, while* $\{g_j(x_1, x_2)\colon 1 \leqq j \leqq N'\}$ *step functions on* S *and let* $\varepsilon>0$. *Then there exist functions* $\{G_j(x_1, x_2)\colon 1 \leqq j \leqq N'\}$ *and a measurable subset* E *of* S *with the following properties:*

(a) *The functions* G_j *are continuous on* S;

(b) $|E| \leqq \varepsilon$;

(c) *For every* $(x_1, x_2) \in S \setminus E$ *and for every* $1 \leqq j \leqq N'$,

$$G_j(x_1, x_2) = (-1)^{j(x_1, x_2)} g_j(x_1, x_2)$$

where $j(x_1, x_2)$ *equals* 0 *or* 1 *depending on* (x_1, x_2) *but not on* j;

(d) $$\max_{(x_1, x_2) \in S} |G_j(x_1, x_2)| \leqq \max_{(x_1, x_2) \in S} |g_j(x_1, x_2)| \quad (1 \leqq j \leqq N');$$

(e) $$\left|\int_0^1 \int_0^1 f_i(x_1, x_2) G_j(x_1, x_2)\, dx_1\, dx_2\right| \leqq \varepsilon \quad (1 \leqq i \leqq N,\ 1 \leqq j \leqq N').$$

This auxiliary result is the restatement of [4, Lemma 2, pp. 30—32] with a similar proof. The only thing to explain is that if g is a step function on S, then for every $\varepsilon > 0$ there exists a continuous function G on S such that

$$|\{(x_1, x_2)\colon\ G(x_1, x_2) \neq g(x_1, x_2)\}| \leqq \varepsilon \tag{6.1}$$

and

$$\max_{(x_1, x_2)\in S} |G(x_1, x_2)| \leqq \max_{(x_1, x_2)\in S} |g(x_1, x_2)|. \tag{6.2}$$

This is clear if $g(x_1, x_2) = g^{(1)}(x_1)g^{(2)}(x_2)$ even with some $G(x_1, x_2) = G^{(1)}(x_1)G^{(2)}(x_2)$. In the general case, it is enough to consider the characteristic function $g(x_1, x_2) = \chi_R(x_1, x_2)$ of a rectangle R inside S given by $R = \langle\alpha_1, \alpha_2\rangle \times \langle\beta_1, \beta_2\rangle$, where $\langle\alpha_1, \alpha_2\rangle$ denotes one of the intervals (α_1, α_2), $[\alpha_1, \alpha_2)$, $(\alpha_1, \alpha_2]$, $[\alpha_1, \alpha_2]$ and $\langle\beta_1 \beta_2\rangle$ has a similar meaning. Setting

$$\delta = \min\{\varepsilon/4, (\alpha_2 - \alpha_1)/2, (\beta_2 - \beta_1)/2\}$$

we define $G(x_1, x_2)$ to be $G^{(1)}(x_1)G^{(2)}(x_2)$ where

$$G^{(1)}(x_1) = \begin{cases} 1 & \text{for } \ \alpha_1 + \delta \leqq x_1 \leqq \alpha_2 - \delta, \\ 0 & \text{for } \ 0 \leqq x_1 \leqq \alpha_1 \ \text{ and } \ \alpha_2 \leqq x_1 \leqq 1, \\ \text{linear} & \text{for } \ \alpha_1 < x_1 < \alpha_1 + \delta \ \text{ and } \ \alpha_2 - \delta < x_1 < \alpha_2 \end{cases}$$

in such a way that $G^{(1)}$ is continuous on I; and $G^{(2)}$ is defined in an analogous manner. It is easy to check that this G meets the conditions (6.1) and (6.2).

Remark 7. If $N' = N_1' N_2'$ and the functions f_i and g_j are given in the forms

$$f_i(x_1, x_2) = f_i^{(1)}(x_1) f_i^{(2)}(x_2) \quad (1 \leqq i \leqq N)$$

and

$$g_{jl}(x_1, x_2) = g_j^{(1)}(x_1) g_l^{(2)}(x_2) \quad (1 \leqq j \leqq N_1',\ 1 \leqq l \leqq N_2'),$$

then the functions G_j can be also represented in the form

$$G_{jl}(x_1, x_2) = G_j^{(1)}(x_1) G_l^{(2)}(x_2) \quad (1 \leqq j \leqq N_1',\ 1 \leqq l \leqq N_2'). \tag{6.3}$$

In order to see this, apply the original Menšov's lemma [4, Lemma 2] separately to the following two systems $\{f_i^{(1)}(x_1), g_j^{(1)}(x_1)\colon 1 \leqq i \leqq N,\ 1 \leqq j \leqq N_1'\}$ and $\{f_i^{(2)}(x_2), g_l^{(2)}(x_2)\colon 1 \leqq i \leqq N,\ 1 \leqq l \leqq N_2'\}$ with $\varepsilon^{(1)} = \varepsilon^{(2)} = \varepsilon/2$ instead of $\varepsilon > 0$. As a result, we obtain two systems $\{G_j^{(1)}(x_1)\colon 1 \leqq j \leqq N_1'\}$ and $\{G_l^{(2)}(x_2)\colon 1 \leqq l \leqq N_2'\}$ with corresponding sets $E^{(1)}$ and $E^{(2)}$, and corresponding exponents $j^{(1)}(x_1)$ and $j^{(2)}(x_2)$. Letting (6.3),

$$E = (E^{(1)} \times I) \cup (I \times E^{(2)}), \quad \text{and} \quad j(x_1, x_2) = j^{(1)}(x_1) + j^{(2)}(x_2),$$

properties (a), (b), (c), and (e) are obviously satisfied (in case (e) provided $\varepsilon \leqq 1$). To verify the fulfillment of (d), we have to take into account that the extreme values of the step functions $g_j^{(1)}$and $g_l^{(2)}$ are not altered during the linearization process. Thus, for every $(x_1, x_2)\in S$ there exists a pair $(x_1', x_2')\in S$ such that

$$|G_j^{(1)}(x_1)| \leqq |G_j^{(1)}(x_1')| = |g_j^{(1)}(x_1')|$$

and

$$|G_l^{(2)}(x_2)| \leqq |G_l^{(2)}(x_2')| = |g_l^{(2)}(x_2')|.$$

Consequently, (d) is also satisfied.

Lemma 2. *Let* $0<r<r'$, $\{\Pi_i(x_1, x_2)\colon 1\leqq i\leqq r\}$ *and* $\{Q_k(x_1, x_2)\colon r<k\leqq r'\}$ *be nonidentically vanishing polynomials in* x_1 *and* x_2,

$$\nu = \max_{i,k}\Big\{\max_{(x_1,x_2)\in S} |\Pi_i(x_1, x_2)|,\ \max_{(x_1,x_2)\in S} |Q_k(x_1, x_2)|\Big\},$$

$$\varkappa = \min_{i,k}\Big\{\int_0^1\int_0^1 \Pi_i^2(x_1, x_2)\,dx_1\,dx_2,\ \int_0^1\int_0^1 Q_k^2(x_1, x_2)\,dx_1\,dx_2\Big\},$$

$$\sigma = \max_{\substack{i,k,l\\ k\neq l}}\Big\{\int_0^1\int_0^1 \Pi_i(x_1, x_2)Q_k(x_1, x_2)\,dx_1\,dx_2,\ \int_0^1\int_0^1 Q_k(x_1, x_2)Q_l(x_1, x_2)\,dx_1\,dx_2\Big\},$$

$$\gamma = \max\{4r', \nu, 1/\varkappa\}, \quad \textit{and} \quad \lambda = \gamma^{6(r'-r+1)}.$$

If the polynomials $\{\Pi_i(x_1, x_2)\colon 1\leqq i\leqq r\}$ *are orthogonal on* S *and* $\sigma\lambda<1$, *then there exist polynomials* $\{\Pi_k(x_1, x_2)\colon r<k\leqq r'\}$ *in* x_1 *and* x_2 *such that the following properties are satisfied:*

($\bar{\text{a}}$) *The polynomials* $\{\Pi_i(x_1, x_2)\colon 1\leqq i\leqq r'\}$ *are orthogonal on* S;

($\bar{\text{b}}$) $\max_{(x_1,x_2)\in S} |Q_k(x_1, x_2)-\Pi_k(x_1, x_2)| \leqq \sigma\lambda \quad (r < k \leqq r')$.

The proof is essentially a repetition of the proof of the corresponding result of Menšov [4, Lemma 3, pp. 32—36].

Remark 8. If $r'=r_1'r_2'$ and the polynomials Π_i and Q_k are given in the forms

$$\Pi_i(x_1, x_2) = \Pi_i^{(1)}(x_1)\Pi_i^{(2)}(x_2) \quad (1 \leqq i \leqq r)$$

and

$$Q_{kl}(x_1, x_2) = Q_k^{(1)}(x_1)Q_l^{(2)}(x_2) \quad (r < k \leqq r_1',\ r < l \leqq r_2'),$$

then the polynomials Π_k can also be represented in the form

$$\Pi_{kl}(x_1, x_2) = \Pi_k^{(1)}(x_1)\Pi_l^{(2)}(x_2) \quad (r < k \leqq r_1',\ r < l \leqq r_2'). \tag{6.4}$$

Indeed, apply the original Menšov's lemma [4, Lemma 3] separately to the systems $\{\Pi_i^{(1)}(x_1),\ Q_k^{(1)}(x_1)\colon 1\leqq i\leqq r<k\leqq r_1'\}$ and $\{\Pi_i^{(2)}(x_2),\ Q_l^{(2)}(x_2)\colon 1\leqq i\leqq r<l\leqq r_2'\}$ with the corresponding notations $\nu^{(1)}, \varkappa^{(1)}, \sigma^{(1)}, \gamma^{(1)}, \lambda^{(1)}$ and $\nu^{(2)}, \ldots, \lambda^{(2)}$. If $\sigma^{(1)}\lambda^{(1)}<1$ and $\sigma^{(2)}\lambda^{(2)}<1$, then we can obtain polynomials $\Pi_k^{(1)}$ for $r<k\leqq r_1'$ and $\Pi_l^{(2)}$ for $r<$

$<l \leqq r_2'$ such that the systems $\{\Pi_k^{(1)}(x_1)\colon 1 \leqq k \leqq r_1'\}$ and $\{\Pi_l^{(2)}(x_2)\colon 1 \leqq l \leqq r_2'\}$ are orthonormal on I, respectively, and

$$\max_{x_1 \in I} |Q_k^{(1)}(x_1) - \Pi_k^{(1)}(x_1)| \leqq \sigma^{(1)} \lambda^{(1)} \quad (r < k \leqq r_1')$$

and

$$\max_{x_2 \in I} |Q_l^{(2)}(x_2) - \Pi_l^{(2)}(x_2)| \leqq \sigma^{(2)} \lambda^{(2)} \quad (r < l \leqq r_2').$$

Now letting (6.4), the fulfillment of $(\bar{a})$ is clear, while a slightly modified version of $(\bar{b})$ follows via the elementary estimate

$$\max_{(x_1, x_2) \in S} |Q_k^{(1)}(x_1) Q_l^{(2)}(x_2) - \Pi_k^{(1)}(x_1) \Pi_l^{(2)}(x_2)| \leqq$$

$$\leqq \nu^{(2)} \max_{x_1 \in I} |Q_k^{(1)}(x_1) - \Pi_k^{(1)}(x_1)| + \nu^{(1)} \max_{x_2 \in I} |Q_l^{(2)}(x_2) - \Pi_l^{(2)}(x_2)| \leqq$$

$$\leqq \nu^{(2)} \sigma^{(1)} \lambda^{(1)} + \nu^{(1)} \sigma^{(2)} \lambda^{(2)}.$$

This form is still enough during the proof of Lemma 4 below (cf. [3, p. 26, formula (3.4)]).

Lemma 3. *Let* $\{\varphi_{ik}(x_1, x_2)\colon i, k = 0, 1, \ldots\}$ *be a double* ONS *on* S, $\{\varepsilon_{rs}\colon r, s = 1, 2, \ldots\}$ *a double sequence of positive numbers,* $\{M_r\colon r = 1, 2, \ldots\}$ *and* $\{N_s\colon s = 1, 2, \ldots\}$ *two strictly increasing sequences of nonnegative integers. Then there exist a double system* $\{\psi_{ik}(x_1, x_2)\colon i, k = 0, 1, \ldots\}$ *of bounded functions on* S *and a double sequence* $\{E_{rs}\colon r, s = 1, 2, \ldots\}$ *of measurable subsets of* S *such that the following properties are satisfied:*

(α) *The functions* ψ_{ik} *are orthonormal on* S *in each block* $M_{r-1} < i \leqq M_r$ *and* $N_{s-1} < k \leqq N_s$ $(r, s = 1, 2, \ldots;\ M_0 = N_0 = -1)$;

(β) $|E_{rs}| \leqq \varepsilon_{rs}$ $(r, s = 1, 2, \ldots)$;

(γ) *For every* $(x_1, x_2) \in S \setminus E_{rs}$, *and for every* $M_{r-1} < i \leqq M_r$ *and* $N_{s-1} < k \leqq N_s$,

$$|\varphi_{ik}(x_1, x_2) - \psi_{ik}(x_1, x_2)| \leqq \varepsilon_{rs} \quad (r, s = 1, 2, \ldots).$$

This lemma is a straightforward extension of a lemma due to Leindler [3, Lemma 4, pp. 33—36]. The original proof works in the two-dimensional setting, since the blocks $\{\varphi_{ik}(x_1, x_2)\colon M_{r-1} < i \leqq M_r$ and $N_{s-1} < k \leqq N_s\}$ and the corresponding ε_{rs} $(r, s = 1, 2, \ldots)$ can be treated in an arrangement similar to the Cantor diagonal process, i.e. in the following succession: $\varepsilon_{11}, \varepsilon_{12}, \varepsilon_{21}, \varepsilon_{13}, \varepsilon_{22}, \varepsilon_{14}, \ldots$ and the blocks are taken accordingly.

Lemma 4. *Let* $\{\varepsilon_{rs}\colon r, s = 1, 2, \ldots\}$ *be a double sequence of positive numbers,* $\{M_r\colon r = 1, 2, \ldots\}$ *and* $\{N_s\colon s = 1, 2, \ldots\}$ *two strictly increasing sequences of nonnegative integers, and* $\{\psi_{ik}(x_1, x_2)\colon i, k = 0, 1, \ldots\}$ *a double system of bounded functions such that the* ψ_{ik} *are orthonormal on* S *in each block* $M_{r-1} < i \leqq M_r$ *and* $N_{s-1} < k \leqq N_s$ $(r, s = 1, 2, \ldots;\ M_0 = N_0 = -1)$. *Then there exist a double* ONSP $\{P_{ik}(x_1, x_2)\colon i, k =$

$=0, 1, \ldots\}$ *on* S *and a double sequence* $\{\bar{E}_{rs}: r, s=1, 2, \ldots\}$ *of measurable subsets of* S *with the following properties:*

($\bar{\alpha}$) $|\bar{E}_{rs}| \leqq \varepsilon_{rs}$ $(r, s=1, 2, \ldots)$;

($\bar{\beta}$) *For every* $(x_1, x_2) \in S \setminus \bar{E}_{rs}$, *and for every* $M_{r-1} < i \leqq M_r$ *and* $N_{s-1} < k \leqq N_s$,

$$|\psi_{ik}(x_1, x_2) - (-1)^{j_{rs}(x_1, x_2)} P_{ik}(x_1, x_2)| \leqq \varepsilon_{rs} \quad (r, s = 1, 2, \ldots)$$

where $j_{rs}(x_1, x_2)$ *equals* 0 *or* 1;

($\bar{\gamma}$) $\max_{(x_1, x_2) \in S} |P_{ik}(x_1, x_2)| \leqq 2\{\sup_{(x_1, x_2) \in S} |\psi_{ik}(x_1, x_2)| + 1\}$ $(i, k = 0, 1, \ldots)$.

Remark 9. If in each block $M_{r-1} < i \leqq M_r$ and $N_{s-1} < k \leqq N_s$ the functions ψ_{ik} can be represented in a product form analogous to (4.2):

$$\psi_{ik}(x_1, x_2) = \psi_i^{(1, r)}(x_1) \psi_k^{(2, s)}(x_2)$$

where both $\{\psi_i^{(1, r)}(x_1): M_{r-1} < i \leqq M_r\}$ and $\{\psi_k^{(2, s)}(x_2): N_{s-1} < k \leqq N_s\}$ are bounded orthonormal functions on I $(r, s=1, 2, \ldots)$, then the P_{ik} can be also represented in the product form (4.3) where both

$$\{P_i^{(1, r)}(x_1): M_{r-1} < i \leqq M_r\}$$

and

$$\{P_k^{(2, s)}(x_2): N_{s-1} < k \leqq N_s\}$$

are orthonormal polynomials on I $(r, s=1, 2, \ldots)$.

The proof of Lemma 4 can be modelled on that of Leindler's basic lemma [3, Lemma 3, pp. 26—33]. We only note that both the Egorov theorem and the Weierstrass approximation theorem are valid in two-dimensional setting, as well.

The former one states that if $\psi(x_1, x_2)$ is a bounded measurable function on S, then for every $\varepsilon > 0$ there exist a measurable step function $\varphi(x_1, x_2)$ on S and a measurable subset E of S such that

(1) $|E| \leqq \varepsilon$;

(2) $|\psi(x_1, x_2) - \varphi(x_1, x_2)| \leqq \varepsilon$ for $(x_1, x_2) \in S \setminus E$;

(3) $\max_{(x_1, x_2) \in S} |\varphi(x_1, x_2)| \leqq \sup_{(x_1, x_2) \in S} |\psi(x_1, x_2)|$;

(4) If $\psi(x_1, x_2) = \psi^{(1)}(x_1) \psi^{(2)}(x_2)$, then φ can be chosen in the form of $\varphi(x_1, x_2) = \varphi^{(1)}(x_1) \varphi^{(2)}(x_2)$.

Concerning the two-dimensional version of the Weierstrass theorem, we refer to [2, pp. 89—90]. Choosing $T=S$ and $\mathfrak{A}$ to be the set of the polynomials $P(x_1, x_2)$ in x_1 and x_2, properties (i)—(iv) in the cited paper are obviously satisfied, thereby ensuring the uniform approximation of continuous functions on S by the elements of $\mathfrak{A}$.

Finally, the validity of Remark 9 can be verified by means of Remarks 7 and 8.

7. Proof of Theorem 2. We will present only the proof of the sharpening of Theorem A′. The sharpenings of Theorem B′ and C′ can be proved similarly.

So, assume the fulfillment of (3.1) and (3.2). In the proof of [10, Theorem 4] a double ONS $\{\varphi_{ik}(x_1, x_2): i, k=0,1, \dots\}$ of step functions on S and a double sequence $\{H_{rs}: r, s=-1, 0, 1, \dots\}$ of measurable subsets of S were constructed with the following properties:

(i) $|H|=1$ where $H=\limsup H_{rs}$ as $\max(r, s)\to\infty$;

(ii) For every $(x_1, x_2)\in H_{rs}$

(7.1)
$$\max_{2^{r-1}<m\leq 2^r}\ \max_{2^{s-1}<n\leq 2^s}\Big|\sum_{i=2^{r-1}+1}^{m}\ \sum_{k=2^{s-1}+1}^{n} a_{ik}\varphi_{ik}(x_1, x_2)\Big| \geqq C\eta_{\max(r,s)} \quad (r, s=-1, 0, 1, \dots)$$

where C is a positive constant and $\{\eta_r: r=-1, 0, 1, \dots\}$ is an increasing sequence of positive numbers tending to ∞ as $r\to\infty$;

(iii) In each block $2^{r-1}<i\leqq 2^r$ and $2^{s-1}<k\leqq 2^s$ the functions φ_{ik} can be represented in the product form (4.2).

Given any $\delta>0$, on the basis of Theorem 1 we can construct a double ONSP $\{P_{ik}(x_1, x_2)\}$ and a double sequence $\{\bar{H}_{rs}\}$ of measurable subsets of S such that

($\bar{\text{i}}$) $|\bar{H}|=1$ where $\bar{H}=\limsup \bar{H}_{rs}$ as $\max(r, s)\to\infty$;

($\bar{\text{ii}}$) For every $(x_1, x_2)\in\bar{H}_{rs}$

(7.2)
$$\max_{2^{r-1}<m\leq 2^r}\ \max_{2^{s-1}<n\leq 2^s}\Big|\sum_{i=2^{r-1}+1}^{m}\ \sum_{k=2^{s-1}+1}^{n} a_{ik}P_{ik}(x_1, x_2)\Big| \geqq (C-\delta)\eta_{\max(r,s)} \quad (r, s=-1, 0, 1, \dots)$$

(cf. [3, Theorem 2, p. 21 and its proof on pp. 38—39]);

($\overline{\text{iii}}$) In each block $2^{r-1}<i\leqq 2^r$ and $2^{s-1}<k\leqq 2^s$ the polynomials P_{ik} can be represented in the product form (4.3).

Relation (7.2) implies the a.e. divergence of the double series

$$\sum_{i=0}^{\infty}\sum_{k=0}^{\infty} a_{ik}P_{ik}(x_1, x_2)$$

in the same way as (7.1) implies the a. e. divergence of the double series (1.1).

References

[1] P. R. AGNEW, On double orthogonal series, *Proc. London Math. Soc.*, Ser. 2, 33 (1932), 420—434.

[2] B. BROSOWSKI and F. DEUTSCH, An elementary proof of the Stone—Weierstrass theorem, *Proc. Amer. Math. Soc.*, **81** (1981), 89—92.

[3] L. Leindler, Über die orthogonalen Polynomsysteme, *Acta Sci. Math.*, **21** (1960), 19—46.
[4] D. Menchoff, Sur les multiplicateurs de convergence pour les séries de polynômes orthogonaux, *Recueil Math. Moscou*, **6** (48) (1939), 27—52.
[5] F. Móricz, On the convergence in a restricted sense of multiple series, *Analysis Math.*, **5** (1979), 135—147.
[6] F. Móricz, On the growth order of the rectangular partial sums of multiple non-orthogonal series, *Analysis Math.*, **6** (1980), 327—341.
[7] F. Móricz, On the $(C, \alpha \geqq 0, \beta \geqq 0)$-summability of double orthogonal series, *Studia Math.*, **81** (1985), 79—94.
[8] F. Móricz, The order of magnitude of the arithmetic means of double orthogonal series, *Analysis Math.*, **11** (1985), 125—137.
[9] F. Móricz, The order of magnitude of the $(C, \alpha \geqq 0, \beta \geqq 0)$-means of double orthogonal series, *Rocky Mountain J. Math.*, **16** (1986), 323—334.
[10] F. Móricz and K. Tandori, On the divergence of multiple orthogonal series, *Acta Sci. Math.*, **42** (1980), 133—142.
[11] F. Móricz and K. Tandori, On the a. e. divergence of the arithmatic means of double orthogonal series, *Studia Math.*, **82** (1985), 271—294.
[12] K. Tandori, Über die Cesàrosche Summierbarkeit von mehrfachen Orthogonalreihen, *Acta Sci. Math.*, **49** (1985), 179—210.

UNIVERSITY OF SZEGED
BOLYAI INSTITUTE
ARADI VÉRTANÚK TERE 1
6720 SZEGED, HUNGARY

Acta Sci. Math., 50 (1986), 381—390

Birkhoff quadrature formulas based on Tchebycheff nodes

A. K. VARMA

1. In 1974 P. Turán [6] raised the following problems on Birkhoff quadrature. If in the n^{th} row of a matrix A, there are n interpolation points $1 \geqq x_{1n} > x_{2n} > \ldots > x_{nn} \geqq -1$ then A is called "very good" if for an arbitrary set of numbers y_{kn} and y''_{kn} there is a uniquely determined polynomial $D_n(f;\, A) = D_n(f)$ of degree at most $2n-1$ for which

$$D_n(f;\, A)_{x=x_{kn}} = y_{kn} = f(x_{kn}), \quad \left(\frac{d^2}{dx^2} D_n(f;\, A)\right)_{x=x_{kn}} = y''_{kn}, \quad k = 1, 2, \ldots, n.$$

In that case $D_n(f;\, A)$ can be uniquely written as

$$D_n(f;\, A) = \sum_{i=1}^{n} f(x_{in})\gamma_{in}(x;\, A) + \sum_{i=1}^{n} y''_{in}\varrho_{in}(x;\, A)$$

where $\gamma_{in}(x;\, A)$, $\varrho_{in}(x;\, A)$ are fundamental functions of the first and second kind, respectively.

Problem XXXVI. What is the best class of functions for which the integrals of the polynomials

$$\sum_{i=1}^{n} f(x_{in})\gamma_{in}(x, \Pi) \quad (n \text{ even})$$

tend to $\int_{-1}^{1} f(x)\, dx$?

Here the n^{th} row of the Π matrix is referred to the zeros of $\Pi_n(x) = \int_{-1}^{x} P_{n-1}(t)\, dt$ where $P_n(x)$ is the Legendre polynomial of degree n.

Problem XXXVIII. Does there exist a matrix A satisfying

$$\int_{-1}^{1} \gamma_{in}(x;\, A)\, dx \geqq 0, \quad i = 1, 2, \ldots, n;\ n \geqq n_0?$$

Received June 21, 1984, and in revised form June 4, 1985.

Problem XXXIX. Determine the "good" matrices for which

$$\sum_{i=1}^{n}\left|\int_{-1}^{1}\gamma_{in}(x;\ A)\,dx\right|$$

is minimal.

In 1982 the author [7] was able to answer the above problems. This can be summarized by the following quadrature formula exact for polynomials of degree $\le 2n-1$:

$$\int_{-1}^{1} f(x)\,dx = \frac{3((f(1)+f(-1)))}{n(2n-1)}+\frac{2(2n-3)}{n(n-2)(2n-1)}\sum_{i=2}^{n-1}\frac{f(x_{in})}{P_{n-1}^2(x_{in})}+$$

$$+\frac{1}{n(n-1)(n-2)(2n-1)}\sum_{i=2}^{n-1}\frac{(1-x_{in}^2)f''(x_{in})}{P_{n-1}^2(x_{in})}.$$

In the above formula x_{in}'s are chosen to be the zeros of $\Pi_n(x)$.

In 1961, the author [9] extended the results of Saxena and Sharma [6] of (0, 1, 3) interpolation to Tchebycheff abscissas. We proved that if n is even, then for preassigned values y_{i0}, y_{i1}, y_{i3} $(i=1,2,\dots,n)$ there exists a uniquely determined polynomial $f_n(x)$ of degree $\le 3n-1$ such that

$$f_n(x_{in}) = y_{i0},\quad f_n'(x_{in}) = y_{i1},\quad f_n'''(x_{in}) = y_{i3},\quad i = 1, 2, \dots, n \tag{1.1}$$

where x_{in}'s are the zeros of $T_n(x)$.

The object of this paper is to obtain new quadrature formulas based on $f(x_{in})$, $f'(x_{in})$, $f'''(x_{in})$ where x_{in}'s are the zeros of $T_n(x)$. We now state the main theorems of this paper.

Theorem 1. *Let*

$$1 > x_{1n} > x_{2n} > \dots > x_{nn} > -1 \tag{1.2}$$

be the zeros of $T_n(x)=\cos n\theta$, $\cos\theta=x$. Let $f(x)$ be any polynomial of degree $\le 3n-1$. Then we have

$$\int_{-1}^{1}\frac{f(x)}{(1-x^2)^{1/2}}\,dx = \sum_{i=1}^{n} f(x_{in})A_{in}+\sum_{i=1}^{n} f'(x_{in})B_{in}+\sum_{i=1}^{n} f'''(x_{in})C_{in} \tag{1.3}$$

where

$$C_{in} = \frac{(1-x_{in}^2)^2}{12n^2}\int_{-1}^{1}\frac{l_{in}'(x)}{(1-x^2)^{1/2}}\,dx = \frac{(1-x_{in}^2)^2\pi}{12n^3}\left(T_n'(x_{in})-\frac{x_{in}}{1-x_{in}^2}\right), \tag{1.4}$$

$$B_{in} = -\frac{\pi}{4n}(1-x_{in}^2)T_n'(x_{in})+\left(\frac{3+2(2n^2+1)(1-x_{in}^2)}{12n^2}\right)\int_{-1}^{1}\frac{l_{in}'(x)\,dx}{(1-x^2)^{1/2}} \tag{1.5}$$

and

(1.6) $$A_{in}=\frac{\pi}{n}\left[1+\frac{1}{3(1-x_{in}^2)}\left(\frac{1}{n^2}-1\right)-\frac{1}{2n^2(1-x_{in}^2)^2}+\frac{x_iT_n'(x_i)}{4}+\frac{T_n''(x_{in})}{2n^2}\right].$$

Theorem 2. *Let* $f_0(x)=1-x^2$ *then*

(1.7) $$\int_{-1}^{1}\frac{f_0(x)}{(1-x^2)^{1/2}}dx-\sum_{i=1}^{n}f_0(x_{in})A_{in}=\frac{\pi}{3}-\frac{\pi}{3n^2}.$$

An interesting consequence of Theorem 2 is the following:

Corollary 1. *For* $f_0(x)=1-x^2$

(1.8) $$\lim_{n\to\infty}\sum_{i=1}^{n}f_0(x_{in})u_{in}(x)\neq 1-x^2 \quad \textit{at some} \quad x\in[-1,1],$$

where $u_{in}(x)$ *are the fundamental polynomials of the first kind* (0, 1, 3) *interpolation based on Tchebycheff nodes. The explicit representation of* $u_{in}(x)$ *is given in the next section.*

Theorem 3. *There exist positive constants* c_1 *and* c_2 *independent of* n *such that*

(1.9) $$c_1 n\ln n<\sum_{i=1}^{n}|A_{in}|\leqq c_2 n\ln n.$$

Theorems 1, 2, 3 reveal an important fact that the quadrature formula obtained by integrating the Birkhoff interpolation polynomials of (0, 1, 3) interpolation based on Tchebycheff nodes is essentially very different from those obtained by integrating Lagrange or Hermite interpolation.

2. Explicit representation of the interpolatory polynomials; (0, 1, 3) case. In an earlier work [9] we obtained the explicit form of the polynomial $R_n(x)$ (n even positive integer) of degree $\leqq 3n-1$ satisfying

(2.1) $$R_n(x_{kn})=f_{kn},\quad R_n'(x_{kn})=g_{kn},\quad R_n'''(x_{kn})=h_{kn},\quad k=1,2,\ldots,n.$$

It is given by

(2.2) $$R_n(x)=\sum_{i=1}^{n}f_{in}u_{in}(x)+\sum_{i=1}^{n}g_{in}v_{in}(x)+\sum_{i=1}^{n}h_{in}w_{in}(x),$$

where the polynomials $u_{in}(x)$, $v_{in}(x)$, $w_{in}(x)$ are uniquely determined by the following conditions:

(2.3) $$u_{in}'(x_{kn})=u_{in}'''(x_{kn})=0,\quad u_{in}(x_{kn})=\begin{cases}1 & \text{for } i=k\\ 0 & \text{for } i\neq k,\end{cases}\quad k=1,2,\ldots,n,$$

(2.4) $$v_{in}(x_{kn})=v_{in}'''(x_{kn})=0,\quad v_{in}'(x_{kn})=\begin{cases}1 & \text{for } i=k\\ 0 & \text{for } i\neq k,\end{cases}\quad k=1,2,\ldots,n,$$

(2.5) $$w_{in}(x_{kn})=w_{in}'(x_{kn})=0,\quad w_{in}'''(x_{kn})=\begin{cases}1 & \text{for } i=k\\ 0 & \text{for } i\neq k,\end{cases}\quad k=1,2,\ldots,n.$$

The explicit form of fundamental polynomials is given by

(a)

$$w_{in}(x) = \frac{(1-x_{in}^2)^2 T_n^2(x) q_{n-1,i}(x)}{6n^2}, \tag{2.6}$$

where $q_{n-1,i}(x)$ is a polynomial of degree $\leqq n-1$. It is given by

$$q_{n-1,i}(x) = (1-x^2)^{1/2}\left[a_{in}\int_0^x \frac{T_n(t)}{(1-t^2)^{3/2}}\,dt + \int_0^x \frac{l_{in}(t)}{(1-t^2)^{3/2}}\,dt + c_{in}\right] \tag{2.7}$$

where a_{in}, c_{in} are chosen so that $q_{n-1,i}(x)$ is a polynomial of degree $\leqq n-1$.

(b)

$$a_{in} = -\frac{1}{n\pi}\int_{-1}^{1} \frac{t l_{in}'(t)}{(1-t^2)^{1/2}}\,dt,$$

$$c_{in} = (1/2)\int_{-1}^{1} \frac{l_{in}'(t)}{(1-t^2)^{1/2}}\,dt - (1/2)\int_0^1 \frac{l_{in}(t)-l_{in}(-t)}{(1-t)^{1/2}(1+t)^{3/2}}\,dt,$$

$$v_{in}(x) = \frac{T_n(x)\, l_{in}^2(x)}{T_n'(x_{in})} + \frac{T_n^2(x) s_{n-1,i}(x)}{T_n'(x_{in})} \tag{2.8}$$

where $s_{n-1,i}(x)$ is a polynomial of degree $\leqq n-1$. It is expressed by the formula

(2.9)

$$s_{n-1,i}(x) = (1-x^2)^{1/2}\left[\alpha_{in}\int_0^x \frac{T_n(t)}{(1-t^2)^{3/2}}\,dt + \beta_{in}\int_0^x \frac{l_{in}(t)}{(1-t^2)^{3/2}}\,dt + \int_0^x \frac{F_{in}(t)}{(1-t^2)^{3/2}}\,dt + \gamma_{in}\right]$$

where

$$F_{in}(t) = \frac{(1-t^2)\, l_{in}''(t) - t l_{in}'(t) + (n^2+1)\, l_{in}(t)}{2T_n'(x_{in})}, \tag{2.10}$$

$$\alpha_{in} = \frac{-1}{n\pi}\int_{-1}^{1} \frac{tF_{in}'(t) + \beta_{in} l_{in}'(t)}{(1-t^2)^{1/2}}\,dt, \tag{2.11}$$

$$\beta_{in} = \frac{1}{2T_n'(x_{in})}\left(\frac{n^2-7}{3} - \frac{5x_{in}^2}{1-x_{in}^2}\right), \tag{2.12}$$

(2.13)

$$2\gamma_{in} = \int_{-1}^{1} \frac{\beta_{in} l_{in}'(t) + F_{in}'(t)}{(1-t^2)^{1/2}}\,dt - \int_0^1 \frac{\beta_{in}(l_{in}(t)-l_{in}(-t)) + F_{in}(t) - F_{in}(-t)}{(1-t)^{1/2}(1+t)^{3/2}}\,dt.$$

(c)

$$u_{in}(x)=\frac{(1-x^2)\,l_{in}^3(x)}{1-x_{in}^2}+\frac{1}{3}\frac{(1-x^2)(x-x_{in})}{(1-x_{in}^2)}\,l_{in}^2(x)\,l_{in}'(x)+ \tag{2.14}$$

$$+\frac{x_{in}}{3(1-x_{in}^2)}\,v_{in}(x)+\lambda_{in}w_{in}(x)$$

where

$$\lambda_{in}=\frac{x_{in}}{3(1-x_{in}^2)}\left[8n^2+\frac{13+2x_{in}^2}{1-x_{in}^2}\right].$$

The above representation of $u_{in}(x)$ is new and very useful in obtaining $\int_{-1}^{1}\frac{u_{in}(x)}{(1-x^2)^{1/2}}\,dx.$

3. Preliminaries. Here we shall prove the following lemmas.

Lemma 3.1. *For $k=1,2,\dots,n$ we have*

$$\int_{-1}^{1}\frac{T_n(x)\,l_{kn}^2(x)}{T_n'(x_{kn})}(1-x^2)^{-1/2}\,dx=\frac{\pi}{2n^3}\,x_{kn}, \tag{3.1}$$

$$\int_{-1}^{1}\frac{(1-x^2)\,l_{kn}^3(x)}{(1-x_{kn}^2)}(1-x^2)^{-1/2}\,dx=\frac{\pi}{n}\left\{\frac{3}{4}-\frac{1}{4n^2(1-x_{kn}^2)}\right\}, \tag{3.2}$$

$$\int_{-1}^{1}\left(\frac{1-xx_{kn}}{1-x_{kn}^2}\right)l_{kn}^3(x)(1-x^2)^{-1/2}\,dx=\frac{\pi}{n}\left\{\frac{3}{4}+\frac{1}{4n^2(1-x_{kn}^2)}\right\}, \tag{3.3}$$

$$\int_{-1}^{1}\frac{(1-x^2)(x-x_{kn})\,l_{kn}^2(x)\,l_{kn}'(x)}{1-x_{kn}^2}(1-x^2)^{-1/2}\,dx=\frac{\pi}{4n}\left\{-1+\frac{1}{n^2(1-x_{kn}^2)}\right\}. \tag{3.4}$$

Proof. According to a theorem of MICHELLI and RIVLIN [5] if $g(x)$ is a polynomial of degree $\leqq 4n-1$ then

$$\int_{-1}^{1}g(x)(1-x^2)^{-1/2}\,dx= \tag{3.5}$$

$$=\frac{\pi}{n}\left[\sum_{i=1}^{n}g(x_{in})+\frac{1}{4n^2}\sum_{i=1}^{n}(1-x_{in}^2)g''(x_{in})-x_{in}g'(x_{in})\right]$$

where x_{in}'s are the zeros of $T_n(x)$. First let

$$g(x)=\frac{T_n(x)\,l_{kn}^2(x)}{T_n'(x_{kn})}$$

and note that

$$g(x_{in})=0,\quad g'(x_{in})=\begin{cases}1 & \text{if } i=k\\ 0 & \text{if } i\neq k\end{cases}$$

and

$$g''(x_{in})=\begin{cases}3x_{kn}/(1-x_{kn}^2) & \text{if } i=k\\ 0 & \text{if } i\neq k,\end{cases}$$

on applying (3.5) we obtain (3.1). The proofs of (3.2) and (3.3) are similar, so we omit the details. The proof of (3.4) is on the following lines. Since

$$\int_{-1}^{1}\frac{(1-x^2)(x-x_{kn})l_{kn}^2(x)l_{kn}'(x)}{(1-x_{kn}^2)}(1-x^2)^{-1/2}\,dx=$$

$$=\frac{1}{3}\int_{-1}^{1}\frac{(1-x^2)^{1/2}(x-x_{kn})}{(1-x_{kn}^2)}\frac{d}{dx}l_{kn}^3(x)\,dx=$$

$$=-\frac{1}{3}\int_{-1}^{1}\frac{l_{kn}^3(x)}{(1-x_{kn}^2)}\left((1-x^2)^{1/2}-\frac{x(x-x_{kn})}{(1-x^2)^{1/2}}\right)dx=$$

$$=-\frac{1}{3}\int_{-1}^{1}\frac{l_k^3(x)}{(1-x_{kn}^2)}\left(\frac{2(1-x^2)-(1-xx_{kn})}{(1-x^2)^{1/2}}\right)dx=$$

$$=-\frac{2}{3}\int_{-1}^{1}\frac{(1-x^2)}{(1-x_{kn}^2)}l_{kn}^3(x)(1-x^2)^{-1/2}\,dx+\frac{1}{3}\int_{-1}^{1}\frac{(1-xx_{kn})}{(1-x_{kn}^2)}l_{kn}^3(x)(1-x^2)^{-1/2}\,dx.$$

Now applying (3.2) and (3.3) we obtain (3.4). This proves the lemma.

Lemma 3.2. *For* $k=1,2,\dots,n$ *we have*

(3.6)
$$\int_{-1}^{1}l_{kn}'(t)(1-t^2)^{-1/2}\,dt=\frac{\pi}{n}\left[T_n'(x_{kn})-\frac{x_{kn}}{1-x_{kn}^2}\right],$$

and

(3.7)
$$\int_{-1}^{1}tl_{kn}''(t)(1-t^2)^{-1/2}\,dt=$$
$$=\frac{\pi}{n}\frac{x_{kn}}{1-x_{kn}^2}+\frac{\pi}{2}nT_n'(x_{kn})-\frac{(2+x_{kn}^2)}{(1-x_{kn}^2)}\int_{-1}^{1}l_{kn}'(t)(1-t^2)^{-1/2}\,dt.$$

Proof. It is well known that

(3.8)
$$l_{kn}(x)=\frac{1}{n}+\frac{2}{n}\sum_{r=1}^{n-1}T_r(x_{kn})T_r(x)$$

and

(3.9) $$T'_{2r}(x) = 4r \sum_{i=1}^{r} T_{2i-1}(x), \quad T'_{2r-1}(x) = (2r-1)\left[1+2 \sum_{i=1}^{r} T_{2i}(x)\right].$$

Therefore

(3.10) $$\int_{-1}^{1} l'_{kn}(t)(1-t^2)^{-1/2}\,dt = \frac{2\pi}{n} \sum_{r=1}^{n/2} (2r-1)T_{2r-1}(x_{kn}).$$

But a simple computation shows that

(3.11) $$2 \sum_{r=1}^{[n/2]} (2r-1)T_{2r-1}(x_{kn}) = T'_n(x_{kn}) - x_{kn}/(1-x_{kn}^2).$$

From (3.10), (3.11) we obtain (3.6). For the proof of (3.7) we first note from (3.8), (3.9)

$$\int_{-1}^{1} tl''_{kn}(t)(1-t^2)^{-1/2}\,dt = \frac{2}{n} \sum_{r=1}^{n/2} T_{2r-1}(x_{kn}) \int_{-1}^{1} tT''_{2r-1}(t)(1-t^2)^{-1/2}\,dt +$$

$$+\frac{2}{n} \sum_{r=1}^{n/2} T_{2r}(x_{kn}) \int_{-1}^{1} tT''_{2r}(t)(1-t^2)^{-1/2}\,dt.$$

But

$$\int_{-1}^{1} tT''_{2r}(t)(1-t^2)^{-1/2}\,dt = 0,$$

and

$$2 \int_{-1}^{1} tT''_{2r-1}(t)(1-t^2)^{-1/2}\,dt = ((2r-1)^2-1) \int_{-1}^{1} T'_{2r-1}(t)(1-t^2)^{-1/2}\,dt =$$

$$= ((2r-1)^3-(2r-1))\pi.$$

Therefore

(3.12) $$\int_{-1}^{1} tl''_{kn}(t)(1-t^2)^{-1/2}\,dt = \frac{\pi}{n} \sum_{r=1}^{n/2} T_{2r-1}(x_{kn})((2r-1)^3-(2r-1)).$$

But a simple computation shows that

(3.13) $$\sum_{r=1}^{n/2} (2r-1)^3 T_{2r-1}(x_{kn}) = \frac{x_{kn}}{1-x_{kn}^2} + \frac{n^2 T'_n(x_{kn})}{2} - \frac{3n(1+x_{kn}^2)}{(1-x_{kn}^2)} \int_{-1}^{1} \frac{l'_{kn}(t)}{(1-t^2)^{1/2}}\,dt.$$

From (3.10), (3.17), (3.13) we obtain (3.7). This proves Lemma 3.2.

4. Proof of Theorem 1. First we will show that

$$\int_{-1}^{1} w_{kn}(t)(1-t^2)^{-1/2}\,dt = \frac{(1-x_{kn}^2)^2}{12n^2}\int_{-1}^{1} l'_{kn}(t)(1-t^2)^{-1/2}\,dt = \tag{4.1}$$
$$= \frac{\pi}{12n^3}(1-x_{kn}^2)^2\left(T_n'(x_{kn})-\frac{x_{kn}}{1-x_{kn}^2}\right).$$

Since

$$T_n^2(x) = (1+T_{2n}(x))/2, \tag{4.2}$$

it follows from (2.6) and orthogonal properties of Tchebycheff polynomials

$$\int_{-1}^{1} w_{kn}(t)(1-t^2)^{-1/2}\,dt =$$
$$= ((1-x_{kn}^2)/12n^2)\int_{-1}^{1}(1+T_{2n}(t))q_{n-1,k}(t)(1-t^2)^{-1/2}\,dt = \tag{4.3}$$
$$= ((1-x_{kn}^2)^2/12n^2)\int_{-1}^{1} q_{n-1,k}(t)(1-t^2)^{-1/2}\,dt.$$

On differentiating (2.7) twice it follows that

$$(1-x^2)\,q''_{n-1,k}(x)-xq'_{n-1,k}(x)+q_{n-1,k}(x) = a_{kn}T_n'(x)+l'_{kn}(x). \tag{4.4}$$

Next, we note that

$$\int_{-1}^{1}((1-x^2)\,q''_{n-1,k}(x)-xq'_{n-1}(x))\,(1-x^2)^{-1/2}\,dx = \tag{4.5}$$
$$= \int_{-1}^{1}(d((1-x^2)^{1/2}q'_{n-1}(x))/dx)\,dx = 0.$$

Therefore on using (4.4) and (4.5) we obtain

$$\int_{-1}^{1} q_{n-1,k}(x)(1-x^2)^{-1/2}\,dx = \tag{4.6}$$
$$= a_{kn}\int_{-1}^{1} T_n'(x)(1-x^2)^{-1/2}\,dx+\int_{-1}^{1} l'_{kn}(x)(1-x^2)^{-1/2}\,dx.$$

We also note that n is an even positive integer. Therefore $T_n'(x)$ is an odd polynomial of x, and it follows that

$$\int_{-1}^{1} T_n'(x)(1-x^2)^{-1/2}\,dx = 0. \tag{4.7}$$

On using (4.6), (4.7) and (4.3) we obtain (4.1). We also obtain from (3.6) the second part of (4.1). Next we will prove that

$$\int_{-1}^{1} v_{in}(x)(1-x^2)^{-1/2}\,dx =$$

(4.8)

$$= -\frac{\pi}{4n}(1-x_{in}^2)\,T'(x_{in})+\left(\frac{3+2(2n^2+1)(1-x_{in}^2)}{12n^2}\right)\int_{-1}^{1}\frac{l'_{in}(t)}{(1-t^2)^{1/2}}\,dt.$$

On using (2.8), (3.1) and (4.2) we obtain

$$\int_{-1}^{1} v_{in}(x)(1-x^2)^{-1/2}\,dx =$$

(4.9)

$$= \frac{\pi}{2n^3}x_{in}+\frac{1}{2T'_n(x_{in})}\int_{-1}^{1}\frac{(1+T_{2n}(t))s_{n-1}(t)}{(1-t^2)^{1/2}}\,dt =$$

$$= \frac{\pi}{2n^3}x_{in}+\frac{1}{2T'_n(x_{in})}\int_{-1}^{1}\frac{s_{n-1}(t)}{(1-t^2)^{1/2}}\,dt.$$

Next, differentiating twice we obtain from (2.9)

(4.10) $$(1-x^2)s''_{n-1}(x)-xs'_{n-1}(x)+s_{n-1}(x) = \alpha_{in}T'_n(x)+\beta_{in}l'_{in}(x)+F'_{in}(x).$$

On using (4.5), (4.7) we obtain

(4.11) $$\int_{-1}^{1}\frac{s_{n-1}(x)}{(1-x)^{1/2}}\,dx = \beta_{in}\int_{-1}^{1}\frac{l'_{in}(x)}{(1-x^2)^{1/2}}\,dx+\int_{-1}^{1}\frac{F'_{in}(x)}{(1-x^2)^{1/2}}\,dx,$$

where β_{in} is given by (2.12) and $F_{in}(x)$ by (2.10). From (2.10) we obtain

$$\int_{-1}^{1}\frac{F'_{in}(x)}{(1-x^2)^{1/2}}\,dx = \int_{-1}^{1}\frac{(1-t^2)l'''_{in}(t)-3tl''_{in}(t)+n^2l'_{in}(t)}{2T'_n(x_{in})(1-t^2)^{1/2}}\,dt =$$

$$= \int_{-1}^{1}\frac{(1-t^2)l'''_{in}(t)-tl''_{in}(t)}{2T'_n(x_{in})(1-t^2)^{1/2}}\,dt+\int_{-1}^{1}\frac{-2tl''_{in}(t)+n^2l'_{in}(t)}{2T'_n(x_{in})(1-t^2)^{1/2}}\,dt =$$

$$= \int_{-1}^{1}\frac{(d/dt)((1-t^2)^{1/2}l''_{in}(t))}{2T'_n(x_{in})}\,dt+\int_{-1}^{1}\frac{-2tl''_{in}(t)+n^2l'_{in}(t)}{2T'_n(x_{in})(1-t^2)^{1/2}}\,dt =$$

$$= \int_{-1}^{1}\frac{-2tl''_{in}(t)+n^2l'_{in}(t)}{2T'_n(x_{in})(1-t^2)^{1/2}}\,dt.$$

Therefore, on using (4.9), (4.11), (2.12) together with the above statement it follows that

$$\int_{-1}^{1} v_{in}(x)\frac{1}{(1-x^2)^{1/2}}\,dx = \frac{\pi}{2n^3}x_{in}-\frac{(1-x_{in}^2)}{2n^2}\int_{-1}^{1}\frac{xl''_{in}(x)}{(1-x^2)^{1/2}}\,dx+$$

(4.12)

$$+(1-x_{in}^2)\left(\frac{1}{4}+\frac{1}{4n^2}\left(\frac{n^2-7}{3}-\frac{5x_{in}^2}{1-x_{in}^2}\right)\right)\int_{-1}^{1}\frac{l'_{in}(t)}{(1-t^2)^{1/2}}\,dt.$$

From (3.7) we have

$$(4.13)\quad \int_{-1}^{1} \frac{t l_{in}''(t)}{(1-t^2)^{1/2}}\,dt = \frac{\pi}{n}\frac{x_{in}}{1-x_{in}^2}+\frac{\pi}{2}\,nT_n'(x_{in})-\frac{2+x_{in}^2}{1-x_{in}^2}\int_{-1}^{1}\frac{l_{in}'(t)}{(1-t^2)^{1/2}}\,dt.$$

Now, on using (4.12) and (4.13) we obtain (4.8). Lastly, from (2.14), (3.2), (3.4), (4.1), (4.8) and (3.7) after simplyfying we obtain

$$(4.14)\quad \begin{aligned}&\int_{-1}^{1} u_{in}(x)\frac{1}{(1-x^2)^{1/2}}\,dx =\\ &= \frac{\pi}{n}\left\{1+\frac{1}{3(1-x_{in}^2)}\left(\frac{1}{n^2}-1\right)-\frac{1}{2n^2(1-x_{in}^2)^2}+\frac{(1-x_{in}^2)T_n''(x_{in})}{4}+\frac{T_n''(x_{in})}{2n^2}\right\}.\end{aligned}$$

From (4.1), (4.8) and (4.14) one can prove Theorem 1.

The proofs of Theorem 2 and Theorem 3 follow easily from Theorem 1, so we omit the details.

References

[1] J. Balázs and P. Turán, Notes on interpolation. II, *Acta Math. Acad. Sci. Hungar.*, **8** (1957), 201—215.

[2] J. Balázs and P. Turán, Notes on interpolation. III, *Acta Math. Acad. Sci. Hungar.*, **9** (1958), 195—213.

[3] G. D. Birkhoff, General mean value and remainder theorems with application to mechanical differentiation and integration, *Trans. Amer. Math. Soc.*, **7** (1906), 107—136.

[4] G. G. Lorentz, K. Jetter, S. D. Riemenschneider, *Birkhoff Interpolation,* Encyclopedia of Mathematics and its applications, Vol. 19, Addison-Wesley Pub. Co. (Reading, Mass., 1983).

[5] C. A. Micehelli and T. J. Rivlin, The Turán's formula and highest precision quadrature rules for Chebyshev coefficients, *I.B.M. J. Res. Develop.*, **16** (1972), 373—379.

[6] R. B. Saxena and A. Sharma, Convergence of interpolatory polynomials (0, 1, 3) interpolation, *Acta Math. Acad. Sci. Hungar.*, **10** (1959), 157—175.

[7] P. Turán, On some open problems of approximation theory, *J. Approx. Theory,* **29** (1980), 23—85.

[8] A. K. Varma, On some open problems of P. Turán concerning Birkhoff Interpolation, *Trans. Amer. Math. Soc.*, **274** (1982), 797—808.

[9] A. K. Varma, Some interpolatory properties of Tchebycheff polynomials; (0, 1, 3) case, *Duke Math. J.*, **28** (1961), 449—462.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF FLORIDA
201 WALKER HALL
GAINESVILLE, FLORIDA 32611, U.S.A.

Acta Sci. Math., 50 (1986), 391—396

Remarks on the strong summability of numerical and orthogonal series by some methods of Abel type

L. REMPULSKA

In this paper we shall prove that Leindler's theorems on the strong summability of orthogonal series, given in [2], are true for the methods $(A; B_n)$ of Abel type.

1. Let $C^\infty(0, 1\rangle$ be the class of real functions defined in $(0, 1\rangle$ and having derivatives of all orders in $(0, 1\rangle$. Denote by $B_n=\{b_k(r; n)\}_{k=0}^n$ a sequence of functions of the class $C^\infty(0, 1\rangle$ and such that

$$b_0(r; n) \equiv 1; \left(\frac{d^p}{dr^p} b_k(r; n)\right)_{r=1} = \begin{cases} 0 & \text{if } p \neq k, \\ (-1)^p & \text{if } p = k, \end{cases} \tag{1}$$

for $k, p=0, 1, \ldots, n$. As in [3] we write

$$R_k(r; B_n) = \sum_{p=0}^{n} b_p(r; n) \frac{d^p}{dr^p} r^k$$

and $\Delta R_k(r; B_n)=R_k(r; B_n)-R_{k+1}(r; B_n)$ for $k=0, 1, \ldots$ and $r\in(0, 1\rangle$. In [3] the following definition is given: A real numerical series

$$\sum_{k=0}^{\infty} u_k \qquad (S_k = u_0+\ldots+u_k) \tag{2}$$

is summable to s by the method $(A; B_n)$ if the series $\sum_{k=0}^{\infty} r^k u_k$ is convergent in $(0, 1)$ and if the function $L(B_n)$,

$$L(r; B_n) = \sum_{k=0}^{\infty} R_k(r; B_n) u_k \equiv \sum_{k=0}^{\infty} \Delta R_k(r; B_n) S_k \tag{3}$$

$(r\in(0, 1))$ satisfies the condition $\lim_{r\to 1-} L(r; B_n)=s$. The classical Abel method, i.e. $(A; B_0)$ method, will be denoted by (A). We shall write $L(r)$ for $L(r; B_0)$.

Received May 22, 1984.

In [3] and [4] there were given fundamental properties of the methods $(A; B_n)$ of summability of numerical and orthogonal series, and some applications of those methods to the Dirichlet problem for some equations of Laplace type. In [3] and [4] it was proved that

Theorem A. *Series* (2) *is summable to s by a method* $(A; B_n)$ *if and only if*

$$\lim_{r\to 1-} (1-r)^p \frac{d^p}{dr^p} L(r) = \begin{cases} s & \text{if } p=0, \\ 0 & \text{if } p=1, \dots, n. \end{cases}$$

If the sequence B_n is defined as follows:

$$b_0(r;\, n) = 1, \quad b_n(r;\, n) = (r-r^2)^n/n!, \tag{4}$$

$$b_k(r;\, n) = b_k(r;\, n-1) + \frac{r-r^2}{n}\left(b_{k-1}(r;\, n-1) + \frac{d}{dr} b_k(r;\, n-1)\right)$$

for $k=1, \dots, n-1$ and $n=0, 1, \dots$, then

$$L(r;\, B_n) = (1-r)^{n+1} \sum_{k=0}^{\infty} \binom{k+n}{n} r^k S_k$$

for $n=0, 1, \dots$ and $r\in\langle 0, 1)$ ([3], [4]).

Moreover in [3] it was proved that

$$\Delta R_k(r;\, B_n) = \sum_{p=0}^{n} W_p(r;\, B_n) \frac{d^p}{dr^p} r^k \tag{5}$$

for $r\in(0, 1\rangle$, $k=0, 1, \dots$ and $n\geqq 0$, if $W_p(B_n)$ are some functions of the class $C^\infty(0, 1\rangle$ with

$$\left(\frac{d^q}{dr^q} W_p(r;\, B_n)\right)_{r=1} = 0 \quad \text{for} \quad p, q = 0, 1, \dots, n. \tag{6}$$

From (5)—(6) and from the Taylor formula for $W_p(B_n)$ we obtain

Lemma 1. *Let* $r_0\in(0, 1)$. *Then, for every sequence* B_n, *there exist positive constants* $M_1(r_0)$ *and* $M_2(r_0)$ *depending on* r_0 *such that*

$$M_1(r_0)(1-r)^{n+1}(k+1)^n r^k \leqq |\Delta R_k(r; B_n)| \leqq M_2(r_0)(1-r)^{n+1}(k+1)^n r^k$$

for $k=0, 1, \dots$ *and* $r\in\langle r_0, 1)$.

2. We shall say that series (2) is strongly $(A; B_n)$-summable to s with exponent $q>0$ if the function $H(B_n, q)$,

$$H(r;\, B_n,\, q) = \sum_{k=0}^{\infty} |\Delta R_k(r;\, B_n)|\,|S_k - s|^q \tag{7}$$

$(r\in\langle 0, 1))$ satisfies the condition

$$\lim_{r\to 1-} H(r;\, B_n,\, q) = 0. \tag{8}$$

By (7), (8) and Lemma 1, we obtain

Lemma 2. *Series* (2) *is strongly* $(A; B_n)$*-summable to* s *with exponent* $q>0$ *if and only if*

$$\lim_{r\to 1-}(1-r)^{n+1}\sum_{k=0}^{\infty}(k+1)^n r^k |S_k-s|^q = 0. \tag{9}$$

Lemma 2 implies

Corollary 1. *For a fixed* n, *the methods* $(A; B_n)$, *for the strong summability of numerical series* (2) *are equivalent, i. e. if* B_n *and* B_n^* *are two sequences having properties* (1), *then* $\lim_{r\to 1-} H(r; B_n, q)=0$ *if and only if* $\lim_{r\to 1-} H(r; B_n^*, q)=0$.

Corollary 2. *If series* (2) *is strongly* $(A; B_n)$*-summable to* s *with exponent* $q_1>0$, *then it is strongly* $(A; B_n)$*-summable to* s *with every exponent* $0<q<q_1$.

The next statement is obvious:

Lemma 3. *If series* (2) *is strongly* $(C, 1)$*-summable to* s *with exponent* $q>0$, *i.e.*

$$\lim_{n\to\infty}(1/(n+1))\sum_{k=0}^{n}|S_k-s|^q = 0,$$

then

$$\lim_{n\to\infty}(1/(n+1)^p)\sum_{k=0}^{n}(k+1)^{p-1}|S_k-s|^q = 0$$

for every $p>1$.

Applying Lemma 3, we shall prove

Lemma 4. *If series* (2) *is strongly* $(C, 1)$*-summable to* s *with exponent* $q>0$, *then condition* (9) *is satisfied for* $n=0, 1, \dots$.

Proof. If (2) is strongly $(C, 1)$-summable with exponent $q>0$, then $|S_k-s|^q= =o(k)$. Hence the series $\sum_{k=0}^{\infty}(k+1)^n r^k|S_k-s|^q$ is convergent in $\langle 0, 1)$ and for $n= =0, 1, \dots$. Applying the Abel transformation, we get

$$(1-r)^{n+1}\sum_{k=0}^{\infty}(k+1)^n r^k|S_k-s|^q = (1-r)^{n+2}\sum_{k=0}^{\infty}(k+1)^{n+1}r^k l_k$$

for $r\in\langle 0, 1)$ and $n=0, 1, \dots$, where

$$l_k = (1/(k+1)^{n+1})\sum_{p=0}^{k}(p+1)^n|S_p-s|^q.$$

By Lemma 3 and by Toeplitz's theorem ([1], p. 14), we obtain (9) for $n=0, 1, \dots$. Thus the proof is complete.

Lemma 5. *Suppose that for series* (2) *condition* (9) *holds with* $n=p+1$ $(p\in N)$ *and with some exponent* $q>0$. *Then* (9) *also holds with* $n=p$ *and with exponent* q.

Proof. Let

$$U_n(r;\ q) = (1-r)^{n+1}\sum_{k=0}^{\infty}(k+1)^n r^k |S_k - s|^q$$

for $r\in\langle 0, 1)$. Hence

$$rU_p(r;\ q) = (1-r)^{p+1}\int_0^r (1-t)^{-p-2}U_{p+1}(t;\ q)\,dt$$

for $r\in\langle 0, 1)$. But,

$$\int_0^r (1-t)^{-p-2}U_{p+1}(t;\ q)\,dt = o\big((1-r)^{-p-1}\big)\quad (\text{as } r\to 1-)$$

if $\lim\limits_{r\to 1-} U_{p+1}(r;q)=0$. This proves our statement.

Lemmas 2 and 5 prove

Theorem 1. *For a fixed integer* $n\geqq 0$, *the following conditions are equivalent for every numerical series* (2), *for every* $q>0$ *and every sequence* B_n: (*here* $H(r;q)\equiv \equiv H(r;B_0,q)$).

(a) $\lim\limits_{r\to 1-} H(r;\ B_n,q) = 0,$

(b) $\lim\limits_{r\to 1-} (1-r)^{n+1}\sum\limits_{k=0}^{\infty}(k+1)^n r^k |S_k - s|^q = 0,$

(c) $\lim\limits_{r\to 1-} (1-r)^p \dfrac{d^p}{dr^p} H(r;\ q) = 0$ *for* $m = 0, 1, \dots, n.$

3. Let $\{\varphi_k(x)\}_{k=0}^{\infty}$ be a real and orthonormal system on the interval $\langle 0, 1\rangle$. We shall consider the strong summability of orthogonal series

(10) $$\sum_{k=0}^{\infty} c_k\varphi_k(x)\quad\text{with}\quad \sum_{k=0}^{\infty} c_k^2 < \infty$$

by the methods $(A;B_n)$. The strong summability of (10) by the methods $(A;B_n)$, defined by the sequence (4), was examined by L. Leindler [2].

Let $S_k(x)=\sum\limits_{p=0}^{k} c_p\varphi_p(x)$ and let f be the function given by the Riesz—Fischer theorem, having expansion (10). By $L(r,x;B_n)$ and $H(r,x;B_n,q)$ with $s=f(x)$ $\big(r\in\langle 0,1),\ x\in\langle 0,1\rangle\big)$ we denote the functions as in (3) and (7) but for series (10). As usual ([1]) we say that two methods of summability are equivalent in L^2 if the summability of series (10) in a set E of positive measure by one of those methods implies the summability of (10) to the same sum almost everywhere in E by the other method.

In [3] we proved the following

Theorem B. *The methods* $(A; B_n)$, $n=0, 1, \dots,$ *and the Cesàro* $(C, 1)$ *method of summability for orthogonal series* (10) *are equivalent in* L^2.

In [2] L. Leindler proved

Theorem C. *If orthogonal series* (10) *is Abel-summable to* $f(x)$ *in* $\langle 0, 1\rangle$ *almost everywhere, then*

$$\lim_{r\to 1-} (1-r)^{n+1} \sum_{k=0}^{\infty} \binom{k+n}{n} r^k |S_k(x)-f(x)|^q = 0$$

for any $n\in N$ *and* $q>0$ *in* $\langle 0, 1\rangle$ *almost everywhere.*

Applying Theorem C and Corollary 1, or arguing as in [2], we obtain

Theorem 2. *If orthogonal series* (10) *is* (A)*-summable to* $f(x)$ *in* $\langle 0,1\rangle$ *almost everywhere, then it is strongly* $(A; B_n)$*-summable to* $f(x)$ *in* $\langle 0, 1\rangle$ *almost everywhere with every exponent* $q>0$ *and every sequence* B_n $(n=0, 1, \dots)$.

Applying Lemma 1 and arguing as in the proof of Theorem 5 given in [2], we can prove

Theorem 3. *Suppose that* α *and* q *are two positive numbers and* B_n $(n\geqq 0)$ *is a sequence having properties* (1). *If the coefficients of series* (10) *satisfy the condition*

$$\sum_{k=1}^{\infty} c_k^2 k^{2\alpha} < \infty,$$

then

$$H(r, x; B_n, q) = o_x((1-r)^{\alpha})$$

if $q\alpha<1$; *and*

$$H(r, x;\, B_n, q) = \begin{cases} o_x((1-r)^{\alpha}) & \text{if } n+1 > q\alpha, \\ o_x((1-r)^{\alpha}|\log(1-r)|^{1/q}) & \text{if } n+1 = q\alpha, \\ O_x((1-r)^{(n+1)/q}) & \text{if } n+1 < q\alpha \end{cases}$$

in the case $q\alpha\geqq 1$ *but* $0<q\leqq 2$, *almost everywhere in* $\langle 0, 1\rangle$ *as* $r\to 1-$.

References

[1] S. Kaczmarz and H. Steinhaus, *Theory of orthogonal series*, Gosudarstv. Izdat. Fiz.-Mat. Lit. (Moscow, 1958). (Russian)

[2] L. Leindler, On the strong and very strong summability and approximation of orthogonal series by generalized Abel method, *Studia Sci. Math. Hungar.*, 16 (1981), 35—43.

[3] L. Rempulska, On some summability methods of the Abel type, *Comment. Math. Prace Mat.*, in print.

[4] L. Rempulska, Some properties and applications of summability methods of the Abel type, *Funct. Approximatio Comment. Math.*, **14** (1983), 17—22.

TECHNICAL UNIVERSITY OF POZNAŃ
INSTITUTE OF MATHEMATICS
3 A PIOTROWO STREET
60—965 POZNAŃ, POLAND

Acta Sci. Math., 50 (1986), 397—403

Behavior of the extended Cauchy representation of distributions

DRAGIŠA MITROVIĆ

1. Introduction. There is an interesting correspondence between the spaces $\mathcal{O}'_\alpha=\mathcal{O}'_\alpha(\mathbf{R})$ of distributions and the class of functions that are analytic in the complex plane $\mathbf{C}$ with a boundary on $\mathbf{R}$, except for a set of points lying in $\mathbf{C}-\mathbf{R}$, and vanish at the point of infinity. In the present paper we make a study of this correspondence. As we shall see it depends essentially on the support of distributions, order relation of included functions, and their distributional boundary value in either half plane

$$\Delta^+=\{z\in\mathbf{C}\colon \operatorname{Im}(z)>0\},\quad \Delta^-=\{z\in\mathbf{C}\colon \operatorname{Im}(z)<0\},\quad z=x+iy.$$

The problem under study is motivated by some facts from the theory of integrals of the Cauchy type. Namely, to every function $u\colon \mathbf{R}\to\mathbf{C}$ Hölder continuous with compact support equal K there corresponds the function

$$\hat{u}(z)=\frac{1}{2\pi i}\int_{-\infty}^{\infty}\frac{u(t)}{t-z}\,dt,\quad z\bar{\in}K.$$

If $v(z)\equiv\hat{u}(z)$, then: (1) v is an analytic function in $\mathbf{C}-K$; (2) $v(z)$ has the boundary values $v^+(x)$ and $v^-(x)$ in $\mathbf{C}$; (3) $v(z)=O(1/|z|)$ as $|z|\to\infty$. Conversely, given a function v which satisfies the conditions (1)—(3), then it is the Cauchy integral of some u with $\operatorname{supp} u=K$.

If T is a distribution, then the notation T_t is used to indicate that the testing functions on which T is defined have t as their variable. The pairing between a testing function space and its dual is denoted by $\langle T,\varphi\rangle$. The space of $C^\infty=C^\infty(\mathbf{R})$ functions having compact support is denoted by $\mathcal{D}=\mathcal{D}(\mathbf{R})$; its dual $\mathcal{D}'=\mathcal{D}'(\mathbf{R})$ is the space of Schwartz distributions on $\mathbf{R}$. As regards the general properties of the spaces $\mathcal{O}_\alpha$ and $\mathcal{O}'_\alpha$ we refer to [1].

2. Definitions. In order to describe the correspondence in question in a condensed form we introduce some classes of functions.

Received April 10, 1984.

Let K be a closed subset of $\mathbf{R}$ and let $\{a_1, a_2, \ldots, a_n\}$ $(n \in N)$ be a finite set of distinct complex points lying in $\Delta^+ U \Delta^-$. A function f is said to belong to the class $\{M\}$ if

(m.1) f is analytic in the domain $\mathbf{C}-(K \cup \{a_1, a_2, \ldots, a_n\})$, a_k being a pole of order α_k $(k=1, 2, \ldots, n)$;

(m.2) $f(z)$ converges (weakly) in either half plane to a $\mathcal{D}'$-boundary value;

(m.3) $$f(z) = O(1/|z|) \quad \text{as} \quad |z| \to \infty.$$

We use the notation $\{M_c\}$ for the class of functions in $\{M\}$ that satisfy (m.1) when K is a compact set. Also, a function f is said to belong to the class $\{M_0\}$ if it satisfies the conditions (m.1), (m.2) and the condition

(m.4) $$f(\infty) \equiv \lim_{z \to \infty} f(z) = 0.$$

Thus we have the inclusions $\{M_c\} \subset \{M\} \subset \{M_0\}$. Further, the class of functions that satisfy the conditions (m.1)—(m.3) when the set of poles is empty is denoted by $\{A\}$. The class $\{A_c\}$ is the subclass of $\{A\}$ relative to compact set K in (m.1). If here the condition (m.3) is replaced by (m.4) we have the class $\{A_0\}$.

Remark. The arbitrary sets involved in (m.1) are not necessarily the same for all functions in a class defined above.

Now denote by $R(z)$ a meromorphic function, vanishing at the point $z=\infty$, with prescribed poles $a_1, a_2, \ldots, a_n$ (in $\Delta^+ \cup \Delta^-$) and their principal parts. Let $T \in \mathcal{O}'_\alpha$ $(\alpha \geqq -1)$. The function $\hat{F}$ from $\mathbf{C}-(\operatorname{supp} T \cup \{a_1, a_2, \ldots, a_n\})$ to $\mathbf{C}$ defined by

(1) $$\hat{F}(z) = (1/2\pi i)\langle T_t, 1/(t-z)\rangle + R(z)$$

will be referred to as *the extended Cauchy representation of* T.

Let us observe that every function f in $\{A_0\}$ ($\{M_0\}$) is sectionally analytic in $\mathbf{C}$ with a boundary on $\mathbf{R}$ (except for the poles), that is, it can be decomposed into two independent functions $f^+(z)$ and $f^-(z)$ such that $f(z)=f^+(z)$ for $z \in \Delta^+$, $f(z)=f^-(z)$ for $z \in \Delta^-$ (the half planes being punctured at the points of poles).

3. Main result. We need the following

Lemma [5]. *If $f^+(z)$ is a function analytic in Δ^+ with $f^+(z)=O(1/|z|)$ as $|z| \to \infty$ in Δ^+, and if $f^+(x+i\varepsilon)$ converges to $\mathcal{D}'$-boundary value f_x^+ as $\varepsilon \to +0$, then*: 1) *f_x^+ belongs to $\mathcal{O}'_\alpha$ for all $\alpha<0$;* 2) *$f^+(x+i\varepsilon)$ converges to $\mathcal{O}'_\alpha$-boundary value f_x^+ as $\varepsilon \to +0 (\alpha<0)$;* 3) *$f_x^+$ generates the Cauchy representation*

(2) $$(1/2\pi i)\langle f_t^+, 1/(t-z)\rangle = \begin{cases} f^+(z) & \text{for } z \in \Delta^+, \\ 0 & \text{for } z \in \Delta^-. \end{cases}$$

For a function $f^-(z)$ analytic in Δ^- and satisfying here the conditions similar to ones of $f^+(z)$, we have

$$(3)\qquad -(1/2\pi i)\langle f_t^-, 1/(t-z)\rangle = \begin{cases} f^-(z) & \text{for } z\in\Delta^-, \\ 0 & \text{for } z\in\Delta^+. \end{cases}$$

The distributional version of the previous discussion concerning the integral of the Cauchy type leads to the following

Theorem. *Let* $T\in\mathcal{O}'_\alpha$ $(\alpha\geqq-1)$ *with* supp $T=K$ *and let* $\{a_1, a_2, \ldots, a_n\}$ $(n\in N)$ *be a set of distinct complex points located in* $\Delta^+\cup\Delta^-$. *If* $f(z)\equiv\hat{F}(z)$, *then* $f\in\{M_0\}$. *Conversely, given an* $f\in\{M\}$, *then it is the extended Cauchy representation of some* $T\in\mathcal{O}'_\alpha$ *for all* $\alpha\in[-1, 0)$ *with* supp $T=K$.

Proof. Consider the direct part of the theorem. To prove the statement (m.1) it suffices to note that the Cauchy representation $\hat{T}(z)$ of T is an analytic function in the domain $\mathbf{C}-K$ ([1, p. 56]). The statement (m.2) follows directly from [4, Theorem 2]:

$$f_x^+ = \hat{F}_x^+ = T_x/2-(1/2\pi i)(T_x*\mathrm{vp}\,1/x)+R(x),$$

$$f_x^- = \hat{F}_x^- = -T_x/2-(1/2\pi i)(T_x*\mathrm{vp}\,1/x)+R(x).$$

Observe that the rational function $R(x)$ is a regular distribution (in $\mathcal{O}'_\alpha$ for all $\alpha<0$). As regards the statement (m.4) it is a simple consequence of the hypothesis $R(\infty)=0$ and the fact that every sequence of functions $\varphi_n(t)=1/(t-z_n)$ converges to zero in $\mathcal{O}'_\alpha$ $(\alpha\geqq-1)$ as $z_n\to\infty(n\to\infty)$.

Conversely, suppose given an $f\in\{M\}$. Then in view of Lemma the assertions (m.2) and (m.3) together imply $f_x^+\in\mathcal{O}'_\alpha$, $f_x^-\in\mathcal{O}'_\alpha$ for all $\alpha<0$. Now define $T_x=f_x^+-f_x^-$. Since $(f_x^+-f_x^-)\in\mathcal{O}'_\alpha$ for all $\alpha<0$ and the Cauchy kernel belongs to $\mathcal{O}'_\alpha$ for all $\alpha\geqq-1$, we can associate to T the Cauchy representation

$$\hat{T}(z) = (1/2\pi i)\langle T_t, 1/(t-z)\rangle = (1/2\pi i)\langle (f_t^+-f_t^-), 1/(t-z)\rangle$$

for all $\alpha\in[-1, 0)$. Clearly, $\hat{T}$ is analytic in $\mathbf{C}-$supp T and vanishes at the point $z=\infty$; moreover, it is easy to show that in this situation $\hat{T}(z)=O(1/|z|)$ as $|z|\to\infty$. To prove that f is the extended Cauchy representation of T first we shall show that the function H from $\mathbf{C}-(\text{supp } T\cup\{a_1, a_2, \ldots, a_n\})$ to $\mathbf{C}$ defined by

$$(4)\qquad H(z) = f(z)-\hat{T}(z)$$

is meromorphic in $\mathbf{C}$. In fact, after a simple computation we have

$$\langle (H_x^+-H_x^-), \varphi\rangle = \langle (f_x^+-f_x^-), \varphi\rangle = \langle (\hat{T}_x^+-\hat{T}_x^-), \varphi\rangle$$

for all $\varphi\in\mathcal{D}$. Since $T_x=\hat{T}_x^+-\hat{T}_x^-$ it follows

$$(5)\qquad \langle H_x^+, \varphi\rangle = \langle H_x^-, \varphi\rangle$$

for all $\varphi\in\mathcal{D}$. Further, let $\Delta=\{z\in\mathbf{C}\colon -d<\operatorname{Im}(z)<d\}$ be the strip of the half height

$$d=\operatorname{Min}\{|\operatorname{Im}(a_1)|, |\operatorname{Im}(a_2)|, \ldots, |\operatorname{Im}(a_n)|\}.$$

Let (a, b) be an arbitrary finite open interval in $\mathbf{R}$, E^+ and E^- two open rectangles contained in Δ which have (a, b) as a common edge. Evidently, H is an analytic function in Δ except the boundary on $\mathbf{R}$ consisting of the set $\operatorname{supp} T\cup K$. Applying the distributional analytic continuation principle ([6], [3, p. 244]) the equality (5) implies that the function H is analytic in $E^+\cup(a, b)\cup E^-$, and consequently, in all of Δ. Thus H is analytic everywhere in $\mathbf{C}$ except for the poles a_k of f, and as a meromorphic function which vanishes at the point of infinity it may be written uniquely in the form

$$H(z)=\sum_{k=1}^{n}\sum_{p=1}^{\alpha_k} B_{k,p}/(z-a_k)^p, \tag{6}$$

where the coefficients $B_{k,p}$ must be determined (by means of f). Since the function $\hat{T}$ is analytic in $\mathbf{C}-\operatorname{supp} T$, using Theorem on the partial fraction expansion of rational functions ([2]) from (4) we get

$$B_{k,\alpha_k-m}=(1/m!)\lim_{z\to a_k} d^m[(z-a_k)^{\alpha_k}f(z)]/dz^m \tag{7}$$

$(m=0, 1, 2, \ldots, \alpha_k-1)$. Returning to equality (4) with (6) and (7) it follows the representation

$$f(z)=(1/2\pi i)\langle T_t, 1/(t-z)\rangle+\sum_{k=1}^{n}\sum_{p=1}^{\alpha_k} B_{k,p}/(z-a_k)^p. \tag{8}$$

So we have established that the given $f\in\{M\}$ is the extended Cauchy representation of $T_x=(f_x^+-f_x^-)\in\mathcal{O}'_\alpha$ for all $\alpha\in[-1, 0)$. Next we have to prove that $\operatorname{supp} T=K$. First let K be a closed proper subset of $\mathbf{R}$. Since the function f is analytic on the open set $\mathbf{R}-K$, it follows that

$$\langle f_x^+, \varphi\rangle=\lim_{\varepsilon\to+0}\langle f^+(x+i\varepsilon), \varphi\rangle=\lim_{\varepsilon\to+0}\langle f^-(x-i\varepsilon), \varphi\rangle=\langle f_x^-, \varphi\rangle$$

for all φ with support disjoint from K $(\varphi\in\mathcal{D}(\mathbf{R}-K))$. Thus $\langle(f_x^+-f_x^-), \varphi\rangle=$ $=\langle T_x, \varphi\rangle=0$ for all such φ. Hence we may conclude that $\operatorname{supp} T=K$. The assumption that $\operatorname{supp} T\subset K$ properly leads to the conclusion that there exists an open interval $(a, b)\subset(K-\operatorname{supp} T)$ on which $(f_x^+-f_x^-)$ is zero of $\mathcal{D}'((a, b))$. Therefore (by the analytic continuation principle) f would be analytic on $(\mathbf{R}-K)\cup(a, b)$ contrary to the hypothesis. For the same reason $\operatorname{supp} T=\mathbf{R}$ in the case $K=\mathbf{R}$. Finally suppose that there exists a distribution $S\in\mathcal{O}'_\alpha$ $(\alpha\geqq-1)$ distinct from T and such that $f(z)=\hat{S}(z)+H(z)$ for $z\in\mathbf{C}-(K\cup\{a_1, a_2, \ldots, a_n\})$. According to [4, Theorem 2] we have $f_x^+-f_x^-=\hat{S}_x^+-\hat{S}_x^-=S_x$. Hence $T_x=S_x$ on $\mathcal{D}$ and this implies $T_x=S_x$ on $\mathcal{O}_\alpha$ (since $\mathcal{D}$ is dense in $\mathcal{O}_\alpha$ for all $\alpha\in\mathbf{R}$). But this contradicts the hypothesis on S. Thus, the distribution T is unique. The proof is complete.

In particular, if all poles a_k of the function f are simple $(k=1, 2, \dots, n)$, then in the representation (8) instead of double sum we have

$$\sum_{k=1}^{n} \operatorname{res}[f(z), a_k]/(z-a_k).$$

4. Consequences. First assume that the set of poles of the function $\hat{F}$ is empty. In this case $\hat{F}$ is reduced to the Cauchy representation $\hat{T}$ of T. Thus we have at once

Corollary 1: *Let* $T\in\mathcal{O}'_\alpha$ $(\alpha\geqq -1)$ *with* $\operatorname{supp} T=K$. *If* $f(z)\equiv\hat{T}(z)$, *then* $f\in\{A_0\}$. *Conversely, given an* $f\in\{A\}$, *then it is the Cauchy representation of some* $T\in\mathcal{O}'_\alpha$ *for all* $\alpha\in[-1, 0)$ *with* $\operatorname{supp} T=K$.

Nevertheless we can prove the second part of this Corollary directly, that is, without intervention of the meromorphy. In fact, since the distributions f_x^+ and f_x^- belong to $\mathcal{O}'_\alpha$ $(\alpha<0)$ we may define $T_x=f_x^+-f_x^-$. As T_x is a linear continuous functional on $\mathcal{O}_\alpha$ generating the Cauchy integral $\hat{T}(z)$ we have for all $\alpha\in[-1, 0)$

$$\hat{T}(z) = (1/2\pi i)\langle f_t^+, 1/(t-z)\rangle-(1/2\pi i)\langle f_t^-, 1/(t-z)\rangle.$$

Using the formulas (2) and (3) we get at once the required result

$$\hat{T}(z) = \begin{cases} f^+(z) & \text{for} \quad z\in\Delta^+, \\ f^-(z) & \text{for} \quad z\in\Delta^-, \end{cases}$$

that is, $f(z)=\hat{T}(z)$. So we have proved by Lemma that the given $f\in\{A\}$ is the Cauchy representation of some $T\in\mathcal{O}'_\alpha$.

Denote in Schwartz's notation by $\mathcal{E}'=\mathcal{E}'(\mathbf{R})$ the space of distributions on $\mathbf{R}$ with compact support (recall that $\mathcal{E}'\subset\mathcal{O}'_\alpha$ for all $\alpha\in\mathbf{R}$, but an $T\in\mathcal{O}'_\alpha$ with compact support belongs to $\mathcal{E}'$). From Theorem we derive

Corollary 2. *Let* $T\in\mathcal{E}'$ *with* $\operatorname{supp} T=K$. *If* $f(z)\equiv\hat{F}(z)$, *then* $f\in\{M_c\}$. *Conversely, given an* $f\in\{M_c\}$, *then it is the extended Cauchy representation of some* $T\in\mathcal{E}'$ *with* $\operatorname{supp} T=K$.

We have to comment only the assertion (m.3). The function $\hat{F}$ around the point $z=0$ has the Laurent expansion of the form

$$\hat{F}(z) = c_0+c_1/z+c_2/z^2+\dots$$

which converges uniformly and absolutely outside the smallest disk containing K and all poles a_k $(k=1, 2, \dots, n)$. The fact that $\hat{F}(z)$ vanishes as $z\to\infty$ implies that $c_0=0$, and the required result follows at once.

Consequently, to every pair $(T, \{a_1, a_2, \dots, a_n\})$ with $T\in\mathcal{E}'$, $n\in N$, there corresponds an $f\in\{M_c\}$ and to every $f\in\{M_c\}$ there corresponds a pair $(T, \{a_1, a_2, \dots, a_n\})$ with $T\in\mathcal{E}'$, $n\in N$.

Corollary 3. *Let* $T\in\mathscr{E}'$ *with* $\operatorname{supp} T=K$. *If* $f(z)\equiv\hat{T}(z)$, *then* $f\in\{A_c\}$. *Conversely, given an* $f\in\{A_c\}$, *then it is the Cauchy representation of some* $T\in\mathscr{E}'$ *with* $\operatorname{supp} T=K$.

Thus one can place distributions in $\mathscr{E}'$ into a one-to-one correspondence with functions in $\{A_c\}$.

It may happen that $f\equiv\hat{F}\in\{M\}$ (any given $f\in\{M\}$ is the extended Cauchy representation of some $T\in\mathcal{O}'_\alpha$ $(\alpha\geqq-1)$ with $\operatorname{supp} T=K$). For example, the function f defined by

$$f(z)\equiv\hat{F}(z)=(1/2\pi i)\langle \mathrm{vp}\, 1/t,\, 1/(t-z)\rangle+1/(z-i)$$

belongs to $\{M\}$ with $K=R$. This follows from

$$f^+(z)=1/2z+1/(z-i),\quad z\in\Delta^+-\{i\},$$

$$f^-(z)=-1/2z+1/(z-1),\quad z\in\Delta^-$$

with $f_x^+=1/2(x+i0)+1/(x-i)$, $f_x^-=1/2(x-i0)+1/(x-i)$. Conversely, given $f^+(z)$ and $f^-(z)$ we reconstruct $f(z)$ starting with $f_x^+-f_x^-=\mathrm{vp}\, 1/x$.

In addition, by means of the second part of Theorem we solve the following boundary value

Problem 1. *Let T be a given distribution in* $\mathcal{O}'_\alpha$ $(\alpha\geqq-1)$. *Find a function* $f\in\{M\}$ *whose $\mathscr{D}'$-boundary values f_x^+ and f_x^- satisfy the condition* $f_x^+-f_x^-=T_x$ *on* $\mathbf{R}$.

The general solution is given by (8), where $B_{k,p}$ are arbitrary real or complex coefficients.

It is of interest to sketch the following results: if in Corollaries 2—3 we replace (via condition (m.2)) the convergence in the $\mathscr{D}'$ topology by one in $\mathcal{O}'_\alpha$ for a given $\alpha\in[-1,0)$, we get new corollaries 2.1—3.1 respectively.

Fact 1. Corollaries 2—3 are equivalent to Corollaries 2.1—3.1.

To prove this first observe that $f\in\{M\}$ remains in $\{M\}$ if we substitute the convergence in $\mathscr{D}'$ for one in $\mathcal{O}'_\alpha$ $(\alpha\in\mathbf{R})$. Next, we use the representation (8) or Lemma.

Also, if in Problem 1 we replace $T\in\mathcal{O}'_\alpha$ $(\alpha\geqq-1)$ by $T\in\mathcal{O}'_\alpha$ $(-1\leqq\alpha<0)$ and the convergence in $\mathscr{D}'$ by one in $\mathcal{O}'_\alpha$, we come to

Problem 1.1. *Let T be a given distribution in* $\mathcal{O}'_\alpha$ $(-1\leqq\alpha<0)$. *Find a function* $f\in\{M\}$ *whose $\mathcal{O}'_\alpha$-boundary values f_x^+ and f_x^- satisfy the condition* $f_x^+-f_x^-=T_x$ *on* $\mathbf{R}$.

Fact 2. Problem 1 with $T\in\mathcal{O}'_\alpha$ $(-1\leqq\alpha<0)$ is equivalent to Problem 1.1.

Similarly, substituting under previous conditions the class $\{M\}$ for $\{M_c\}$ and $\{A_c\}$ we come to an equivalent Problem 1.2 and Problem 1.3, respectively.

References

[1] H. J. BREMERMANN, *Distributions, complex variables, and Fourier transforms,* Addison-Wesley (New York, 1965).

[2] J. W. DETTMAN, *Applied complex variables,* Macmillan (New York, 1965).

[3] A. MARTINEAU, Distributions et valeurs au bord des fonctions holomorphes, in: *Proceedings of an International Summer Institute held in Lisbon* (1964).

[4] D. MITROVIĆ, The Plemelj distributional formulas, *Bull. Amer. Math. Soc.*, 77 (1971), 562—563.

[5] D. MITROVIĆ, A distributional representation of strip analytic functions, *Internat. J. Math. Math. Sci.*, 5 (1982), no. 1, 1—9.

[6] W. RUDIN, *Lectures on the edge-of-the wedge theorem,* Amer. Math. Soc. (Providence, R. I., 1971).

UNIVERSITY OF ZAGREB
FACULTY OF TECHNOLOGY
DEPARTMENT OF MATHEMATICS
PIEROTTIJEVA 6
ZAGREB, YUGOSLAVIA

Acta Sci. Math., 50 (1986), 405—410

On Stieltjes transform of distributions behaving as regularly varying functions

V. MARIĆ, M. SKENDŽIĆ, A. TAKAČI

1. Introduction. The asymptotics of the Stieltjes transform of distributions T with support in $[0, \infty)$ belonging to a subset, specified below, of the space of (Schwartz) distributions, whose behavior (at zero) is of the type $T \sim x^{\nu} \log^{j} x_{+}$ in the Lojasiewicz sense, or (at ∞) in the Sebastiao E Silva sense, is studied by LAVOINE and MISRA [1], [2]. The aim of this paper is to extend their results to the cases when $T \sim x^{\nu} L_0(x)_{+}$, $x \to 0^{+}$ and $T \sim x^{\nu} L(x)$, $x \to \infty$. Here L_0 and L belong to the class of slowly varying functions (s.v.f.) introduced by KARAMATA [3] in 1930.

A real valued function $L(x)$ is slowly varying at infinity, if it is positive, measurable on $[a, \infty)$ for some $a > 0$, and such that for each $\lambda > 0$

$$\lim_{x \to \infty} L(\lambda x)/L(x) = 1. \tag{1.1}$$

A function $L_0(x)$ is s.v. at zero if $L_0(1/x)$ is s.v. at infinity. E.g. all positive functions tending to positive constants are s.v. at infinity, products of powers of iterated logarithms, the function $(1/x) \int^{x} dt/\ln t$, are such, etc.

Slowly varying functions are of frequent occurrence in various branches of analysis (Fourier analysis, number theory, differential equations, Tauberian theorems) and of stochastic processes, whenever more information than the mere fact of convergence is needed. Here we also emphasize the use of s.v.f. in the theory of distributions.

Also, the function $R(x) = x^{\nu} L(x)$ is called regularly varying at infinity with index ν.

1.1. Following [2] we denote by $J'(r)$, $\operatorname{Re} r > -1$, the space of distributions T with support in $[0, \infty)$, admitting the decomposition

$$T = B + D^{k} f(x) \tag{1.2}$$

Received April 28, 1984.

where k is a non-negative integer, D^k is the distributional differentiation operator of order k, $f(x)$ is a locally integrable function with support in $[a, \infty)$ for some $a \geqq 0$ and such that

$$\int^{\infty} |f(x)x^{-r-k-1}|\,dx < \infty, \tag{1.3}$$

and B is a distribution with support in $[0, a]$. Notice that T is a tempered distribution.

Further, the Stieltjes transform of $T \in J'(r)$ is defined by

$$F(s) = \mathcal{S}_s\{T\} = \langle T_x, (x+s)^{-r-1}\rangle = \tag{1.4}$$

$$= \langle B_x, (x+s)^{-r-1}\rangle + \frac{\Gamma(r+k+1)}{\Gamma(r+1)} \int_a^{\infty} f(x)(x+s)^{-r-k-1}\,dx, \quad s \in C \setminus (-\infty, 0].$$

Here the first term on the right-hand side in the second line of (1.4) exists since $(x+s)^{-r-1}$ coincides on the support of B with some infinitely differentiable function.

Throughout the paper we assume that $s > 0$.

The following result of Lavoine and Misra [2] is needed in the sequel:

Lemma 1.1. *Let B be a distribution with support in $[a, b]$ where $0 < a < b < \infty$, then*

$$\mathcal{S}_s\{B\} \to \langle B, x^{-r-1}\rangle, \quad s \to 0^+; \tag{1.5}$$

if $a=0$ then

$$s^{r+1}\mathcal{S}_s\{B\} \to \langle B_x, 1\rangle, \quad s \to \infty. \tag{1.6}$$

1.2. We next give the basic properties of the slowly varying functions ([3], [4]) needed in the paper.

(i) The limit (1.1) holds uniformly in any finite interval $[a, b]$, $a > 0$.

(ii) For any $p > 0$ there holds

$$x^p L(x) \to \infty, \quad x^{-p} L(x) \to 0, \quad x \to \infty.$$

The next property is a Theorem of Aljančić, Bojanić and Tomić [5], and represents our main tool for the proofs.

(iii) Let $g(x)$ be a Lebesgue integrable function on an interval I. Then

$$\int_I g(x)L(\lambda x)\,dx \sim L(\lambda) \int_I g(x)\,dx, \quad \lambda \to \infty,$$

provided that one of the following conditions is satisfied:

A) $I = [0, b]$, $b < \infty$, and the integrals

$$\int_{0+}^{b} g(x)L(\lambda x)\,dx, \quad \int_{0+}^{b} x^{-p}|g(x)|\,dx \tag{1.7}$$

converge; the latter for some $p > 0$.

B) $I=[a,\infty)$, $a>0$, and the integral

$$\int_a^\infty x^p |g(x)|\,dx \tag{1.8}$$

converges for some $p>0$.

C) $I=[0,\infty)$ and (1.7) and (1.8) both hold.

1.3. Among the various definitions of the behaviour (at zero and at infinity) of generalized functions, we use the following two:

Definition 1.1 (cf. LOJASIEWICZ [6]). The distribution $T\in\mathcal{D}'_+$ behaves at zero as $x^\nu L_0(x)_+$, i.e.

$$T\sim x^\nu L_0(x)_+,\quad x\to 0^+,\quad \operatorname{Re}\nu>-1,$$

if there exist $a>0$ and a distribution R with support in $[0,a]$ such that $T=x^\nu L_0(x)_+ + R$ for $x\in[0,a]$ and

$$t^{-\nu-1}L_0^{-1}(t)_+\langle R_x, \varphi(x/t)\rangle\to 0,\quad t\to 0^+ \tag{1.9}$$

for each function φ infinitely differentiable on some neighborhood of $[0,\infty)$. The subscript "+" means that the functions bearing it are equal to zero for $x\leqq 0$.

Definition 1.2 (cf. SEBASTIAO E SILVA [7]). The distribution $T\in\mathcal{D}'_+$ behaves at infinity as $x^\nu L(x)$ i.e.

$$T\sim x^\nu L(x),\quad x\to\infty$$

if for some $a>1$ and $x\in[a,\infty)$, there holds $T_x=D^k f(x)$ and

$$L^{-1}(x)x^{-k-\nu}f(x)\to\frac{1}{(\nu+1)_k},\quad x\to\infty$$

(where $(\nu+1)_k=(\nu+1)(\nu+2)\dots(\nu+k)$, $k>1$ and $(\nu+1)_0=1$).

2. Results. We prove the following two theorems giving the behavior of the Stieltjes transform $\mathcal{S}_s$ of the distribution $T\in J'(r)$ at zero and at infinity respectively. Notice that $\mathcal{S}_s\{T\}=F(s)$ is a (holomorphic) function and the asymptotics has to be understood accordingly.

Theorem 2.1. *Let* $\operatorname{Re}r>-1$, $\operatorname{Re}\nu>-1$, $\operatorname{Re}(r-\nu)>0$, *further let* $L_0(x)$ *be slowly varying at zero and* $T\in J'(r)$. *If*

$$T\sim x^\nu L_0(x)_+,\quad x\to 0^+ \tag{2.1}$$

then

$$\mathcal{S}_s\{T\}\sim B(\nu+1, r-\nu)s^{\nu-r}L_0(s),\quad s\to 0^+.$$

Theorem 2.2. *Let* $\operatorname{Re} r > -1$, $\operatorname{Re} \nu > -1$, $\operatorname{Re}(r-\nu) > 0$, *further let* $L(x)$ *be slowly varying at* ∞ *and* $T \in J'(r)$. *If*

$$T \sim x^{\nu} L(x), \quad x \to \infty \tag{2.2}$$

then

$$\mathcal{S}_s\{T\} \sim B(\nu+1, r-\nu) s^{\nu-r} L(s), \quad s \to \infty.$$

By taking in Theorem 2.1 $L_0(x) = 1$ and $L_0(x) = \ln^j x$, $j \in N$, one obtains respectively Theorems 3.2. I in [1] and 2.1 in [2] for $\operatorname{Re} \nu > -1$ of Lavoine and Misra. Similarly, by taking in Theorem 2.2, $k=0$, $L(x)=1$, $L(x)=\ln^j x$ one obtains their Theorem 5.1. III in [1] and Theorem 3.1 in [2].

3. Proofs. Proof of Theorem 2.1. By virtue of (1.2) and (2.1) one has

$$T = x^{\nu} L_0(x)_+ + R + B + D^k f(x); \tag{3.1}$$

here the supports of R, B, $f(x)$ are in $[0, a]$, $[a, b]$, $[b, \infty)$ respectively, and R satisfies (1.9); $L_0(x)$ may be chosen conveniently in $[a, \infty)$. We apply the Stieltjes transform to the distributions at both sides of (3.1), multiply by $\left(s^{\nu-r} L_0(s)\right)^{-1}$, and then estimate each summand of the right-hand side.

To treat the first term, put in the occurring integral $s = 1/\lambda$, $x = s/u$, and to the obtained integral

$$\lambda^{r-\nu} \int_0^{\infty} u^{r-\nu-1}(1+u)^{-r-1} L(\lambda u)\, du \quad \text{with} \quad L(x) = L_0(1/x)$$

apply the result 1.2 (iii) C). Thus for the first term one obtains

$$\left(s^{\nu-r} L_0(s)\right)^{-1} \int_0^{\infty} \frac{x^{\nu} L_0(x)\, dx}{(x+s)^{r+1}} \to B(\nu+1, r-\nu), \quad s \to 0^+.$$

To complete the proof one has to show that the remaining three terms tend to zero with s. The second term is such due to (1.9) and to the property 1.2 (ii) (with $L_0(s) = L(1/s)$). The third term is such due to (1.5) of Lemma 1.1, and to the property 1.2 (ii) as above. The fourth term is

$$\left(s^{\nu-r} L_0(s)\right)^{-1} \mathcal{S}_s\{D^k f(x)\} = \left(s^{\nu-r} L_0(s)\right)^{-1} \frac{\Gamma(k+r+1)}{\Gamma(r+1)} \int_b^{\infty} f(x)(x+s)^{-r-k-1}\, dx.$$

The occurring integral is bounded by an absolute constant and $\left(s^{\nu-r} L_0(s)\right)^{-1} \to 0$, $s \to 0^+$, as before, which completes the proof.

Proof of Theorem 2.2. Because of (2.2) the function $f(x)$ in (1.2) is of the form

$$f(x) = c x^{k+\nu} L(x)\left(1 + \omega(x)\right),$$

where $\omega(x)$ is a locally integrable function with support in $[a, \infty)$ and such that $\omega(x)\to 0$, $x\to\infty$, and $c^{-1}=(\nu+1)_k$. Hence

$$T = cD^k\{x^{k+\nu}L(x)_+\}+B^1+D^k\{x^{k+\nu}L(x)\,\omega(x)\} \tag{3.2}$$

where B^1 is with support in $[0, a]$; $L(x)$ may be chosen conveniently in $[0, a]$. Now we proceed as in the proof of Theorem 2.1, i.e. apply the Stieltjes transform to both sides of (3.2), multiply by $(s^{\nu-r}L(s))^{-1}$ and estimate each term on the right-hand side separately.

We apply to the integral occurring in the first term the result 1.2 (iii) C), yielding

$$\mathcal{S}_s\{D^k x^{k+\nu}L(x)\}\sim B(\nu+1, r-\nu)s^{\nu-r}L(s), \quad s\to\infty.$$

Now we see that the second term tends to zero for $s\to\infty$; this time we have to use 1.2 (ii) and (1.6) of Lemma 1.1. The third term I_3, say, is estimated as follows

$$|I_3| \leqq (L(s))^{-1}\int\limits_0^{a/\sqrt{s_0}} s^{\mathrm{Re}\,\nu+k}L(sy)\,dy+(L(s))^{-1}M(s)\int\limits_{a/\sqrt{s_0}}^{\infty} y^{\mathrm{Re}(\nu-r)-1}L(sy)\,dy$$

where $M(s)=\sup|\omega(sy)|$ for $y\geqq as_0^{-1/2}$. Hence $|I_3|\leqq\varepsilon_1+\varepsilon_2$ for $s\geqq s_0$, since $|\omega(sy)|$ is bounded, $M(s)\to 0$, $s\to\infty$, and by applying to the occurring integrals (1.2), (iii) A) and (1.2), (iii), B) respectively.

Remark. By altering slightly the method of proof used above we can obtain similar results when the distributions behave as some functions more general than the regularly varying ones. Thus the following result holds:

Theorem 3.1. *Let* $\mathrm{Re}\,r>-1$, $T\in J'(r)$, *and let* $h(x)$ *be such that for some* $p>0$, $\int\limits_a^{\infty}|h(x)x^{p+\nu}|dx$ *converges* $(a>0)$. *If*

$$T\sim x^{\nu}h(x), \quad x\to\infty$$

then $\mathcal{S}_s\{T\}\sim ms^{-r-1}$, $s\to\infty$, *where m is a constant that can be calculated.*

References

[1] J. Lavoine et O. P. Misra, Théorèmes abéliens pour la transformation de Stieltjes des distributions, *C.R. Acad. Sci. Paris*, Série A, **279** (1974), 99—102.

[2] J. Lavoine and O. P. Misra, Abelian theorems for the distributional Stieltjes transformation, *Math. Proc. Cambridge, Philos. Soc.*, **86** (1979), 287—293.

[3] J. Karamata, Sur un mode de croissance régulière des fonctions, *Mathematica (Cluj)*, **4** (1930), 38—53.

[4] E. SENETA, *Regulary varying functions*, Lecture Notes in Math. 508, Springer-Verlag (Berlin—Heidelberg—New York, 1976).

[5] S. ALJANČIĆ, R. BOJANIĆ, M. TOMIĆ, Sur la valeur asymptotique d'une classe des intégrales définies, *Publ. de l'Inst. Math. Beograd*, VII (1954), 81—94.

[6] S. LOJASIEWICZ, Sur la valeur d'une distribution en un point, *Studia Math.*, 16 (1957), 1—36.

[7] J. SEBASTIAO E SILVA, Integrals and order of growth of distributions, *Inst. Gulbenkian de Ciencia Lisboa*, 35 (1964), 7124.

INSTITUTE OF MATHEMATICS
UNIVERSITY OF NOVI SAD
NOVI SAD, YUGOSLAVIA

Acta Sci. Math., 50 (1986), 411—419

Normal approximation for sums of non-identically distributed random variables in Hilbert spaces

V. V. ULYANOV

The problem of estimation of the speed of convergence in the central limit theorem in Hilbert spaces has a history of nearly twenty years. In most papers the speed is studied on the class of balls with a fixed center. This is an important and natural class of sets, but it is not very rich. However, in contrast to the finite dimensional case, one has shown that in Hilbert spaces (in general) it is impossible to construct estimates which are uniform with respect to rich classes, since not even on the class of all balls the speed of convergence in the central limit theorem in Hilbert spaces is uniform (see e.g. [1], p. 70).

The first estimates of order $n^{-1/2}$ on balls with a fixed center under the assumption of finiteness of some moments and without any other additional restrictions (such as independence of coordinates) were obtained by GÖTZE [2]. Following Götze's paper a series of papers appeared, mostly based on Götze approach, which improved and extended his results (see e.g. [3], [4], [5]).

The estimates for the case of independent not necessarily identically distributed random variables (i.non-i.d.r.v.) were obtained by BENTKUS [5] (see Theorem 3.3 in [5] or the condition (5) and the estimate (6) below). The previous results for the case of i.non-i.d.r.v. were obtained by BERNOTAS, PAULAUSKAS [6], ULYANOV [7], [8]. However, corollaries from results [6]—[8] for i.i.d.r.v. give estimates of the order $n^{-1/6}$.

In the present paper we construct estimates on some classes of Borel sets, in particularly on balls with a fixed center, for the case of i.non-i.d.r.v. Our results improve the corresponding estimates of BENTKUS [5], have the "natural" form and at the same time they are obtained under somewhat different conditions. One of the main features of our estimates is that they require minimal moment conditions and their dependence on the (truncated) moments has an explicit form. We shall use the methods of [2], [3], [5] and some ideas from [7].

Received July 2, 1984 and in revised form, April 5, 1985.

In what follows, H is a real separable Hilbert space with inner product (x, y), $x, y \in H$, and norm $|x|=(x, x)^{1/2}$, $D: H \to H$ is a bounded symmetric operator

$$|D| = \sup_{x \neq 0} |(Dx, x)|/|x|^2,$$

$h: H \to R^1$ is a linear continuous functional,

$$W(x) = (Dx, x)+h(x),$$

$$A_{a,r} = \{x \in H: W(x+a) < r\}, \quad r \geqq 0, \quad a \in H;$$

$$N_n = \{1, 2, \ldots, n\}.$$

Let $A: H \to H$ be a bounded symmetric operator with eigenvalues $\sigma_1 \geqq \sigma_2 \geqq \ldots$. We write $A \in G(\beta, k)$, $\beta > 0$, if and only if $\sigma_k \geqq \beta$. Denote $\operatorname{tr} A = \sum_{i=1}^{\infty} \sigma_i$. Let X be a random variable with values in H. Denote by $\tilde{X}$ the symmetrization of X, i.e. $\tilde{X} = X_1 - X_2$, where X_1 and X_2 are independent copies of X. For $\delta > 0$ put

$$X^\delta = X \cdot I_{\{|x| < \delta\}}, \quad X_\delta = X \cdot I_{\{|x| \geqq \delta\}},$$

where I_B is the indicator of the set $B \subset H$. By c (resp. $c(\cdot)$) with or without indices, we denote constants (resp. constants depending only on quantities in the parentheses); the same symbol may stand for different constants. Let λ_i, $i \in N_n$, be any numbers and $\Theta \subset N_n$. Put $\lambda(\Theta) = \sum_{i \in \Theta} \lambda_i$.

Our main result is the following theorem.

Theorem. *Let X_i, $i \in N_n$, be i.non-i.d.r.v. with values in H with zero means and covariance operators A_i, $i \in N_n$, respectively. Assume that there exists an operator A_0 such that*

(1) $$A_i = \lambda_i A_0, \quad \lambda_i \geqq 0, \quad i \in N_n,$$

$$\sum_{i=1}^{n} \lambda_i = 1$$

and

$$\sum_{i=1}^{n} \operatorname{tr} A_i = 1, \quad (DA_0)^2 \in G(\beta, 13), \quad \textit{for some} \quad \beta > 0.$$

Put $S_n = \sum_{i=1}^{n} X_i$, and let Z be a Gaussian $(0, A_0)$ r.v. with values in H,

Then for all $n \geqq 1$

(2) $$\Delta = \sup_{r \geqq 0} |P(S_n \in A_{a,r}) - P(Z \in A_{a,r})| \leqq c_1(1+|a|^3)(\Lambda_2 + L_3),$$

where $\Lambda_2 = \sum_{i=1}^{n} E|X_{i1}|^2$, $L_3 = \sum_{i=1}^{n} E|X_i^1|^3$, $c_1 = c_1(|D|, |h|, \beta)$.

Corollary 1. *Assume that* $A_0\in G(\beta, 13)$ *for some* $\beta>0$. *Then for all* $n\geqq 1$

$$\Delta_1 = \sup_{r\geqq 0}\left|P(|S_n+a| < r)-P(|Z+a| < r)\right| \leqq c(\beta)(1+|a|^3)(\Lambda_2+L_3). \tag{3}$$

Corollary 2. *Assume that* $A_1=A_2=\ldots=A_n$, $A_1\in G(\beta, 13)$, *for some* $\beta>0$, $E|X_i|^3\leqq L$, $i\in N_n$. *Then for all* $n\geqq 1$

$$\Delta_1 \leqq c(\beta)(1+|a|^3)Ln^{-1/2}. \tag{4}$$

Remarks. 1. Our theorem improves estimate (3.14) of Theorem 3.3 in [5]. For completeness we recall the corresponding result proved by Bentkus [5] (Theorem 3.3).

Let X_i, $i\in N_n$, *be i.non-i. d.r.v. with values in* H *with zero means and covariance operators* A_i, $i\in N_n$, *respectively. Assume that* $\sum_{i=1}^{n}\operatorname{tr} A_i=1$ *and there exists a nonnegative operator* $A_0\colon H\to H$ *such that*

$$A_i \geqq A_0/n, \quad i\in N_n, \tag{5}$$

and $(DA_0)^2\in G(\beta, k)$, *for some* $\beta>0, k>0$. *Let* q, ε, B *be any numbers*, $q>2$, $0<\varepsilon\leqq 1$, $B>0$. *Then there exists a constant* $c=c(\varepsilon)$ *such that if* $k\geqq c$ *then for all* $n\geqq 1$

$$\Delta \leqq c_2(1+|a^3|)\big(\Lambda_2+L_3+(n/\sigma_q^2)^{\varepsilon-1}+\big(n\max_{1\leqq i\leqq n} E|X_{i1}|^2\big)^B\big), \tag{6}$$

where $c_2=c_2(\beta, \varepsilon, q, |D|, |h|, B)$, $\sigma_q=\max\limits_{1\leqq i\leqq n}(n^{q/2}E|X_i^1|^q)^{1/(q-2)}$.

Thus our theorem shows that the last two terms on the right hand side of (6) may be omitted. At the same time we replace condition (5) by condition (1).

2. Estimate (4) was obtained earlier by Yurinskiĭ [3].

The proof of the theorem is based on a series of lemmas.

Lemma 1. *Let* λ_i, $i\in N_n$, *be nonnegative numbers such that*

$$\sum_{i=1}^{n}\lambda_i = 1, \quad \max_{1\leqq i\leqq n}\lambda_i \leqq 1/3.$$

Then there exist sets Θ_1, Θ_2 *such that* $\Theta_1\cap\Theta_2=\emptyset$, $\Theta_1\cup\Theta_2=N_n$, $\lambda(\Theta_i)\geqq 1/3$, $i=1, 2$.

Proof. It is easy to see that there exists an i_0 such that $\sum_{i=1}^{i_0}\lambda_i\leqq 1/3$, $\sum_{i=1}^{i_0+1}\lambda_i>1/3$. Put $\Theta_1=\{1, 2, \ldots, i_0+1\}$. The above construction implies Lemma 1.

Lemma 2. *Let* λ_i, $i\in N_n$, *be nonnegative numbers such that*

$$\sum_{i=1}^{n}\lambda_i = 1, \quad \max_{1\leqq i\leqq n}\lambda_i \leqq R \leqq 1/3.$$

Let M_i, $i \in N_n$, *be any nonnegative numbers. Then there exists* $\Theta \subset N_n$ *such that* $R \leqq \lambda(\Theta) \leqq 3R$, $M(\Theta)/\lambda(\Theta) \leqq \sum_{i=1}^{n} M_i$.

Proof. As in Lemma 1 it is easy to see that there exist $\Theta_1, \Theta_2, \dots, \Theta_m$, such that $\Theta_i \cap \Theta_j = \emptyset$, $i \neq j$, $\bigcup_{i=1}^{m} \Theta_i = N_n$ and $R \leqq \lambda(\Theta_i) \leqq 3R$, $i = 1, 2, \dots, m$. Assume that the ratios $M(\Theta_i)/\lambda(\Theta_i)$ are arranged in the following way

$$\frac{M(\Theta_{i_1})}{\lambda(\Theta_{i_1})} \leqq \frac{M(\Theta_{i_2})}{\lambda(\Theta_{i_2})} \leqq \dots \leqq \frac{M(\Theta_{i_m})}{\lambda(\Theta_{i_m})}.$$

This implies

$$M(\Theta_{i_1})/\lambda(\Theta_{i_1}) \leqq \sum_{i=1}^{n} M_i.$$

Put $\Theta = \Theta_{i_1}$. Lemma 2 is proved.

Lemma 3. *Let* X *be a r.v. with values in* H *and* $EX=0$, $E|X|^2 < \infty$. *Then for any* $z \in H$, $\delta > 0$

(7) $$E((\tilde{X}^1)^\delta, z)^2 \geqq 2E(X, z)^2 - 4|z|^2(E|X_1|^2 + 2E|X^1|^3/\delta),$$

where $\tilde{X}^1 = (X^1)^\sim$, $X_1 = XI_{\{|x| \leqq 1\}}$.

Proof. We have

(8) $$E((\tilde{X}^1)^\delta, z)^2 = E(\tilde{X}^1, z)^2 - E((\tilde{X}^1)_\delta, z)^2 \geqq E(\tilde{X}^1, z)^2 - |z|^2 E|(\tilde{X}^1)_\delta|^2.$$

(9) $$E(\tilde{X}^1, z)^2 = 2E(X^1, z)^2 - 2(E(X^1, z))^2.$$

As in (8) we get

(10) $$E(X^1, z)^2 \geqq E(X, z)^2 - |z|^2 E|X_1|^2.$$

Since $EX=0$,

(11) $$E(X^1, z) = -E(X_1, z).$$

Moreover

(12) $$|E(X_1, z)| \leqq |z|(E|X_1|^2)^{1/2}.$$

From (9)—(12) it follows that

(13) $$E(\tilde{X}^1, z)^2 \geqq 2E(X, z)^2 - 4|z|^2 E|X_1|^2.$$

Furthermore

(14) $$E|(\tilde{X}^1)_\delta|^2 \leqq E|\tilde{X}^1|^3/\delta \leqq 8E|X^1|^3/\delta.$$

Using (8), (13) and (14) we get (7). Lemma 3 is proved.

Lemma 4. *Let* A, B *be any bounded linear operators in* H, $A \geqq 0$. *Then the sets of non-zero eigenvalues of the operators* AB, BA *and* $A^{1/2}BA^{1/2}$ *are the same (taking into account the multiplicity of the eigenvalues).*

Proof. See VAKHANIA [9], p. 84, or Lemma 2.3 in [5].

Lemma 5. *Let $X_i(Y_i)$, $i\in N_n$, be i.non-i.d.r.v. (independent Gaussian r.v.) with values in H with zero means and covariance operators A_i, $i\in N_n$, respectively. Let R be any positive number, $R\leqq 1/6$. Assume that*

$$A_i=\lambda_i A_0,\quad \lambda_i\geqq 0,\quad i\in N_n,$$

(15) $$\sum_{i=1}^{n}\operatorname{tr}A_i=\sum_{i=1}^{n}\lambda_i=1,\quad (DA_0)^2\in G(\beta,13)\quad \textit{for some}\quad \beta>0,$$

$$\max_{1\leqq i\leqq n}\lambda_i\leqq R,\quad \Lambda_2\leqq R_\beta/(200|D|^2).$$

Let $\Theta_1\cap\Theta_2=\emptyset$, $\Theta_1\cup\Theta_2=N_n$. *Put* $A=\sum_{i\in\Theta_1}\operatorname{cov}V_i$, $B=\sum_{i\in\Theta_2}\operatorname{cov}V_i$, *where*

(16) $$V_i=(\tilde{X}_i^1)^\delta\quad or\quad V_i=\tilde{Y}_i,\quad i\in N_n,\quad \delta=400|D|^2(\Lambda_2+L_3)/\beta.$$

Then there exists Θ_1 *such that*

(17) $$(DAD)^{1/2}B(DAD)^{1/2}\in G(R_\beta/2,13),\quad \operatorname{tr}A\leqq 12R.$$

Proof. Let $x\in H$. Put $z=(DAD)^{1/2}x$,

$$\Lambda_2(\Theta)=\sum_{i\in\Theta}E|X_{i1}|^2,\quad L_3(\Theta)=\sum_{i\in\Theta}E|X_i^1|^3.$$

Note that

(18) $$E(\tilde{Y}_i,x)^2=2E(Y_i,x)^2.$$

From (18) and Lemma 3 it follows that

(19) $$(Bz,z)\geqq 2(A_0z,z)\lambda(\Theta_2)-4|z|^2\big(\Lambda_2(\Theta_2)+2L_3(\Theta_2)/\delta\big).$$

Furthermore

(20) $$|z|^2\leqq 4|D|^2|x|^2\lambda(\Theta_1).$$

By Lemma 4 the sets of the non-zero eigenvalues of the operators $(DAD)^{1/2}A_0(DAD)^{1/2}$ and $A_0^{1/2}DADA_0^{1/2}$ are the same. Put $y=DA_0^{1/2}x$. As in (19) we have

(21) $$(Ay,y)\geqq 2(A_0y,y)\lambda(\Theta_1)-4|y|^2\big(\Lambda_2(\Theta_1)+2L_3(\Theta_1)/\delta\big).$$

Moreover

(22) $$|y|^2\leqq 4|D|^2|x|^2\lambda(\Theta_2)\leqq 4|D|^2|x|^2.$$

Since under the assumptions of Lemma 5 $(DA_0)^2\in G(\beta,13)$, by Lemma 4 we have

(23) $$A_0^{1/2}DA_0DA_0^{1/2}\in G(\beta,13).$$

By Lemma 2 there exists a Θ_1 such that

(24) $$R\leqq\lambda(\Theta_1)\leqq 3R,\quad L_3(\Theta_1)/\lambda(\Theta_1)\leqq L_3.$$

Now from (15), (21), (22) and (24) we have for any $x\in H$

$$(25)\quad \begin{aligned}(A_0^{1/2}DADA_0^{1/2}x, x) &\geqq 2(A_0^{1/2}DA_0DA_0^{1/2}x, x)R-16|D|^2|x|^2(\Lambda_2+2L_3(\Theta_1)/\delta) \geqq \\ &\geqq 2(A_0^{1/2}DA_0DA_0^{1/2}x, x)R-\beta R|x|^2.\end{aligned}$$

From (23), (25) and the results of §4, Ch. X in [10] it follows that

$$(26)\qquad A_0^{1/2}DADA_0^{1/2}\in G(R\beta, 13).$$

Similarly from (15), (16), (19), (20), (24), (26) and from the simple inequality

$$(27)\qquad \operatorname{tr} A \leqq 4\lambda(\Theta_1)$$

we get (17). Lemma 5 is proved.

Proof of Theorem. Put $\hat{S}_n^1=X_1^1+X_2^1+\dots+X_n^1$, $F(r)=P(S_n\in A_{a,r})$, $F_1(r)=P(\hat{S}_n^1\in A_{a,r})$, $b(r)=P(Z\in A_{a,r})$. Let $f(t)$ and $g(t)$ be the Fourier—Stieltjes transforms of F_1 and b respectively. Using the inequality

$$|b'(r)| \leqq \int_{-\infty}^{\infty} g(t)\,dt,$$

the symmetrization inequality (see Lemma 2.1 in [3]) and Lemma 2.4 in [5] we get

$$(28)\qquad |b'(r)| \leqq c(|D|, \beta)(1+|a|^3).$$

It is easy to see that

$$(29)\qquad |F(r)-F_1(r)| \leqq \sum_{i=1}^{n} P(|X_i| \geqq 1) \leqq \Lambda_2.$$

By Theorem 2, §1, Ch. 5 in [11], from (28), (29) we have for any $T>0$

$$(30)\quad |P(S_n\in A_{a,r})-P(Z\in A_{a,r})| \leqq \Lambda_2+c(1+|a|^3)/T+\int_{-T}^{T} |t|^{-1}|f(t)-g(t)|\,dt.$$

Now we estimate $|f(t)-g(t)|$. By Theorem 4.6 in [12] we have

$$(31)\qquad |f(t)-g(t)| \leqq c(|t|+|t|^3)(1+|a|^3)(\Lambda_2+L_3)\varkappa(t),$$

where

$$\varkappa(t) = \sup_V \sup_M \inf_{\bigcup_{i=1}^{5} B_i=N_n\setminus M} \sup_{1\leqq q\leqq 4} \inf_{B\subset B_q} E^{1/4} \exp\Big\{2it\Big(\sum_{j\in B} DV_j, \sum_{j\in B_q\setminus B} V_j\Big)\Big\},$$

and M is any subset of N_n containing not more than one element, $V=(V_1, V_2, \dots, V_n)$, $V_i=\tilde{X}_i^1$ or $V_i=\tilde{Y}_i$, $i\in N_n$, $Y_1, Y_2, \dots, Y_n$ are independent Gaussian r.v.'s with zero means and covariance operators $A_1, A_2, \dots, A_n$, respectively.

Denote $\Lambda = \Lambda_2 + L_3$. The left hand side of (2) is not greater than 1. Hence we may assume without loss of generality that

(32) $$\Lambda \leqq c_3,$$

where c_3 is a constant small enough. In fact, if (32) is not true then (2) is obvious with $c_1 \geqq 1/c_3$. We may also assume that

(33) $$\max_{1 \leqq i \leqq n} \lambda_i \leqq \Lambda^{2/25}.$$

In fact, if there exists an i_0 such that $\lambda_{i_0} > \Lambda^{2/25}$ then tr $A_{i_0} > \Lambda^{2/25}$. Since tr $A_{i_0} = E|X_{i_0}|^2$ we have $E|X_{i_0}|^2 > \Lambda^{2/25}$. Moreover,

$$E|X_{i_0}|^2 = E|X_{i_0 1}|^2 + E|X_{i_0}^1|^2.$$

Now we consider two possible cases.

Case 1. $E|X_{i_0 1}|^2 \geqq E|X_{i_0}^1|^2$. Then $E|X_{i_0 1}|^2 > \Lambda^{2/25}/2$. Since $\Lambda \geqq E|X_{i_0 1}|^2$ we have $\Lambda > \Lambda^{2/25}/2$, that is $\Lambda > (1/2)^{25/23}$. This contradicts assumption (32).

Case 2. $E|X_{i_0}^1|^2 > E|X_{i_0 1}|^2$. Then $E|X_{i_0}^1|^2 > \Lambda^{2/25}/2$. We have

$$\Lambda \geqq \frac{(\Lambda^{2/25}/2)^{3/2}}{(E|X_{i_0}^1|^2)^{3/2}} \cdot \Lambda > \frac{\Lambda^{3/25}}{2^{3/2}} \cdot \frac{E|X_{i_0}^1|^3}{(E|X_{i_0}^1|^2)^{3/2}} \geqq \Lambda^{3/25}/2^{3/2}.$$

Hence $\Lambda > (1/2)^{75/44}$. This also contradicts assumption (32).

Furthermore, from the definition of $\varkappa(t)$, (33) and Lemma 1 it follows that if we denote

(34) $$\delta_1^4 = \inf_{\Theta_1, \Theta_2} E \exp\{2it(\sum_{j \in \Theta_1} DV_j, \sum_{j \in \Theta_2} V_j)\}, \quad \delta_1 > 0,$$

where $\Theta_1 \cap \Theta_2 = \emptyset$ and

(35) $$\sum_{i \in \Theta_1 \cup \Theta_2} \lambda_i \geqq c,$$

then

(36) $$\varkappa(t) \leqq \delta_1.$$

Note that for any symmetric r.v. X, $z \in H$, $\delta > 0$ we have

$$E \exp\{i(z, X)\} \leqq E \exp\{i(z, X^\delta)\}.$$

Therefore

(37) $$\delta_1^4 \leqq \inf_{\Theta_1, \Theta_2} E \exp\{2it(\sum_{j \in \Theta_1} DV_j', \sum_{j \in \Theta_2} V_j')\},$$

where $V_j' = V_j^\delta$ if $V_j = \tilde{X}_j^1$ and $V_j' = V_j$ if $V_j = \tilde{Y}_j$, $j \in \Theta_1 \cup \Theta_2$. By Lemma 2.5 in [5] we get for all t and M that

$$4|D|\delta\varrho|t| \leqq 1, \quad 4|D|M\delta \max\{\gamma, \varrho\} \leqq 1,$$

(38) $$\delta_1^4 \leqq c \inf_{\Theta_1, \Theta_2} (\exp(-\varrho^2/(\mathrm{tr}\, A + \delta\varrho)) + \exp(-\gamma^2/\mathrm{tr}\, B) + \varphi(s)),$$

where $s=\min\{2|t|, M\}$, $\varphi(s)=E\exp\{\mathrm{is}(DU, V)/2\}$, U, V are independent Gaussian r.v.'s with zero means and covariance operators $A=\sum_{j\in\Theta_1}\operatorname{cov} V_j'$ and $B=\sum_{j\in\Theta_2}\operatorname{cov} V_j'$, respectively. From (1.4) in [3] it follows that

$$\varphi(s) = \prod_{j=1}^{\infty}(1+s^2\beta_j/4)^{-1/2}, \tag{39}$$

where $\beta_j, j=1, 2, \ldots$ are the eigenvalues of $(DAD)^{1/2}B(DAD)^{1/2}$.

Now we estimate the right hand side of (38) for different values of t.

Case 1. $|t|\leqq c/(\Lambda\ln(1/\Lambda))$. Put $\gamma=c\ln^{1/2}(1/\Lambda)$, $\varrho=c\ln(1/\Lambda)$, $\delta=c\Lambda$, $M=c/(\Lambda\ln(1/\Lambda))$. From (1), (27) we get

$$\operatorname{tr} A+\operatorname{tr} B\leqq 4. \tag{40}$$

Hence for the above values of $\gamma, \varrho, \delta, M$ we have

$$\exp\left(-\varrho^2/(\operatorname{tr} A+\delta\varrho)\right)+\exp\left(-\gamma^2/\operatorname{tr} B\right)\leqq c\Lambda^c. \tag{41}$$

By Lemma 5 and (32), (33), (35) there exist Θ_1 and a constant c such that

$$(DAD)^{1/2}B(DAD)^{1/2}\in G(c\beta, 13). \tag{42}$$

From (39), (42) we have

$$\varphi(s)\leqq c(1+t^{13})^{-1}. \tag{43}$$

Case 2. $c/(\Lambda\ln(1/\Lambda))\leqq|t|\leqq c/\Lambda$. Put $\gamma=c\ln^{1/2}(1/\Lambda)$, $\varrho=c$, $M=c/(\Lambda\ln(1/\Lambda))$, $\delta=c\Lambda$. By Lemma 5 and (32), (33), (35) there exist Θ_1 and a constant c such that

$$(DAD)^{1/2}B(DAD)^{1/2}\in G(c\Lambda^{2/25}\beta, 13),\quad \operatorname{tr} A\leqq c\Lambda^{2/25}. \tag{44}$$

From (39), (40), (44) we have

$$\delta_1^4\leqq c\left(\Lambda^c+(1+\Lambda^{1/25}/(\Lambda\ln(1/\Lambda)))^{-13}\right)\leqq c\left(\Lambda^c+\Lambda^{312/25}\ln^{13}(1/\Lambda)\right). \tag{45}$$

Furthermore, put $T=c/\Lambda$, $T_1=c/(\Lambda\ln(1/\Lambda))$. From (31), (34), (36), (37), (41), (43), (45) we get

$$\int_{-T}^{T}|t|^{-1}|f(t)-g(t)|\,dt\leqq c(1+|a|^3)\Lambda\int_{-T}^{T}(1+t^2)\varkappa(t)\,dt\leqq \tag{46}$$

$$\leqq c(1+|a|^3)\Lambda\int_{-T}^{T}(1+t^2)\delta_1\,dt\leqq c(1+|a|^3)\Lambda\Big(\int_{-T_1}^{T_1}+\int_{T_1}^{T}+\int_{-T}^{-T_1}\Big)(1+t^2)\delta_1\,dt\leqq$$

$$\leqq c(1+|a|^3)\Lambda\Big(1+\int_{-\infty}^{\infty}t^2(1+t^{13/4})^{-1}\,dt+\Lambda^{0.12}\ln^{13/4}(1/\Lambda)\Big)\leqq c(1+|a|^3)\Lambda.$$

Estimates (30) and (46) imply (2). The theorem is proved.

P r o o f o f C o r o l l a r y 1. This follows from the theorem. To this end it is enough to put $h=0$, $D=I$, the identity operator, and to note that if $A_0 \in G$ $(\beta, 13)$, then $A_0^2 \in G(\beta^2, 13)$.

The proof of Corollary 2 is obvious.

I am grateful to professor J. Mogyoródi for his attention to my work.

References

[1] V. V. Sazonov, *Normal approximation — some recent advances,* Lecture Notes in Math., vol. 879, Springer-Verlag (Berlin, 1981).

[2] F. Götze, Asymptotic expansions for bivariate von Mises functionals, *Z. Wahrsch. Verw. Gebiete,* **50** (1979), 333—355.

[3] V. V. Yurinskiĭ, On the accuracy of Gaussian approximation for the probability of hitting a ball, *Teor. Verojatnost. i Primenen.,* **27** (1982), 270—278.

[4] B. A. Zalesskiĭ, Estimates of the accuracy of normal approximation in a Hilbert space, *Teor. Verojatnost. i Primenen.,* **27** (1982), 279—285.

[5] V. Bentkus, Asymptotic expansions for distributions of sums of independent random elements in a Hilbert space, *Litovsk. Mat. Sb.,* **24** (1984), No. 4, 29—48.

[6] V. Bernotas, V. Paulauskas, Non-uniform estimate in the central limit theorem in some Banach spaces, *Litovsk. Mat. Sb.,* **19** (1979), No. 2, 23—43.

[7] V. V. Ulyanov, On the rate of convergence in the central limit theorem in a real separable Hilbert space, *Mat. Zametki,* **29** (1981), No. 1, 145—153.

[8] V. V. Ulyanov, On the accuracy of closeness estimates for two distributions of sums of random variables with values in some Banach spaces, *Vestnik Moskov. Univ. Ser. 15,* **1981,** No. 1, 50—57.

[9] N. N. Vakhania, *Probability distributions in linear spaces,* Mezniereba (Tbilisi, 1971).

[10] N. Dunford, J. T. Schwartz, *Linear operators. II,* Wiley (New York, 1962).

[11] V. V. Petrov, *Sums of independent random variables,* Springer-Verlag (Berlin, 1975).

[12] V. Bentkus, Asymptotic expansions in the central limit theorem in a Hilbert space, *Litovsk. Mat. Sb.,* **24** (1984), No. 3, 29—50.

MOSCOW STATE UNIVERSITY
FACULTY OF APPLIED MATHEMATICS AND CYBERNETICS
117234 MOSCOW V—234, USSR

Acta Sci. Math., 50 (1986), 421—425

A connection between the unitary dilation and the normal extension of a subnormal contraction

C. R. PUTNAM

1. Introduction and theorem. Let H be an infinite dimensional, separable, complex Hilbert space and let T be a bounded (linear) operator on H. If T is a contraction ($\|T\| \leqq 1$) on H, then, by a well-known result of B. Sz.-Nagy [7] there exists a Hilbert space $K \supset H$ and a unitary operator U on K for which

$$(1.1) \qquad T^n = PU^n|H \quad \text{and} \quad T^{*n} = PU^{*n}|H, \quad n=0, 1, 2, \ldots,$$

where P is the orthogonal projection $P: K \to H$. If K is the least subspace of K which reduces U and contains H (as will be supposed) then U is the (unique) minimal unitary dilation of T. See Halmos [3], Sz.-Nagy and Foiaş [8].

Next, let T be any subnormal operator, so that there exists a Hilbert space $K' \supset H$ and a normal operator N on K' for which $NH \subset H$ and $T = N|H$. Thus, N is a normal extension of T and, if P' denotes the orthogonal projection $P': K' \to H$,

$$(1.2) \qquad T^n = N^n|H \text{ and } T^{*n} = P'N^{*n}|H, \quad n = 0, 1, 2, \ldots.$$

In case K' is the least subspace of K' which reduces N and contains H (as will be supposed) then N is the (unique) minimal normal extension of T. (See Halmos [3] and, for an extensive treatment of subnormal operators, Conway [2].) The operator T is said to be a pure subnormal operator if it has no normal part.

Henceforth, it will be supposed that T is both a contraction and a pure subnormal operator. Let the associated operators U and N defined above have the corresponding spectral resolutions

$$(1.3) \qquad U = \int_C z\,dG_z \quad \text{on } K \text{ and} \quad N = \int_{D^-} z\,dE_z \quad \text{on } K',$$

This work was supported by a National Science Foundation research grant.
Received July 4, 1984.

where D is the unit disk $D=\{z: |z|<1\}$ with closure D^- and $C=\{z: |z|=1\}$. The main object of this note is to point out the following explicit connection between the operators U and N:

Theorem. *Let T be a pure subnormal contraction on H with the minimal unitary dilation U on K and the minimal normal extension N on K' of* (1.3). *Then, for any Borel set β on C and for any vector x in H,*

$$\|E(\beta)x\|^2+\int_D h_\beta(z)\,d\|E_z x\|^2=\|G(\beta)x\|^2, \tag{1.4}$$

where

$$h_\beta(z)=(1/2\pi)\int_{\beta_0}\operatorname{Re}\big(P_z(t)\big)\,dt, \quad \text{with} \quad P_z(t)=(e^{it}+z)/(e^{it}-z) \tag{1.5}$$

and $\beta_0=\{t: 0\leqq t\leqq 2\pi,\ e^{it}\in\beta\}$.

The function $\operatorname{Re}\big(P_z(t)\big)$ is the Poisson kernel and, as is well known, is positive for all $t\in C$, $z\in D$, while $h_\beta(z)$ is harmonic in D.

The formula (1.4) is contained "between the lines" in [6], pp. 333—334, but apparently has not appeared explicitly in the literature. For completeness, the argument will be given below.

As above, let P and P' denote the orthogonal projections $P: K\to H$ and $P': K'\to\to H$, so that, by (1.1) and (1.2), for x in H and $n=0, 1, 2, \dots$, one has $T^n x= =PU^n x=N^n x$ and $T^{*n}x=PU^{*n}x=P'N^{*n}x$. Hence, if $f=f(z)$ is analytic in D and continuous in D^- then

$$\int_{D^-} f\,dE_z x=P\int_C f\,dG_z x \quad \text{and} \quad P'\int_{D^-}\bar f\,dE_z x=P\int_C \bar f\,dG_z x.$$

Consequently, if $h=h(z)$ is any real harmonic function in D which is continuous on D^-, then

$$P'\int_{D^-} h\,dE_z x=P\int_C h\,dG_z x, \quad x\in H.$$

Next, let β be any closed subset of C and let φ be a real-valued continuous function on C satisfying $\varphi=1$ on β and $0\leqq\varphi<1$ on $C-\beta$. Then there exists a function $h(z)$, given by the Poisson integral, which is harmonic in D, continuous in D^-, and satisfies $h=\varphi$ on C. Consequently,

$$P'\Big(\int_D h\,dE_z+\int_C \varphi\,dE_z\Big)x=P\int_C \varphi\,dG_z x, \quad x\in H.$$

On forming inner products with x one obtains

$$\int_C \varphi\,d\|E_z x\|^2+\int_D h\,d\|E_z x\|^2=\int_C \varphi\,d\|G_z x\|^2. \tag{1.6}$$

On replacing φ by $\varphi_n=\varphi^n$ and h by the corresponding h_n, $n=1, 2, \dots$, one sees that $\varphi_1\geqq\varphi_2\geqq\dots$ and the sequence $\{\varphi_n\}$ converges to the characteristic function of β. Similarly, $0\leqq h_n\leqq 1$, $h_1\geqq h_2\geqq\dots$, and $\{h_n\}$ converges to $h_\beta(z)$ of (1.5). Clearly, one has the relation (1.4), when β is closed, and the extension of (1.4) to arbitrary Borel sets β readily follows.

It is known that $\|G_z x\|^2$ is, for each x in H, $x\neq 0$, equivalent to arc length Lebesgue measure on C; see Sz.-Nagy and Foiaş [8], p. 84. The absolute continuity of E_z on C follows from (1.4). (That is, $E(\beta)=0$ whenever β is a Borel set on C having arc length measure zero.) Other proofs of this last result are given in Conway and Olin [2], p. 35, Olin [4] and Putnam [5] (see also [6]).

2. ***U*** **as the sweep of** ***N*****.** It may be noted that (1.4) of the Theorem or, equivalently, (1.6), in which φ is now any continuous function on C and $h=h(z)=\hat{\varphi}(z)$ is its harmonic extension to D^- (via the Poisson integral), can be interpreted in terms of the sweep of a measure. (For the concept of "sweep" see Conway [2], p. 334.) Thus, one has

$$\int_{D^-} \hat{\varphi}\, d\mu = \int_C \varphi\, d\hat{\mu},$$

where $d\mu=d\|E_z x\|^2$ and $d\hat{\mu}=d\|G_z x\|^2$, so that $\hat{\mu}$ on C is the sweep of μ on D^-.

3. Two corollaries.

Corollary 1. *Under the hypotheses of the Theorem, suppose that, in addition,*

(3.1) $$x = E(C)x \quad \text{for some} \quad x\in H, \quad x\neq 0.$$

Then

(3.2) $$E_z \text{ on } C \text{ is equivalent to arc length measure on } C,$$

that is, $E(\beta)=0$ *for a Borel set* β *of* C *if and only if* β *has arc length measure zero.*

Proof. In view of the remarks at the end of section 1, it is sufficient to show that β has arc length measure zero whenever $E(\beta)=0$. It follows from (3.1) and (1.4) that $E(|z|<1)\; x=0$, so that $\|E_z x\|^2=\|G_z x\|^2$, z on C. However, as noted above, $\|G_z x\|^2$ is equivalent to arc length measure on C and the proof is complete.

For use below, let $\alpha_t=\{e^{is}: 0\leqq s\leqq t\}$, $0\leqq t\leqq 2\pi$, and put $E_t=E(\alpha_t)$ and $G_t=G(\alpha_t)$. If $\Delta=[a, b]\subset[0, 2\pi]$, let $\Delta E=E_b-E_a$ and $\Delta G=G_b-G_a$.

Corollary 2. *Suppose that for some* $x\in H$, $x\neq 0$,

(3.3) $$\inf_\Delta \{\|\Delta G x\|^2/|\Delta|\} = 0,$$

where Δ *is any subinterval of* $[0, 2\pi]$ *and* $|\Delta|>0$ *is its length. Then* (3.1), *hence also* (3.2), *holds.*

Proof. By (1.4) and (1.5),

$$\|\Delta Ex\|^2/|\Delta| + (1/2\pi) \int_D (1/|\Delta|) \Big(\int_\Delta \mathrm{Re}\,(P_z(t))\, dt \Big)\, d\|E_z x\|^2 = \|\Delta Gx\|^2/|\Delta|. \tag{3.4}$$

By (3.3), there exists a sequence of intervals Δ_n, $|\Delta_n|>0$, $n=1, 2, \ldots$, where $\Delta_n = [a_n, b_n]$ and $a_n, b_n \to c$ for some c in $[0, 2\pi]$. It follows from (3.4) and Fatou's lemma that

$$\int_D \mathrm{Re}\,(P_z(c))\, d\|E_z x\|^2 = 0.$$

Consequently, $E(D)x=0$, that is, (3.1), and hence (3.2).

4. Remarks. It follows from Corollary 2 that if E_z on C is not equivalent to arc length measure on C (so that there exists a Borel set β on C of positive arc length measure for which $E(\beta)=0$), then, for every x in H, $x\neq 0$, there exists a constant k_x for which $\|\Delta Gx\|^2/|\Delta| \geqq k_x > 0$ for all subintervals Δ of $[0, 2\pi]$. This result can be regarded as a refinement of the relation

$$\log (d\|G_t x\|^2/dt) \in L(0, 2\pi), \tag{4.1}$$

which is valid whether or not E_z on C is equivalent to arc length measure on C. In fact, (4.1) holds for arbitrary completely nonunitary (not necessarily subnormal) contractions T; see Sz.-Nagy and Foiaş [8], p. 84.

Since for each $x \in H$, both $\|E_t x\|^2$ and $\|G_t x\|^2$ are absolutely continuous on $[0, 2\pi]$, it is seen from (3.4) with $\Delta = [t, t+\Delta t]$ that

$$d\|E_t x\|^2/dt + (1/2\pi) \int_D \mathrm{Re}\,(P_z(t))\, d\|E_z x\|^2 = d\|G_t x\|^2/dt \tag{4.2}$$

holds a.e. on $0 \leqq t \leqq 2\pi$. In fact, the relation corresponding to (4.2) but with the equality replaced by "$\leqq$" follows from Fatou's lemma. That, in fact, equality holds (a.e.) follows from an integration and the fact that $x = E(D^-)x = G(C)x$.

We are indebted to K. F. Clancey and to J. B. Conway for very helpful discussions, especially in connection with the "sweep" interpretation of (1.4) as given in section 2.

References

[1] J. B. Conway, Subnormal operators, Research Notes in Mathematics, 51 Pitman Advanced Publishing Program, 1981.

[2] J. B. Conway and R. F. Olin, A functional calculus for subnormal operators. II, *Mem. Amer. Math. Soc.*, **10**, No. 184 (1977).

[3] P. R. Halmos, *A Hilbert space problem book*, Second edition, Graduate Texts in Mathematics, vol. 19, Springer-Verlag (Berlin—Heidelberg—New York, 1982).
[4] R. F. Olin, *Functional relationships between a subnormal operator and its minimal normal extension*, Thesis, Indiana Univ., 1975.
[5] C. R. Putnam, Peak sets and subnormal operators, *Illinois J. Math.*, **21** (1977), 388—394.
[6] C. R. Putnam, Absolute continuity and hyponormal operators, *Internat. J. Math. and Math. Sci.*, **4** (1981), 321—335.
[7] B. Sz.-Nagy, Sur les contractions de l'espace de Hilbert, *Acta Sci. Math.*, **15** (1953), 87—92.
[8] B. Sz.-Nagy and C. Foiaş, *Harmonic analysis of operators on Hilbert space*, North-Holland Publishing Co., American Elsevier Pub. Co., Akadémiai Kiadó (1970).

DEPARTMENT OF MATHEMATICS
PURDUE UNIVERSITY
WEST LAFAYETTE, IN 47907, U.S.A.

Acta Sci. Math., 50 (1986), 427—432

C^*-norms defined by positive linear forms

JÁNOS KRISTÓF

It is well known that the norm of a C^*-algebra A is uniquely defined by a set of its positive linear forms, namely

$$\|x\| = \sup_{f \in S} \sqrt{f(x^*x)} \tag{1}$$

for all $x \in A$, where S is the set of positive linear forms f on A such that $\|f\| \leqq 1$ (cf. [1]). It is worth mentioning that the set S in (1) can be defined by an entirely algebraic way; the linear form f on A is in S if and only if $f(x^*x) \in \mathbf{R}_+$ and $|f(x)|^2 \leqq f(x^*x)$ for all $x \in A$. This means that in the right side of (1) only such entities enter which are related to the algebraic structure of A.

The latter observation leads to the result that defining a C^*-norm on a $*$-algebra is equivalent to indicating a certain set of positive linear forms on it. So the question arises naturally; how to choose a set S of positive linear forms on a given $*$-algebra so as to obtain a C^*-norm on it by the definition (1)?

The aim of this paper is to examine this problem. Due to the elementary character of our further investigations we shall constantly refer to the basic works [1] and [2].

I. C^*-seminorms defined by positive linear forms

In the present study the vector space of the linear forms on the $*$-algebra A is denoted by A^* and $\widetilde{\mathrm{co}}\,(P)$ stands for the $\sigma(A^*, A)$-closed convex hull of the subset P of A^*.

If A is a $*$-algebra with unity and P is a set of positive linear forms on A then the set $\{f \in P \mid f(\mathbf{1}) \leqq 1\}$ is denoted by $P(1)$, where $\mathbf{1}$ is the unit element of A. Further, assuming that $P(1)$ is $\sigma(A^*, A)$-bounded, $\|\cdot\|_P$ denotes the mapping from A into $\mathbf{R}_+$

Received August 23, 1984.

defined by the equation

$$\|x\|_P := \sup_{f \in P(1)} \sqrt{f(x^*x)} \tag{1$'$}$$

for all $x \in A$. It is obvious that $\|\cdot\|_P$ is a seminorm on A. The dual seminorm of $\|\cdot\|_P$ is denoted by $\|\cdot\|'_P$.

Given a $*$-algebra A and a linear form f on it, for all $x \in A$ we define the linear forms $x.f$ and $f.x$ on A as the mappings $y \mapsto f(xy)$ and $y \mapsto f(yx)$, respectively. Clearly, $x.(f.y) = (x.f).y$ thus one may use the simple notation $x.f.y$ instead of $x.(f.y)$ or $(x.f).y$.

Our first result concerns a sufficient condition on a set of positive linear forms providing C^*-seminorms by the aid of (1)$'$.

Theorem 1. *Let A be a $*$-algebra with unity and P a nonvoid set of positive linear forms on A satisfying*

(I) *$P(1)$ is $\sigma(A^*, A)$-bounded.*

(II) *$\mathbf{R}_+ P \subset P$ and $x^*.P.x \subset \overline{\mathrm{co}}(P)$ for all $x \in A$.*

Then $\|\cdot\|_P$ is a C^*-seminorm on A and every $f \in \overline{\mathrm{co}}(P)$ is $\|\cdot\|_P$-continuous and $\|f\|'_P = f(1)$. Moreover, if P separates the points of A then $\|\cdot\|_P$ is a norm on A and the involution of A is proper.

Proof. Since $\overline{\mathrm{co}}(P)$ is nonvoid and $\sigma(A^*, A)$-bounded, we may form the seminorm $\|\cdot\|_{\overline{\mathrm{co}}(P)}$ besides $\|\cdot\|_P$. We claim that these seminorms are equal. Of course, $\|\cdot\|_P \leqq \|\cdot\|_{\overline{\mathrm{co}}(P)}$. In order to prove the reverse inequality it suffices to show that $f(x^*x) \leqq \|x\|_P^2$ for all $x \in A$ and $f \in (\overline{\mathrm{co}}(P))(1)$, $f \neq 0$. If $f \in (\overline{\mathrm{co}}(P))(1)$ then there is generalized sequence $(f_i)_{i \in I}$ in $\mathrm{co}(P)$ such that $f_i \to f$ pointwise on A. In particular, $f_i(1) \to f(1)$ and $f(1) > 0$, thus we may suppose that $f_i(1) > 0$ for all $i \in I$. Then take $f'_i := (f(1)/f_i(1)) f_i$ $(i \in I)$. Clearly, $f'_i \in (\mathrm{co}(P))(1)$ with regard to the first part of (II) and it is easy to see that $\mathrm{co}(P(1)) = (\mathrm{co}(P))(1)$. On the other hand, $f'_i \to f$ pointwise on A. From this we infer that given an element x of A we have $f'_i(x^*x) \to f(x^*x)$ and $f'_i(x^*x) \leqq \|x\|_P^2$, since $f'_i \in \mathrm{co}(P(1))$, thus $f(x^*x) \leqq \|x\|_P^2$. Now fix an element f in $(\overline{\mathrm{co}}(P))(1)$. Then

$$|f(x)|^2 \leqq f(1) f(x^*x) \leqq \|x\|^2_{\overline{\mathrm{co}}(P)} = \|x\|_P^2$$

for all $x \in A$, i.e. f is $\|\cdot\|_P$-continuous and $\|f\|'_P \leqq 1$. The first part of (II) now yields that $\mathbf{R}_+ \overline{\mathrm{co}}(P) \subset \overline{\mathrm{co}}(P)$, hence f is $\|\cdot\|_P$-continuous and $\|f\|'_P = f(1)$ for all $f \in \overline{\mathrm{co}}(P)$.

We show next that

$$f(y^*x^*xy) \leqq \|x\|_P^2 f(y^*y) \tag{2}$$

for all $f \in \overline{\mathrm{co}}(P)$ and $x, y \in A$. If $f(y^*y) = 0$ then choose an arbitrary positive real number ε to obtain

$$f(y^*x^*xy)/\varepsilon = ((y/\sqrt{\varepsilon})^*.f.(y/\sqrt{\varepsilon}))(x^*x).$$

Since by (II) the linear form standing on the right hand side belongs to $(\overline{\text{co}}\,(P))(1)$, we now have $f(y^*x^*xy) \leqq \varepsilon \|x\|_P^2$ for all $\varepsilon > 0$, i.e. the equality $f(y^*x^*xy) = 0 = \|x\|_P^2 f(y^*y)$ holds. If $f(y^*y) > 0$, then

$$f(y^*x^*xy)/f(y^*y) = \big((y/\sqrt{f(y^*y)})^* . f . (y/\sqrt{f(y^*y)})\big)(x^*x)$$

and the linear form on the right hand side belongs to $(\overline{\text{co}}\,(P))(1)$, hence we obtain the desired inequality.

From the inequality (2) it follows that $\|xy\|_P \leqq \|x\|_P \|y\|_P$ for all $x, y \in A$. The only thing that remained to be proved is the inequality $\|x\|_P^2 \leqq \|x^*x\|_P$ for all $x \in A$. If $x \in A$ and $f \in P(1)$ then $f(x^*x) \leqq \|f\|_P' \|x^*x\|_P = f(1)\|x^*x\|_P \leqq \|x^*x\|_P$ thus $\|\cdot\|_P$ is a C^*-seminorm on A. The last assertion of the theorem is an immediate consequence of our previous considerations.

II. C^*-norms defined by positive linear forms

The assumptions (I) and (II) introduced in Theorem 1 are not sufficient for P to ensure that $\|\cdot\|_P$ be a C^*-norm on A. Our next aim is to impose further conditions on P in order to have possibility of proving the completeness of A with respect to the uniform structure defined by $\|\cdot\|_P$.

We need two auxiliary lemmas. Before formulate them we agree that given a $*$-algebra A with unity and a nonvoid set P of positive linear forms on A satisfying (I), the linear subspace and the $\|\cdot\|_P'$-closed linear subspace of A^* spanned by P will be denoted by $\text{sp}\,(P)$ and $\overline{\text{sp}}\,(P)$, respectively.

Lemma 1. *Let A be a $*$-algebra with unity and P a separating set of positive linear forms on A satisfying* (I). *Then the $\sigma(A, \overline{\text{sp}}\,(P))$ and $\sigma(A, \text{sp}\,(P))$ topologies coincide in each $\|\cdot\|_P$-bounded subset of A.*

Proof. Let $(x_i)_{i\in I}$ be a generalized sequence in A such that $x_i \to x$ in the $\sigma(A, \text{sp}\,(P))$-topology and suppose that we have $M := \sup_{i\in I} \|x_i\|_P < +\infty$. We claim that $x_i \to x$ in the $\sigma(A, \overline{\text{sp}}\,(P))$-topology. If $\bar{f} \in \overline{\text{sp}}\,(P)$, $f \in \text{sp}\,(P)$ and $i \in I$ then

$$|\bar{f}(x_i) - \bar{f}(x)| \leqq |\bar{f}(x_i) - f(x_i)| + |f(x_i) - f(x)| + |f(x) - \bar{f}(x)| \leqq$$
$$\leqq \|\bar{f} - f\|_P'(M + \|x\|_P) + |f(x_i) - f(x)|.$$

Since $\bar{f} \in \overline{\text{sp}}\,(P)$ and $f(x_i) \to f(x)$ for all $f \in \text{sp}\,(P)$, we easily deduce that $\bar{f}(x_i) \to \bar{f}(x)$.

It is obvious that $\sigma(A, \overline{\text{sp}}\,(P))$ is a stronger topology on A than $\sigma(A, \text{sp}\,(P))$, however, Lemma 1 indicates a certain strict intrinsic relation between them.

Lemma 2. *Let A and P be as in Lemma 1 and suppose*

(III) $x.P \subset \overline{\mathrm{sp}}\,(P)$ *for all* $x \in A$.

Then the multiplication in the algebra A is $\|\cdot\|_P$-boundedly left and right continuous in the $\sigma(A, \mathrm{sp}\,(P))$-topology.

Proof. Consider a $\|\cdot\|_P$-bounded generalized sequence $(x_i)_{i\in I}$ in A such that $x_i \to x$ in the $\sigma(A, \mathrm{sp}\,(P))$-topology. Then combine Lemma 1 and (III) to obtain that

$$f(yx_i) = (y.f)(x_i) \to (y.f)(x) = f(yx)$$

for all $f \in P$ and $y \in A$, i.e. $yx_i \to yx$ in the $\sigma(A, \mathrm{sp}\,(P))$-topology.

Due to the obvious equality $f.y = (y^*.f)^*$ and the trivial fact that the set $\overline{\mathrm{sp}}\,(P)$ is closed with respect to the natural adjunction of A^*, we deduce that $x_i y \to xy$ in the same topology.

We are now ready to formulate our main result on C^*-norms defined by positive linear forms.

Theorem 2. *Let A be a $*$-algebra with unity and P a separating set of positive linear forms on A satisfying* (I), (II), (III) *and*

(IV) *A is sequentally complete with respect to the uniform structure defined by the $\sigma(A, \mathrm{sp}\,(P))$-topology.*

Then A is a C^*-algebra whose (unique) C^*-norm equals $\|\cdot\|_P$.

Proof. With regard to Theorem 1, A, equipped with $\|\cdot\|_P$ is a pre-C^*-algebra. Let $\hat{A}$ denote the envelopping C^*-algebra of this pre-C^*-algebra. For every $\|\cdot\|_P$-continuous linear form f on A let $\hat{f}$ denote its unique norm continuous extension to $\hat{A}$. We shall prove that $A = \hat{A}$.

First we show that there exists a unique mapping π from $\hat{A}$ onto A with the property $f \circ \pi = \hat{f}$ for all $f \in P$. The uniqueness of π is an immediate consequence of the assumption that P separates the points of A. To prove the existence of π let us consider a fixed element $\hat{x}$ of $\hat{A}$. There is a sequence $(x_n)_{n\in\mathbf{N}}$ in A such that $\|x_n - \hat{x}\|_P \to 0$, where the C^*-norm of $\hat{A}$ is also denoted by $\|\cdot\|_P$. Then $(x_n)_{n\in\mathbf{N}}$ is a $\|\cdot\|_P$-Cauchy sequence in A, hence a Cauchy sequence in the weaker uniform structure defined by the $\sigma(A, \mathrm{sp}\,(P))$-topology. Now, condition (IV) implies the existence of an element x in A with the property that $x_n \to x$ in the $\sigma(A, \mathrm{sp}\,(P))$-topology. We define $\pi(\hat{x})$ to be equal to x. Then, for all $f \in P$, by virtue of Theorem 1 we have

$$f(\pi(\hat{x})) = f(x) = \lim_n f(x_n) = \lim_n \hat{f}(x_n) = \hat{f}(\hat{x}),$$

thus the existence of π is verified.

We claim that $f \circ \pi = \hat{f}$ holds for all $f \in \overline{\mathrm{sp}}\,(P)$. Indeed, if $f \in \overline{\mathrm{sp}}\,P$ and $(f_n)_{n\in\mathbf{N}}$ is a sequence in $\mathrm{sp}\,(P)$ such that $\|f_n - f\|'_P \to 0$ then we also have $\|\hat{f}_n - \hat{f}\|'_P \to 0$, where $\|\cdot\|'_P$ denotes the dual norm of the C^*-norm of $\hat{A}$. Thus $\hat{f}_n \to \hat{f}$ pointwise on A, hence

$$f(\pi(\hat{x})) = \lim_n f_n(\pi(\hat{x})) = \lim_n \hat{f}_n(\hat{x}) = \hat{f}(\hat{x})$$

for all $\hat{x} \in \hat{A}$, thus providing the desired equality.

Obviously, π is linear and it is continuous in the topology defined by the C^*-norm on $\hat{A}$ and $\sigma(A, \overline{\mathrm{sp}}(P))$ on A, respectively. It is easy to see that π preserves the involution of $\hat{A}$ and A, respectively. On the other hand, $\pi \circ \pi = \pi$, since $f(x) = \hat{f}(x) = f(\pi(x))$ for all $f \in P$ and $x \in A$, i.e. we have $x = \pi(x)$ $(x \in A)$.

We show that the map π is multiplicative, thus π, in fact, is a $*$-algebra morphism between $\hat{A}$ and A. Let $x \in A$ and $\hat{y} \in \hat{A}$. Applying (III) we infer $x.f \in \overline{\mathrm{sp}}(P)$ for every $f \in P$, hence

$$f(\pi(x\hat{y})) = \hat{f}(x\hat{y}) = (x.\hat{f})(\hat{y}) = (\widehat{x.f})(\hat{y}) = (x.f)(\pi(\hat{y})) = f(x\pi(\hat{y}))$$

i.e. $\pi(x\hat{y}) = x\pi(\hat{y})$. Next, let $\hat{x} \in \hat{A}$ and $\hat{y} \in \hat{A}$. Then there is a sequence $(x_n)_{n \in \mathbf{N}}$ in A such that $\|x_n - \hat{x}\|_P \to 0$. The above established continuity property of π now yields $x_n = \pi(x_n) \to \pi(\hat{x})$ in the $\sigma(A, \mathrm{sp}(P))$-topology (moreover, in $\sigma(A, \overline{\mathrm{sp}}(P))$). Since $\pi(x_n\hat{y}) = x_n\pi(\hat{y})$ $(n \in \mathbf{N})$ and the sequence $(x_n)_{n \in \mathbf{N}}$ is $\|\cdot\|_P$-bounded in A, Lemma 2 implies that $\pi(x_n\hat{y}) \to \pi(\hat{x})\pi(\hat{y})$ in the $\sigma(A, \mathrm{sp}(P))$-topology. Furthermore, we obviously have $x_n\hat{y} \to \hat{x}\hat{y}$ in the C^*-algebra $\hat{A}$, thus applying the continuity of π again we obtain $\pi(x_n\hat{y}) \to \pi(\hat{x}\hat{y})$ in the $\sigma(A, \mathrm{sp}(P))$-topology, i.e. $\pi(\hat{x})\pi(\hat{y}) = \pi(\hat{x}\hat{y})$.

To finish the proof we refer to the well known fact that a $*$-algebra morphism from a C^*-algebra into a pre-C^*-algebra is necessarily norm continuous (cf. [1] or [2]). Thus π is norm continuous and $A = \mathrm{Ker}(\mathrm{id}_{\hat{A}} - \pi)$ is dense and closed in the C^*-algebra $\hat{A}$, i.e. $A = \hat{A}$.

III. Examples for C^*-norms defined by positive linear forms

This last section contains two important examples for C^*-norms defined by positive linear forms. Then it becomes clear that it is not difficult to construct in certain $*$-algebras with unity such sets of positive linear forms which satisfy the conditions (I)–(IV) formulated in sections I and II.

Example 1. Let A be a von Neumann algebra in the Hilbert space H and for all $z \in H$ let f_z denote the positive linear form on A defined by the formula $f_z(T) := (Tz|z)$ for all $T \in A$. Then the set $P := \{f_z | z \in H\}$ satisfies the axioms (I)–(IV).

The proof of this assertion is provided by the standard application of the Banach—Steinhaus theorem; we omit the details. In this case $\sigma(A, \mathrm{sp}(P))$ and $\sigma(A, \overline{\mathrm{sp}}(P))$ are the weak and ultraweak operator topologies on A, respectively. Of course, the norm $\|\cdot\|_P$ coincides with the usual operator norm on A.

Example 2. Let $\mathscr{A}$ denote a σ-algebra of subsets in the set T and A be the $*$-algebra of complex valued, bounded, $\mathscr{A}-\mathscr{B}(\mathbf{C})$ measurable functions (where $\mathscr{B}(\mathbf{C})$ denotes the Borel σ-algebra of $\mathbf{C}$). Let us define P as the set of integrals on A arising from σ-additive finite positive measures defined on $\mathscr{A}$. Then P satisfies the axioms (I)—(IV).

In this case $\mathrm{sp}(P)=\overline{\mathrm{sp}}(P)$ and a sequence $(\varphi_n)_{n\in\mathbf{N}}$ in A converges to the function $\varphi\in A$ in the $\sigma(A, \mathrm{sp}(P))$-topology if and only if $\varphi_n\to\varphi$ pointwise on T and the sequence is uniformly bounded. This proposition can be verified by the standard use of the theorem of Lebesgue and that of Banach—Steinhaus. Of course, the norm $\|\cdot\|_P$ coincides with the sup-norm.

These examples make clear that the class of C^*-algebras with unity whose norms are defined by positive linear forms satisfying the axioms (I)—(IV) contains strictly the class of von Neumann algebras. It is easy to show that there are C^*-algebras with unity (even commutative ones) that do not belong to this class. However, these C^*-algebras have certain properties very close to those of von Neumann algebras. As a matter of fact, further investigations on these C^*-algebras yield an interesting version of the spectral theorem for normal elements, analogous to the spectral theorem for normal operators in Hilbert spaces.

References

[1] J. Dixmier, *Les C*-algébres et Leurs Représentations*, Gauthier Villars Éditeurs (1968).
[2] N. Bourbaki, *Théories spectrales*, Hermann (Paris, 1967).

DEPARTMENT OF ANALYSIS
EÖTVÖS LORÁND UNIVERSITY
MÚZEUM KRT. 6—8
1088 BUDAPEST, HUNGARY

Bibliographie

M. Barr—C. Wells, Toposes, Triples and Theories (Grundlehren der mathematischen Wissenschaften, Band 278), XIII+345 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985.

This book provides an introduction to the three concepts of topos, triple and theory, and describes the connections between them. Among the three topics, topos theory is central in the book. That reflects the current state of development and the importance of topos theory as compared to the other two.

A topos is a special kind of a category defined by axioms saying roughly that certain constructions one can make with sets can be done in the category. However, the notion of topos originated as an abstraction of the properties of the category of sheaves of sets on a topological space. Later, mathematicians developed the idea that a theory in the sense of mathematical logic can be regarded as a topos. In this book a topos is regarded as being defined by its elementary axioms, saying nothing about set theory in which its models live. One reason for this attitude is that many people regard topos theory as a possible new foundation for mathematics.

Chapter 1 is an introduction to category theory which develops the basic constructions in categories needed for the rest of the book. A reader familiar with the elements of category theory including adjoint functors can skip nearly all of these. Chapters 2, 3 and 4 introduce the three topics of the title, respectively, and develop them independently up to a certain point. Each of them can be read without the other two chapters. Chapter 5 develops the theory of toposes further, making use of the theory of triples. Chapter 6 covers various fundamental constructions which give toposes, with emphasis on the original idea that toposes are abstract sheaf categories. Chapter 7 provides the basic representation theorems for toposes. Theories are then carried further in Chapter 8, making use the representation theorems. Chapter 9 develops further topics in triple theory, and may be read independently after Chapter 3.

The book provides a fairly thorough introduction to topos theory covering topologies and representation theorems but omitting the connection with algebraic geometry and logic. Each chapter ends with a list of exercies. The exercises provide examples or develop the theory further.

The book can be read by graduate students with a familiarity with elementary algebra.

Gy. Horváth (Szeged)

Kenneth L. Bowles—Stephen D. Franklin—Dennis J. Volper, Problem Solving Using UCSD Pascal. Second Edition with 106 illustrations, XI+340 pages, Springer-Verlag, New York—Berlin—Heidelberg—Tokyo, 1984.

This book is designed both for an introductory course in computer problem solving and for individual self study. This is a revised and extended edition of one of the most successful introductions to Pascal, "Microcomputer Problem Solving Using Pascal", Springer-Verlag, 1977.

In practice, it seems best to learn programming first using Pascal, and then to shift over to one of the other languages. Pascal is clearly the best language now in widespread use for teaching the concepts of structured programming at the introductory level. Structured programming is a method designed to minimize the effort that the programmer has to spend on finding and correcting logical errors in programs. Put more positively, it is a method designed to allow a program to produce correct results with a minimum amount of effort on the part of the programmer. The key to structuring in Pascal is the procedure. Therefore, this book introduces and emphasizes procedures from the very start. Procedures for graphics are introduced in the first chapter and the first programming assignment requires the student to use them. By the second chapter, students are writing and using their own procedures. The early and continuing emphasis on procedures is the major organizational difference between this book and most others which, in contrast, often do not introduce procedures until a third or even half way through their coverage of Pascal.

The subject matter has been chosen to be understandable to all students at about the college freshman level, with almost no dependence on a background in high school mathematics beyond simple algebra. At an introductory level, the basic methods of programming and problem solving differ very little between applications in engineering and science and applications in business, arts or humanities. It is possible to motivate and teach students across this entire spectrum using problem examples with a non-numerical orientation: the manipulation of text strings and graphics.

Chapter 1 of the book introduces the students to the use of the UCSD software system for Pascal. Chapter 2 through 7 present basic tools for programming and for expressing algorithms. Chapter 8 through 12 add tools for working with data transmitted to the computer from external devices and for working with complex data. Chapters 13—15 provide illustrations of complex problems of types that are frequently encountered by virtually all programmers. The appendices at the end of the book are included for reference purposes and survey some additional features of the Pascal language. Each chapter starts with a statement of the objectives that the students should attain before proceeding to the next chapter.

If you have a personal computer, the UCSD software system for Pascal, and this book in addition, you can easily learn to write computer programs and will master the bases of computer problem solving. The book is equally suitable as a textbook of a course.

K. Dévényi (Szeged)

Differential Geometric Methods in Mathematical Physics, Proceedings, Clausthal, August 30— September 2, 1983. Edited by H. D. Doebner and J. D. Hennig (Lecture Notes in Mathematics, 1139), VI+337 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1986.

The aim of this series of conferences is to promote the application of geometrical, analytical and algebraic methods and their interplay for the modelling of complex physical systems. This volume contains 20 papers submitted by participants of the conference (the 12th in the series) organized by H. D. Doebner, S. I. Andersson (Clausthal) and G. Denardo (Trieste) at the Institute for Theoretical Physics A, Technical University of Clausthal, F.R.G. The main topics treated in the proceedings are described by the following key words which are also the titles of the chapters: Momentum Mappings and Invariants — Aspects of Quantizations — Structure of Gauge Theories — Non-Linear Systems, Integrability and Foliations — Geometrical Modelling of Special Systems.

The volume is dedicated to the memory of the outstanding mathematician and mathematical physicist Steven M. Paneitz, who died in a tragic accident while attending this conference at the age of 28.

Péter T. Nagy (Szeged)

Dynamical Systems and Bifurcations (Proceedings, Groningen 1984). Edited by B. L. J. Braaksma, H. W. Broer and F. Takens (Lecture Notes in Mathematics, 1125), 129 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985.

Readers paying attention regularly to the review section of these *Acta* have certainly realized that nowadays more and more monographs, texts and conferences are devoted to the modern theory of differential equations and especially to bifurcation theory. This is of course due to the interest in the topic, both in pure and applied mathematics. The present volume is the proceedings of the International Workshop on Dynamical Systems and Bifurcations, organized by the Department of Mathematics of Groningen University, April 16—20, 1984.

Almost all of the articles are concerned with the geometric theory of dynamical systems (papers by M. Chaperon, R. Dumortier, A. Floer and E. Zehdner, J. Palis and R. Roussavie, F. Takens, G. Vegter). One paper (written by R. Dieckerhoff and E. Zehdner) deals with the boundedness of the solutions of a second order timedependent nonlinear differential equation, and another one (by J. A. Sanders and R. Cushman) is devoted to global Hopf bifurcations.

L. Hatvani (Szeged)

E. Grosswald, Representations of Integers as Sums of Squares, XI+251 pages, Springer-Verlag, New York—Berlin—Heidelberg—Tokyo, 1985.

There are a number of branches of mathematics which seem to have no use in practical applications and in which the problems are merely investigated for their own beauty. The first of these is clearly the theory of numbers, called "The Queen of Mathematics" by Gauss. Everybody knows something about integers. Here many questions or problems can be formulated within the capacity of the man of the street. These questions are sometimes so interesting as the best puzzles having surprising results.

One of the oldest problems is the finding of Pythagorean triangles, right triangles whose sides are integers. The next question is which of the integers can be represented as a sum of two or more squares? Is it true that every integer can be written as a sum of four squares? These are curious questions in themselves and surprisingly they do have applications, for example in lattice point problems, in crystallography and in certain problems of mechanics. In the last few decades it was in fact practice that has raised several questions which can be answered by the aid of number-theoretic results.

This book contains the enlarged versions of lectures given by the author in 1980—1981 for an audience consisting of particularly gifted listeners with widely varying background. Therefore the theme of this work, starting at the most elementary level but pushing ahead as far as possible in some directions, seems to be ideal. Besides the elementary — but by no means simple — methods there appear various other notions from other branches of mathematics too, e.g. quadratic residues, elliptic and theta functions, complex integration and residues, algebraic number theory etc.

The list of mathematicians who have obtained results in the study of the problems in this book includes so illustrious names as Diophantus, Fermat, Lagrange, Gauss, Artin, Hardy, Littlewood, Ramanujan, Siegel and Pfister for instance.

The author made a serious effort to make the book accessible to a wide circle of readers. He follows roughly the historical development of the subject matter. Therefore, in the early chapters, the prerequisities are minimal. More advanced tools are necessary in the later chapters.

A number of interested problems is proposed at the end of many chapters, ranging from fairly routine to difficult ones. Also, open questions are mentioned.

Finally we cite the last sentence of the author's "Introduction": "The success of this book will be measured, up to a point, by the number of readers who enjoy it, but perhaps more by the number who are sufficiently stimulated by it to become actively engaged in the solution of the numerous problems that are still open."

L. Pintér (Szeged)

Erich Hecke, Lectures on the Theory of Algebraic Numbers (Graduate Texts in Mathematics, Vol. 77), Springer-Verlag, New York—Heidelberg—Berlin, 1981.

This is a translation of Erich Hecke's classic book, originally published in German in 1923. It is a welcome event that, after sixty years of its first edition, this excellent book became available to the English-reading public.

The first three chapters are of preparatory character: Chapter I contains the elements of the theory of rational integers, Chapter II summarizes the basic facts on Abelian groups that are needed later on, and Chapter III deals with the structure of the group $\mathfrak{R}(n)$ of the residue classes mod n, relatively prime to n. The theory of algebraic numbers starts in Chapter IV with a short introduction into the algebra of number fields (Galois theory is not discussed). Ideal theory, the core of algebraic number theory, is developed in Chapter V. Next, in Chapter VI, analytic methods are applied to the problem of the class number and to the problem of the distribution of prime ideals. Quadratic number fields are treated in detail in Chapter VII; in particular, the Quadratic Reciprocity Law is derived, and the class number of $k(\sqrt{d})$ is determined with, as well as without, the use of the zeta-function. Finally, Chapter VIII is devoted to the proof of the Quadratic Reciprocity Law in arbitrary algebraic number fields.

After that a book, like this one, had been in continuous use for sixty years, there is no doubt it will serve new generations of students and mathematicians who want to get acquainted with algebraic number theory. There are, however, two things which the present-day reader will miss: a subject index, and a short survey of what has happened in the field since 1923.

Unfortunately, in certain places the translation is not quite correct.

Ágnes Szendrei (Szeged)

Dan Henry, Geometric Theory of Semilinear Parabolic Equations (Lecture Notes in Mathematics, 840), IV+348 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1981.

Nowadays the geometric theory of differential equations is an intensively developing branch of mathematics. The present book also deals with such general questions as existence, uniqueness, continuous dependence of solutions on the right-hand side, the semigroup properties of solutions, stability questions for nonlinear semigroups, Lyapunov functions, invariance principle, existence of equilibria and periodic solutions and the behaviour of solutions in their neighbourhood, questions of bifurcation, the application of the adjoint system, invariant manifolds and the behaviour of solutions in their small neighbourhoods, exponential dichotomies, orbital stability, perturbations of right-hand side, etc. The feature of the book is that the main results are formulated for general differential equations written in Banach spaces. The conditions of the theorems can be met by semilinear parabolic differential equations. Typically, the linear part of the right-hand side of the equation is a sectorial operator.

The questions studied are well-prepared by examples. The results are illustrated by interesting applications concerning nonlinear parabolic equations that arose in physical, biological and engineering problems. One of the chapters gathers the examples that accure in the book. The titles of the sections of this chapter show a wide range of the applications: Nonlinear heat equation, Flow of electrons and holes in a semiconductor, Hodgekin—Huxley equations for nerve axon, Chemical reactions in a catalyst pellet, Population genetics, Nuclear reactor dynamics, Navier—Stokes and related equations.

There are sections concerned with special problems of semilinear parabolic equations, e.g. the existence of travelling waves. Some exercises make this book interesting. They can be well comprehended after the study of the material, but the author also gives hints in more difficult cases.

This book is of interest to experts of the geometric and qualitative theories of differential equations. I feel it essential for researchers of parabolic partial differential equations. It gives a well-structured theoretical background and shows the directions of interesting applications.

J. Terjéki (Szeged)

E. Horowitz, Fundamentals of Programming Languages, Second Edition, XV+446 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1984.

Traditional books on programming languages are like abbreviated language manuals. This book takes a fundamentally different point of view by focusing on a few essential concepts. These concepts include such topics as variables, expressions, statements, typing, procedures, data abstractions, exception handling and concurrency. By understanding what these concepts are and how they are realized in different programming languages, the reader arrives at a level of comprehension far higher than what can be achieved by writing programs in various languages. Moreover, the study of these concepts provides a better understanding of future language designs.

Chapter 1 is devoted to the study of the evolution of programming languages. Twelve criteria by which a programming language design can be judged are presented in Chapter 2. Subsequent chapters develop the concepts mentioned above. Much work has been done on imperative programming languages. The last three chapters cover non-imperative features such as functional programming, data flow programming and object oriented programming. A large number of exercises enriches the text.

This book is warmly recommended as a good text for a graduate course whose objective is to survey the fundamental features of current programming languages.

Gy. Horváth (Szeged)

O. A. Ladyzhenskaya, The Boundary Value Problems of Mathematical Physics (Applied Mathematical Sciences, 49), XXX+322 pages, Springer-Verlag, New York—Berlin—Heidelberg—Tokyo, 1985.

If an instantaneous state of a physical system is described by a function (e.g. string, membrane, temperature of a body, fluid stream) then the mathematical model of the system is often a second order partial differential equation. The purpose of mathematical physics is to study these equations using pure mathematical methods. The basic problems are the following: Under which conditions on the domain and on the functions involved in the equation does the equation have a solution with prescribed values on the boundary? Is the solution unique? How can the solutions be approximated by solutions of simpler problems?

The book is concerned with these problems for linear equations. The investigations for the existence and uniqueness of the solutions of boundary value problems are governed by a very natural principle. If a boundary value problem admits more solutions then it cannot be a good model of a uniquely determined physical process. So the first step is to find conditions for the uniqueness of the solutions. By experience, in case of linear problems the existence of the solutions is a consequence of their uniqueness (e.g. for systems of n linear algebraic equations in n unknowns). The author tries to establish this principle also for boundary value problems introducing various classes of generalized solutions.

There are other features of the book. The author considers elliptic, parabolic and hyperbolic equations alike. She studies also the smoothness of the generalized solutions and the connection between the generalized and classic solutions. To illuminate this, let us have a look at Chapter 2 devoted to the elliptic equation. First the solvability of the boundary value problems is established in the space $W_2^1(\Omega)$ consisting of all the elements in $L_2(\Omega)$ that have generalized first derivatives in $L_2(\Omega)$. The problems are reduced to equations with completely continuous operators and their Fredholm solvability is proved. Examples show that these solutions may not have second order derivatives (not even generalized derivatives either), and they salitisfy the conditions of the problem in some generalized sense. It is proved that under a minor improvement of the functions in the equation and a certain increase in the smoothness of the boundary, all generalized solutions in $W_2^1(\Omega)$ belong to $W_2^2(\Omega)$ and satisfy the equation in the ordinary sense for almost all $x\in\Omega$.

The lengthy final chapter is devoted to the Method of Finite Differences. Introducing grids in the basic domain, the method reduces various problems for differential equations to systems of algebraic equations in which unknowns are the values of grid functions at the vertices of the grids. The limit process obtained when the lengths of the sides of the cells in the grid tend to zero is also examined here. The author is one of the pioneers of proving convergence in $L_2(\Omega)$-norm in case of initial-boundary value problems for hyperbolic equations.

The original Russian edition is supplied in the present translation by "Supplements and Problems" located at the end of each chapter. They are useful to awaken the reader's creativity by providing topics for independent work.

This excellent monograph is highly recommended to everyone interested in the theory of partial differential equations and its applications.

L. Hatvani (Szeged)

S. Lang, Complex Analysis, VII+367 pages, Springer-Verlag, New York—Berlin—Heidelberg—Tokyo, 1985.

The first edition of this book was published in 1977. The author has rewritten many sections, added some new material and made a number of corrections.

The book consists of two parts. Part I (Basic Theory) is intended as an introduction to complex analysis for use by advanced undergraduates and beginning graduate students. Part II (Various Analytic Topics) contains more advanced topics, the chapters here are titled as follows: Applications of the maximum modulus principle; Entire and meromorphic functions; Elliptic functions; Differentiating under an integral; Analytic continuation; The Riemann mapping theorem.

The author has made the necessary material on preliminaries as short as possible to get quickly to power series expansions and Cauchy's theorem. In every book on complex functions, one of the most interesting questions is the presentation of Cauchy's theorem. Perhaps the author's words about this problem enlighten the basic attitude of the book: "I have no fixed idea about the manner in which Cauchy's theorem is to be treated. In less advanced classes, or if time is lacking, the usual hand waving about simple closed curves and interiors is not entirely inappropriate. Perhaps better would be to state precisely the homological version and omit the formal proof. For those who want a more through understanding, I include the relevant material." He has included both Artin's proof and the more recent proof of Dixon for the theorem.

Several solved examples illustrate the results making easier the understanding and carefully selected exercises are proposed.

The chapters of Part II are logically independent and can be read in any order. Here we mention only one of the most striking applications, generally omitted from standard courses, the problem of transcendence: Given some analytic function f, describe those points z such that $f(z)$ is an algebraic number.

The most attractive feature of the book for the reveiwer is the successful composition of the classical and modern methods and results.

L. Pintér (Szeged)

László Leindler, Strong Approximation by Fourier Series, 210 pages, Akadémiai Kiadó, Budapest, 1985.

Shortly after L. Fejér had proved his summability theorem, Hardy and Littlewood noticed that it was true in a stronger sense. This was the first instance when strong means were considered but, except for a few feeble attempts, no one had analysed the question further until the late 1930's when J. Marcinkiewicz and A. Zygmund verified that (with the usual terminology)

$$(*) \qquad \frac{1}{n+1}\sum_{k=0}^{n}|s_k(f,x)-f(x)|^p \to 0 \quad (p>0)$$

almost everywhere. It had taken another quarter of a century before G. Alexits and D. Králik turned to the analogous approximation problem. What they found was quite surprising: for Lip α $(0<\alpha<1)$ functions the left-hand side of $(*)$ with $p=1$ has order $\{n^{-\alpha}\}$, i.e. the classical estimate of S. N. Bernstein holds true in the strong sense, as well. This result inevitably brought up the question about the mechanism behind these — literally — strong results and a rapid development in this field was predictable. At this crucial stage appeared L. Leindler on the scene and began to systematically study various kinds of strong means. His papers in the period 1965—1980 exerted dominating influence on the course of events and his one is the lion's share in the fact that today we have the *theory* of strong approximation at all. By the end of the 1970's the results of Leindler and several other authors began to take the shape of a more or less complete theory and the time was ripe for a monograph collecting and organizing the various results.

The book under review is an up-to-date summary of results about strong means. It can and certainly will serve as a reference book. Its content can be recommended not only to the experts of the field but to anyone interested in trigonometric approximation. Leindler's work may also be useful for graduate students for it contains many important techniques of mathematical analysis together with intricate counterexamples which have already proven to be useful in various other branches of analysis. The organization of the material is clear, the whole book is well got up. It was a good choice to omit the proof of certain theorems when they would have required repetition of earlier used techniques. At the same time the reader can learn about the latest and most general results — the author paid special attention at least to announce them. The only criticism I make is that with a little more effort and some 20—30 extra pages the parallel theory of strong summability could have been incorporated into the book, giving thereby a complete account of results about strong means. (The seemingly analogous theory of strong summability of general orthogonal series requires distinctly different arguments.)

The book consists of four chapters. Chapter I deals with the order of strong approximation, i.e., with so-called direct theorems. One of the most general estimate of this type was proved in Leindler's very first paper on the subject and for every classical mean the estimate he obtained turned out to be sharp in many function classes. However, an inequality being sharp does not mean that it can be reversed, so the question of what can be said in the opposite direction, i.e. when we inquire about properties of functions provided the order of some kind of strong mean is known, is very interesting. Chapter II is devoted to this problem. Chapter III establishes various imbedding relations of function spaces yielding in many cases the identification of several of these spaces. In the last chapter some miscellaneous results in three new directions are treated.

Finally, it is appropriate to note that in spite of the fact that the theory presented in the book seems to be complete (e.g. without embarrassing gaps), some very exciting questions in connection with strong means have not or barely been touched upon until now (one of them is the saturation problem). It is the reviewer's sincere hope that László Leindler's work will stimulate interest in some of these problems.

V. Totik (Szeged)

Model-Theoretic Logic, Edited by J. Bairwise and S. Feferman (Perspectives in Mathematical Logic), XVIII+893 pages, Springer-Verlag, New York—Berlin—Heidelberg—Tokyo, 1986.

This is the second monograph in the *Perspectives* series where Bairwise acts as an editor, between the two he was the editor of the successful Handbook of Mathematical Logic. He and S. Feferman are among those mathematicians who considerably contributed to the flourishing of abstract model theory in the 1970's. The present monograph is research-oriented, the expositions in it reflect intensive present-day investigations. "The aim ... would be to give an entry into the field for anyone sufficiently equipped in general model theory and set theory, and thereby to bring them closer to the frontiers of research". Accordingly, several open problems are mentioned and a bibliography of over a thousand items can serve as a reference for the experts and to-be-experts in the field. The book is divided into six parts:

1. Introduction, Basic Theory and Examples (written by Bairwise, Ebbinghaus, Flum).
2. Finitary Languages with Additional Quantifiers (Kaufmann, Schmerl, Mundici, Baudisch, Seese, Tuschik, Weese).
3. Infinitary Languages (Nadel, Dickmann, Kolaitis, Eklof).
4. Second-Order Logic (Baldwin, Gurevich).
5. Logics of Topology and Analysis (Keisler, Ziegler, Steinhorn), and
6. Advanced Topics in Abstract Model Theory (Väänänen, Makowsky, Mundici).

V. Totik (Szeged)

Bernt Øksendal, Stochastic Differential Equations. An Introduction with Applications (Universitext), XIII+205 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985.

"Unfortunately most of the literature about stochastic differential equations seems to place so much emphasis on rigor and completeness that it scares the nonexperts away. These notes are an attempt to approach the subject from the nonexpert point of new: Not knowing anything ... about a subject to start with, what would I like to know first of all? My answer would be: 1) In what situations does the subject arise? 2) What are its essential features? 3) What are the applications and the connections to other fields?"

The author, a lucid mind with a fine pedagogical instinct, has written a splendid text that achieves his aims set forward above. He starts out by stating six problems in the introduction in which stochastic differential equations play an essential role in the solution. Then, while developing stochastic calculus, he frequently returns to these problems and variants thereof and to many other problems to show how the theory works and to motivate the next step in the theoretical development. Needless to say, he restricts himself to stochastic integration with respect to Brownian motion. He is not hesitant to give some basic results without proof in order to leave room for "some more basic applications". The chapter headings are the following: Introduction, Some mathematical preliminaries, Itô integrals, Stochastic integrals and the Itô formula, Stochastic differential equations, The filtering problem, Diffusions, Applications to partial differential equations, Application to optimal stopping, Application to stochastic control. There are two appendices on the normal distribution and on conditional expectations, a bibliography of 71 items, a list of notation, and a subject index.

It can be an ideal text for a graduate course, but it is also recommended to analysts (in particular, those working in differential equations and deterministic dynamical systems and control) who wish to learn quickly what stochastic differential equations are all about.

Sándor Csörgő (Szeged)

Ordinary and Partial Differential Equations (Proceedings, Dundee 1984), Edited by B. D. Sleeman and R. J. Jarvis (Lecture Notes in Mathematics, 1151), XIV+357 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985.

These proceedings contain one half of the lectures delivered at the eighth International Conference on Ordinary and Partial Differential Equations which was held at the University of Dundee, Scotland, June 25—29, 1984.

The 36 lectures show a very wide spectrum. However, it is common in the articles that the authors investigate nonlinear differential equations, some of which are in fact concrete models of systems or processeses in the real world. The following main directions can be recognized among the themes. Many articles investigate the asymptotic behaviour (stability, oscillation etc.) of solutions of nonlinear second, third and n-th order ordinary differential equations. Differential equations with delays are treated, too. Special attention is paid to periodic problems both for ordinary and partial differential equations (e.g. the probleme of the existence of a periodic solution of prescribed period for Hamiltonian systems is studied). Stability and bifurcation problems are also considered for equations of several types.

The applications give a very valuable part of the proceedings. The reader can find interesting (mostly biological) models such as a hydrodynamical model of the sea hare's propulsive mechanism, models for a myelinated nerve axon, vector models for infectious diseases and multidimensional reaction-convection diffusion equations.

The collections can be recommended to those wishing to get a snapshot of the theory and applications of non-linear differential equations.

L. Hatvani (Szeged)

Richard S. Pierce, Associative Algebras (Graduate Texts in Mathematics, Vol. 88) Springer-Verlag, New York—Heidelberg—Berlin, 1982.

The study of associative algebras has long been, and still is, an area of active research which draws inspiration from and applies tools of many other branches of mathematics such as group theory, field theory, algebraic number theory, algebraic geometry, homological algebra, and category theory. The purpose of this book is twofold: to treat the classical results on associative algebras more deeply than most student-oriented books do, and at the same time to bring the reader to the frontier of active research by discussing some important new advances. The emphasis is put on algebras that are finite dimensional over a field.

The highlights of the classical part include the characterization of semisimple modules, the Wedderburn(—Artin) Structure Theorem for semisimple algebras, Maschke's Theorem, the Jacobson radical, the Krull—Schmidt Theorem, the structure and classification of projective modules over Artinian algebras (Chapters 1 through 6), the Wedderburn—Malcev Principal Theorem, Jacobson's Density Theorem, the Jacobson—Bourbaki Theorem (Chapters 11—12), and, within a detailed, systematic study of central simple algebras and the Brauer group of a field (Chapters 13 through 20), the Cartan—Brauer—Hua Theorem, Wedderburn's theorem that all division algebras of degree 3 are cyclic, the classification of central simple algebras over algebraic number fields, and Tsen's Theorem. Among the more recent developments of the subject presented in the book are the theory of representations of algebras, including a proof of the first Brauer—Thrall Conjecture and an exposition of the representation theory of quivers (Chapters 7 and 8), and Amitsur's Theorem on the existence of finite dimensional central simple algebras that are not crossed products (Chapter 20). Together with these results the reader is acquainted with the most powerful tools of the theory of associative algebras: tensor product, homological methods, cohomology of algebras, Galois cohomology, valuation theory, and polynomial identities.

Each of the twenty chapters ends with a note containing historical remarks and suggestions for further reading. In addition, every section is followed by a set of exercises; some of them are intended to help understanding the material, others call for working out details of proofs omitted in the text, and there are also exercises presenting important results which otherwise couldn't be included.

This excellent book is warmly recommended to students as well as established mathematicians who are interested in associative algebras. For those wishing to read only parts of the text, the subject index and the list of symbols are of great help.

Ágnes Szendrei (Szeged)

D. Pollard, Convergence of Stochastic Processes. XIV+215 pages, Springer-Verlag, New York—Berlin—Heidelberg—Tokyo, 1984.

Properties of empirical processes play an important role in mathematical statistics. Earlier results on this field, especially on the weak convergence of empirical measures can be found in the books of I. I. Gikhman and A. V. Skorokhod (Introduction to the Theory of Random Processes, Saunders, 1969 (in Russian 1965)), K. R. Parthasarathy (Probability Measures on Metric Spaces, Academic Press, 1967) and P. Billingsley (Convergence of Probability Measures, Wiley, 1968). These books have become classics and have generated a lot of work in the area. Recently R. M. Dudley (A Course on Empirical Processes, Lecture Notes in Math. vol. 1097, Springer-Verlag, 1985) and P. Gaenssler (Empirical Processes, IMS Lecture Notes vol. 3, IMS, 1983) have summarized the newest results on this topic and the book under review is another addendum to the literature. These three monographs cover nearly the same area of the theory of stochastic processes.

In Chapter I Pollard introduces notations of stochastic processes and empirical measures. Chapter II contains generalizations of the classical Glivenko—Cantelli theorem. He proves uniform convergence of empirical measures over classes of sets and classes of functions. The author gives a review on the weak convergence of probability measures on Euclidean and metric spaces in Chapters III and IV. Chapters V and VI deal with the weak convergence of empirical processes, properties of the limit processes and also contain some applications of the obtained results in mathematical statistics. Martingale central limit theorems are proven in Chapter VII and an application to the Kaplan—Meier (product-limit) estimator is sketched.

Pollard writes in his Preface: "A more accurate title for this book might be: An Exposition of Selected Points of Empirical Process Theory, With Related Interesting Facts About Weak Convergence, and Applications to Mathematical Statistics." It is certainly true that it is nearly impossible to write a book on empirical processes which would cover all the interesting and important theorems on these processes and also their applications. However, I think a research monograph must contain at least an up-to-date and rich enough list of references, and this cannot be replaced by saying "according to the statistical folklore..." (cf., for example, page 99). This is completely useless for a reader and hence I doubt that Pollard's monograph can be used as a reference book. On the other hand, the interested reader can certainly find some material collected together which was mainly published only in research papers earlier.

Lajos Horváth (Ottawa)

Probability in Banach Spaces V, Proceedings of the International Conference Held in Medford, USA, July 1984. Edited by A. Beck, R. Dudley, M. Hahn, J. Kuelbs and M. Marcus (Lecture Notes in Mathematics, 1153), VI+457 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985.

The proceedings of the first four conferences on probability in Banach spaces have been published as Volumes 526, 709, 860, and 990 in these Lecture Notes series. The present collection containes 25 articles, almost all of which are very high level research papers. 15 papers deal with limit theorems (the central limit theorem, empirical processes, large deviations, ratio limit theorems for sojourns and other weak theorems; the law of large numbers and of the iterated logarithm, almost sure convergence of martingale-related sequences and other strong theorems), the rest address various problems in sample path behaviour, representation questions, moment and other bounds, stable measures and infinite divisibility. The illustrious list of the authors may give an impression of the contents: de Acosta; Alexander; Austin, Bellow and Bouzar; Berman; Borell; Bourgain; Czado and Taqqu; Dudley; Fernique; Frangos and Sucheston; Giné and Hahn; Heinkel; Hoffman—Jørgensen; Jain; Jurek; Klass and Kuelbs; LePage and Schreiber; Marcus and Pisier; McConell; Rosinski and Woyczynski; Samur; Vatan; Weiner; Weron and Weron; and Zinn.

Sándor Csörgő (Szeged)

Murray H. Protter—Charles B. Morrey, Jr., Intermediate Calculus (Undergraduate Texts in Mathematics), X+648 pages, Springer-Verlag, New York—Berlin—Heidelberg—Tokyo, 1985.

If you teach a course on analytic geometry and calculus at a college or university, your first task is to choose a text-book. This is not easy at all. The course usually consists of three semesters. Typically, the first two semesters cover plane analytic geometry and the calculus of functions of one variable, almost independently of the majors in the audience. The decision on the subject-matter of the third semester (and of the fourth one, if any) requires more care. One must take into account the further study of the students: do they go on in mathematics or do they need the calculus only for applications? This book has been written to help the instructors in this decision by providing a high degree of flexibility in structuring the course.

The first five chapters present the material of a standard third-semester course in calculus (the knowledge of plane analytic geometry and one-variable calculus are a prerequisite): 1. Analytic Geometry in Three Dimensions; 2. Vectors; 3. Infinite Series; 4. Partial Derivatives. Applications; 5. Multiple Integration. The further chapters give an opportunity for the instructor to include less traditional topics in the third semester and to design a fourth semester of analysis depending upon special needs: 6. Fourier Series; 7. Implicit Function Theorems. Jacobians; 8. Differentiation under the Integral Sign. Improper Integrals. The Gamma Function; 9. Vector Field Theory; 10. Green's and Stokes' Theorems.

The main feature of the book is its flexibility. Of course, this can be meant in several ways. On the one hand, the chapters are independent of each other. On the other hand, within each chapter readers can find material of different levels. E.g. in Chapter 10 Green's theorem is established first for a simple domain (this results is adequate for most applications), but it is followed by Green's and Stokes' theorems for the general cases proved by using orientable surfaces and a partition of unity.

The book is concluded with three appendices on matrices, determinants, on vectors in three dimensions, and on methods of integration. The sections contain many interesting problems (answers to the odd-numbered ones are available at the end of the book).

This excellent text-book will be very useful both for instructors and students.

L. Hatvani (Szeged)

Representations of Lie Groups and Lie Algebras, Proceedings, Budapest 1971. Edited by A. A. Kirillov, 225 pages, Akadémiai Kiadó, Budapest, 1985.

The present book contains the second part of the Proceedings of the Summer School on representation theory which was held at Budapest in 1971. The first part of the Proceedings was published by the Akadémiai Kiadó (edited by I. M. Gelfand) in 1975. The scientific program of the school was divided into two sections: advanced and beginner. Most of the lectures published here were read at the latter section but some of them are now rewritten or completed by new authors.

A. A. Kirillov's introductory lecture gives a summary of the basic notions, results and methods in the representation theory of finite and compact groups. The article by B. L. Feigin and A. V. Zelevinsky makes the reader acquainted with the theory of contragradient Lie algebras and their representations. In his paper D. P. Zhelobenko dissusses the constructive description of Gelfand—Zetlin bases for classical Lie algebras $\mathrm{gl}(n, \mathbf{C})$, $\mathrm{o}(n, \mathbf{C})$, $\mathrm{sp}(n, \mathbf{C})$. The method presented here is very effective in obtaining explicit formulas of the representation theory. The lecture by S. Tanaka is devoted to an instructive example; explicit description of all irreducible representations of the group $\mathrm{Sl}(2, F)$ where F is a finite field. The survey by I. M. Gelfand, M. I. Graev and A. M. Vershik "Models of representations of current groups" deals with a class of infinite dimensional Lie groups which is of great importance for physical applications. The authors describe in detail several classical as well as new models of the representations of current groups. G. J. Olshansky's article "Unitary representations of the infinite symmetric group: a semigroup approach" is devoted to the representation theory of another type of the "big" groups. The last lecture by G. W. Mackey is addressed first of all to physicists. It explains how the imprimitivity theorem and the concept of induced representations play an important role in quantum mechanics.

Most of the content of this book is accessible for beginners, but experts will also find some new and useful information in the articles published here.

L. Gy. Fehér (Szeged)

Representation Theory II, Proceedings, Ottawa, Carleton University, 1979, edited by V. Dlab and P. Gabriel (Lecture Notes in Mathematics, 832), XIV+673 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1980.

The first volume of these proceedings in two volumes contains reports from the "Workshop on the Present Trends in Representation Theory" held at Carleton University, 13—18 August, 1979. The present volume contains the majority of the lectures delivered at the second part of the meeting "The Second International Conference on Representations of Algebras" (13—25 August, 1979), but some papers which were not reported at the conference are also published here. These two volumes together (the first volume contains also an extensive bibliography of the publications in the field covering the period 1969—1979) provide the interested reader with a comprehensive survey on the modern results and research directions of the representation theory of algebras. The list of the authors contributed to this volume is: M. Auslander—I. Reiten, M. Auslander—S. O. Smalo, R. Bautista, K. Bongartz, S. Brenner—M. C. R. Butler, H. Brune, C. W. Curtis, E. C. Dade, V. Dlab—C. M. Ringel, P. Dowbor—C. M. Ringel—D. Simson, Ju. A. Drozd, E. L. Green, D. Happel—U. Preiser—C. M. Ringel, Y. Iwanaga—T. Wakamatsu, C. U. Jensen—H. Lenzing, V. C. Kač, H. Kupisch—E. Scherzler, P. Landrock, N. Marmaridis, R. Martinez-Villa, F. Okoh, W. Plesken, C. Riedtmann, K. W. Roggenkamp, E. Scherzler—J. Waschbüsch, D. Simson, H. Tachikawa, G. Todorov, J. Waschbüsch, K. Yamagata.

L. Gy. Fehér (Szeged)

Rings and Geometry, Proceedings of the NATO Advanced Study Institute held at Istambul, Turkey, September 2—14, 1984. Edited by R. Kaya, P. Plaumann and K. Strambach (NATO ASI Series C: Mathematical and Physical Sciences, Vol. 160), XI+567 pages, D. Reidel Publishing Company, Dordrecht—Boston—Lancaster—Tokyo, 1985.

This volume contains 11 lectures given at the summer school on Rings and Geometry.

Until quite recently, when looking for applications of ring theory in geometry, we could mainly think of abstract algebraic geometry which can be formulated in the language of commutative algebra. Of course the connections between ring theory and geometry cannot be circumscribed only by the subject of algebraic geometry. There are some old and new areas in mathematics, highly developed in the last decades, which are the results of the interaction of ring theory and geometry. The editors write in the Preface: "It is the aim of these proceedings to give a unifying presentation of those geometrical applications of ring theory outside of algebraic geometry, and to show that they offer a considerable wealth of beautiful ideas, too. Furthermore it becomes apparent that there are natural connections to many branches of modern mathematics, e.g. to the theory of (algebraic) groups and of Jordan algebras, and to combinatorics".

The book consists of four parts. In the first one the non-commutative analogue of the function field of an algebraic variety and the generalization of classical objects of algebraic geometry to the case of non-commutative coordinate field are studied. (P. M. Cohn, Principles of non-commutative algebraic geometry; H. Havlicek, Application of results on generalized polynomial identities in Desarguesian projective spaces.) The second part is devoted to the study of topological, incidence-theoretical, algebraic and combinatorial properties of Hjelmslev planes. (J. W. Lorimer, A topological characterization of Hjelmslev's classical geometries, D. A. Drake—D. Jungnickel, Finite Hjelmslev planes and Klingenberg epimorphisms.) The third part contains the treatment of the theory of projective planes over rings "of stable rank 2". (J. R. Faulkner—J. C. Ferrar, Generalizing the Moufang plane; F. D. Veldkamp, Projective ring planes end their homomorphisms.) The authors of the papers in the fourth part study the possibility of the extension of the classical relations between projective geometry and linear algebra, investigate the structure of linear, orthogonal, symplectic and unitary groups and matrix rings over large classes of rings, the geometric structure of the units of alternative quadratic algebras and the coordinatization of lattice-geometry. (C. Bartolone—F. Bartolozzi, Topics in geometric algebra over rings; B. R. McDonald, Metric geometry over localglobal commutative rings, Linear mappings of matrix rings preserving invariants; H. Karzel—G. Kist, Kinematic algebras and their geometries; U. Brehm, Coordinatization of lattices.) An appendix describes some concepts of geometry indispensable for mathematics. (C. Arf, The advantage of geometric concepts in mathematics.)

This book is warmly recommended to anybody interested in the interaction of algebra and geometry. It can be used as an up-to-date reference book "in that area of mathematics where the ring theory accuring outside of algebraic geometry is harmonically unified with geometry".

Péter T. Nagy (Szeged)

Murray Rosenblatt, Stationary Sequences and Random Fields, 258 pages, Birkhäuser, Boston—Basel—Stuttgart, 1985.

The first systematic book on time series analysis was "Statistical Analysis of Stationary Time Series" by Ulf Grenander and Murray Rosenblatt published in 1957 by Wiley. Since then a number of excellent monographs of the field have appeared reflecting the fast growth of knowledge. Now, 28 years after his first book, here is a second look of one of the foremost researchers of the topic. As he writes in the preface: "This book has a dual purpose. One of these is to present material which selectively will be appropriate for a quarter or semester course in time series analysis and which will cover both the finite parameter and the spectral approach. The second object is the presentation of topics of current research interest and some open questions".

Chapter I presents basic results on the Fourier representation of the covariance function of a weakly stationary process and the harmonic analysis of the process itself, that is the Herglotz and Cramér theorems. Chapter II formulates the problem of linear prediction, or linear mean square approximation, gives the basic relations between moments and cumulants, fully discusses the linear prediction problem for autoregressive and moving average (ARMA) processes, describes the Kalman—Bucy filter, and investigates the identifiability of the phase function of a non-Gaussian linear process (one of the several novelties of the book, to be fully taken up in Chapter VIII). Of particular interest to a probabilist is Chapter III. It first gives Gordin's device to obtain central limit theorems for partial sums of strictly stationary sequences from those for a martingale difference sequence, then this is used to prove asymptotic normality for general covariance estimators and quadratic forms including the periodogram under cumulant summability conditions. A nice discussion of strong mixing, one of the many important spiritual children of the author, is given together with a basic central limit theorem of the author for strongly mixing sequences. Exotic behaviour under long-range dependence is also discussed here. Chapter IV gives the estimation theory for ARMA schemes with new results, based partly on those in Chapter III, on asymptotic normality in which, besides strong mixing, only the finiteness of a few moments are assumed. Chapters V and VI deal with second and higher order cumulant spectral density estimation, respectively, assuming strong mixing and requiring again only the finiteness of a few moments in the asymptotic normality results. The brief Chapter VII is on kernel density and regression function estimates under "short range" dependence. The final Chapter VIII is on various questions of estimating the phase or transfer functions and moments of non-Gaussian linear processes and fields with the associated deconvolution problems. A short appendix gethers some facts of measure theory, of Hilbert and Banach spaces and Banach algebras. Author and subject indices help the reader.

The last sections of the chapters discuss how the results for sequences extend for fields, what are the difficulties, limitations, etc. There are Monte Carlo simulations for the comparison of the deconvolution procedures and various concrete applications involving turbolence and energy transfer are scattered through the book beginning with the fourth chapter. Occasional figures illustrate the text and the arising computational questions receive sensitive discussions. Each chapter ends with a set of problems that can be given to students, followed by a set of notes providing further examples, explanations, references to and descriptions of the literature and many open problems for further research are discussed at some length.

The text goes very smoothly, it is thoughtful, sympathetic and (sometimes overly) modest. You feel as if you would be inventing what you read and forget that you hear everything from the horse's mouth. Both the mathematics and the discussion concentrates on the essence of the problem at hand, heuristics constitute an integral part of the matter, and unnecessary details are elegantly sidestepped. The main achievment of the book is, I think, that it can be read enjoyably and profitably on several different levels of understanding, with various backgrounds. Thus the author has considerably surpassed his "dual purpose".

The reviewer was fortunate enough to have the opportunity of sitting in a course "Time Series Analysis" that Professor Rosenblatt gave for upper undergraduate and early graduate students in the spring quarter of 1985, at the University of California, San Diego, using the galley proofs of the present book. He covered most of the material in Chapters I, II, IV, and V, motivating the necessary results from Chapter III and from the elements of probability theory and Fourier analysis on heuristic grounds. (This is what he advises to do in his preface.) The course, attended besides the 15—20 students by other senior guests with the Department of Mathematics and a few research workers from some applied departments of UCSD, was a real success.

The book will be inevitable for students, instructors, regular users, occasional appliers, and researchers of time series analysis as well.

Sándor Csörgő (Szeged)

James G. Simmonds, A Brief on Tensor Analysis, VIII+92 pages, Under-Graduate Texts in Mathematics, Springer-Verlag, New York—Heidelberg—Berlin, 1982.

The book is divided into four chapters. The first chapter introduces the concept of vectors and defines the dot product and cross product of vectors. A second order tensor is defined as a linear operator that sends vectors into vectors. Chapter 2 is devoted to the description of tensors by using general bases and their dual bases and covariant and contravariant coordinates of vectors. Chapter 3 deals with the Newton law of motion, introduces moving frames and the Christoffel symbols. The last chapter presents a short glimpse into vector and tensor analysis, introducing the notions of a gradient operator, divergence and covariant derivatives. All the chapters end with a set of exercises. The book may serve as a text for first or second-year undergraduates.

L. Gehér (Szeged)

Gary A. Sod, Numerical Methods in Fluid Dynamics: Initial and Initial Boundary-Value Problems, IX+446 pages, Cambridge University Press, Cambridge—London—New York—New Rochelle—Melbourne—Sydney, 1985.

In fact there is practically very little about fluid dynamics in this book, intended to provide the foundations for Volume II, which — according to the author's preface — will deal exclusively with the equations governing fluid motion. This volume is rather a text on numerical methods for solving partial differential equations and it is directed at graduate students.

The book deals with the finite difference method, the other, not less powerful method of finite elements is not discussed. Nevertheless it is very useful for everyone, wishing to actually apply the results of numerical analysis of partial differential equations in any field.

The book consists of the following chapters: I. Introduction, II. Parabolic Equations, III. Hyperbolic Equations, IV. Hyperbolic Conservation Laws, V. Stability in the Presence of Boundaries. It is written from the physicist's and engineer's point of view, which does not mean that it would lack mathematical rigor. It is simply detailed enough to be comprehensible for the mathematically less trained reader. It emphasises the concepts and contains all the necessary definitions and theorems about convergence and stability, indispensable for those too who want only good recipes. Several methods for solving parabolic and hyperbolic equations are introduced and analysed, and the problem of boundaries is dealt thoroughly. The more sophisticated mathematical theorems and proofs are avoided, some of them are left to the 4 appendices.

Reading the book, all the natural questions arising in the reader are answered by the author, except for one: Why this title? It certainly calls the attention of practitioners in the field of fluid dynamics, but one is afraid that the set of potential readers will unnecessarily be restricted. One can warmly recommend this book to anybody who just wants to find a good introduction to the finite difference method for solving parabolic and hyperbolic equations.

M. G. Benedict (Szeged)

Edwin H. Spanier, Algebraic Topology, XIV+528 pages, Springer-Verlag, New York—Heidelberg—Berlin, 1982.

This is the second edition of the original text first published in 1966 by McGraw-Hill. It starts with an introductory part summarising the basic concepts of set theory, general topology and algebra. The material is divided into three main parts each of which consists of three chapters. The first three chapters introduce the concepts of homotopy and the fundamental group and apply these in the study of covering spaces and polyhedras. The second three chapters are devoted to homology and cohomology theory. The general cohomology theory and duality in topological manifolds are studie here, too. For each new concept, applications are presented to illustrate its utility. In the last three chapters homotopy theory is studied; basic facts about homotopy groups are considered, some applications to obstruction theory are presented and in the last chapter some computations of homotopy groups of spheres can be found.

No prior knowledge of algebraic topology is assumed but some faimiliarity of the reader in general topology and algebra is preassumed.

L. Gehér (Szeged)

Stability Problems for Stochastic Models, Proceedings of the 8th International Seminar Held in Uzhgorod, September 1984. Edited by V. V. Kalashnikov and V. M. Zolotarev (Lectures Notes in Mathematics, 1155), VI+447 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985.

Although the 23 papers collected in this volume represent somewhat more diverse research activities than the 22 papers in the predecessor collection under the same title (Lecture Notes in Mathematics, 982), almost everything that I wrote about that one (these *Acta,* 47 (1984), page 260) is valid for the present proceedings. Characterization problems and related questions still constitute a strong topic in the volume, but there is a noticable shift towards limit theorems and convergence-rate problems.

Sándor Csörgő (Szeged)

Stochastic Space-Time Models and Limit Theorems. Edited by L. Arnold and P. Kotelenez (Mathematics and its Applications), XI+266 pages, D. Reidel Publishing Company, Dordrecht—Boston—Lancaster, 1985.

This is the first volume of a new series launched by the D. Reidel Company. In his preface Series Editor M. Hazewinkel emphasizes "the unreasonable effectiveness of mathematics in science" (to quote one of his six mottoes, this one due to E. Wigner) and outlines the aims of this new programme.

The book presents the 13 invited papers presented at a workshop held at the University of Bremen, FRG, in November 1983, describing the state of the art of the mathematics of space-time phenomena, a specific combination of the modern theory of stochastic processes and functional analysis. These widely applicable models describe motions which change with time and are randomly distributed in space, and are usually given by stochastic differential equations. The first seven surveys (by Albaverio, Høegh—Krohn and Holden; Da Prato; Dettweiler; Ichikawa; Kotelenez; Krée; and Ustunel) are devoted to the existence, uniqueness and regularity problems of solutions of stochastic partial differential equations, and in general to stochastic analysis and Markov processes in infinite dimensions. The other six papers (by Van den Broeck; Grigelionis and Mikulevičius; Metivier; Pardoux; Rost; and Zessin) deal with various limit theorems where stochastic processes describing a space-time model emerge as limits of sequences of stochastic processes on lattices or of positions of finitely many particles with several kinds of interaction.

An intelligent unifying introduction by Kotelenez puts the whole contents in a broad perspective and a subject index helps orientation.

If the editors will be able to maintain the high level set by this very carefully compiled first volume, this series will no doubt be a success.

Sándor Csörgő (Szeged)

Symposium on Anomalies, Geometry and Topology, Proceedings, Chicago, United States, 1985. Edited by W. A. Bardeen and A. R. White, XVIII+558 pages, World Scientific, 1985.

This book contains the proceedings of the Symposium on Anomalies, Geometry and Topology, which took place at the Argonne National Laboratory of the US and at the University of Chicago on March 28—30, 1985.

The 56 papers published here report on the recent progress made in field theory and particle physics mostly by means of the application of sophisticated geometrical-topological methods and results. One of the main concerns pursued in the lectures is the new superstring physics—hopefully the right candidate to become a real "Theory of Everything". The other subject which dominated the talks is the mathematical structure of anomalies. Anomalies, originally appeared in perturbative calculations, are now related to properties of Dirac operators and to the connected index theorems of Atiyah and Singer, as well as to homotopy, cohomology and complex structure of manifolds in four and higher dimensions. The investigation of anomalies is an important part of the consistency analysis of quantum field theories. For example, anomaly cancellations played a crucial role in the recent breakthrough achieved in superstring theory. In addition to the main topics of the Symposium, anomalies and superstrings, there were special sessions devoted to charge fractionalization and compactification issues and to the method of effective Lagrangians in various models. Beyond the mentioned ones, the book also contains articles concerning several subjects somehow related to the above. Just to give examples, there are papers addressed to the quantum mechanics of black holes, or dealing with the global structure of supermanifolds. Amongst the authors are M. F. Atiyah, M. Green, D. Gross, R. Jackiw, V. Kac, J. R. Schrieffer, J. Stasheff, G.'t Hooft, E. Witten, S. T. Yau, B. Zumino and many other outstanding scientists. This list clearly proves how close is the connection between pure mathematics and theoretical physics these days.

In conclusion, this collection of high level papers is warmly recommended to everybody interested in the exciting developments reported in it.

L. Gy. Fehér (Szeged)

Universal Algebra and Lattice Theory (Proceedings, Charleston 1984). Edited by S. D. Comer (Lecture Notes in Mathematics 1149), VI+282 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985.

This volume contains research papers on universal algebra and lattice theory, mostly based on lectures presented at the conference in Charleston, 1984. "In keeping with the tradition set by its origin, it is notable that there are a number of papers that deal with connections between lattice theory and universal algebra and other areas of mathematics such as geometry, graph theory, group theory and logic." The list of the papers is as follows.

M. E. Adams and D. M. Clark: Universal terms for pseudo-complemented distributive lattices and Heyting algebras; H. Andréka, S. D. Comer and I. Németi: Clones of operations on relations; M. K. Bennett: Separation conditions on convexity lattices; A. Day: Some independence results in the co-ordinization of Arguesian lattices; Ph. Dwinger: Unary operations on completely distributive complete lattices; R. Freese: Connected components of the covering relation in free lattices; B. Ganter and T. Ihringer: Varieties of linear subalgebra geometries; O. C. Garcia and W. Taylor: Generalized commutativity; A. M. W. Glass: The word and isomorphism problems in universal algebra; M. Haiman: Linear lattice proof theory: an overview; D. Higgs: Interpolation antichains in lattices; J. Jezek: Subdirectly irreducible and simple Boolean algebras with endomorphisms; E. W. Kiss: A note on varieties of graph algebras; G. F. McNulty: How to construct finite algebras which are not finitely based; R. Maddux: Finite integral relation algebras; J. B. Nation: Some varieties of semidistributive lattices; D. Pigozzi and J. Sichler: Homomorphisms of partial and of complete Steiner triple systems and quasigroups; A. F. Pixley: Principal congruence formulas in arithmetical varieties; A. B. Romanowska and J. D. H. Smith: From affine to projective geometry via convexity; S. T. Tschantz: More conditions equivalent to congruence modularity.

The book gives a good account on several directions of the current research, and it is warmly recommended to research workers interested in the subject.

Gábor Czédli (Szeged)

Vertex Operators in Mathematics and Physics, Proceedings, Berkeley, 1983. Edited by J. Lepowsky, S. Mandelstam and I. M. Singer (Mathematical Sciences Research Institute Publications, 3), XIV+482 pages, Springer-Verlag, New York—Berlin, Heidelberg—Tokyo, 1985.

This volume includes proceedings from the Conference on Vertex Operators in Mathematics and Physics, held at the Mathematical Sciences Research Institute, Berkeley, November 10—17, 1983.

Among the subjects of highest current interest in physics and mathematics are the superstring, supergravity theories on the one hand and the theory of infinite dimensional Lie algebras on the other hand. In the last few years interesting connections have been found between the dual-string theory and the affine Kac—Moody algebras, through the use of vertex operators that originally appeared in the interaction Hamiltonians of the string models. The central role of the mentioned theories in contemporary mathematics and physics made it possible to explore interrelations between seemingly so remote topics as string models, number theory, sporadic groups, integrable systems, the Virasoro algebra and so on. To explore further connections — this was the purpose of the Conference. Most informatory for an expert can be the table of contents of the book under review, so we give it below.

Section 1 — String models. S. Mandelstam: Introduction to string models and vertex operators; O. Alvarez: An introduction to Polyakov's string model; T. Curtright: Conformally invariant field theories in two dimensions.

Section 2 — Lie algebra representations. P. Goddard and D. Olive: Algebras, lattices and strings; J. Lepowsky and R. L. Wilson: Z-algebras and the Rogers—Ramanujan identities; J. Lepowski and M. Primc: Structure of the standard modules for the affine Lie algebra $A_1^{(1)}$ in the homogeneous picture; K. C. Misra: Standard representations of some affine Lie algebras; A. J. Feingold: Some applications of vertex operators to Kac—Moody algebras; M. Jimbo and T. Miwa: On a duality of branching coefficients.

Section 3 — The Monster. R. L. Griess: A brief introduction to finite simple groups; I. B. Frenkel, J. Lepowsky and A. Meurman: A Moonshine Module for the Monster.

Section 4 — Integrable systems. M. Jimbo and T. Miwa: Monodromy, solitons and infinite dimensional Lie algebras; K. Ueno: The Riemann—Hilbert decomposition and the *KP* hierarchy; Ling-Lie Chau: Supersymmetric Yang—Mills fields as an integrable system and connections with other non-linear systems; Yong-Shi Wu and Mo-Lin Ge: Lax pairs, Riemann—Hilbert transforms and affine algebras for hidden symmetries in certain nonlinear field theories; L. Dolan: Massive Kaluza—Klein theories and bound states in Yang—Mills; I. Bars: Local charge algebras in quantum chiral models and gauge theories; B. Julia: Supergeometry and Kac—Moody algebras.

Section 5 — The Virasoro algebra. C. B. Thorn: A proof of the no-ghost theorem using the Kac determinant; D. Friedan, Zongan Qiu and S. Shenker: Conformal invariance, unitarity and two dimensional critical exponents; A. Rocha—Caridi: Vacuum vector representations of the Virasoro algebra; N. R. Wallach: Classical invariant theory and the Virasoro algebra.

J. Lepowsky writes in the Introduction: "The excitement of discovering surprising connections between different disciplines has become a rule in the subject of this volume". There is no doubt that the present interaction between mathematicians and physicists continues and that this book will be very useful for all experts involved in it.

L. Gy. Fehér (Szeged)

M. Zamansky, Approximation des Fonctions (Travaux en Cours), V+91 pp., Hermann, Paris, 1985.

A more appropriate title would be "Approximation of periodic functions" because Zamansky's small treatise is entirely devoted to periodic functions of a single or several variables. The author belongs to that prominent group of mathematicians who nursed the theory of harmonic approximation through its infancy and in this book he twisted again on the usual course of events, namely he provided us with a rather unconventional treatment of the subject. Today it is uncommon, though it may be refreshing, to put multipliers into the heart of the subject. The notations are also peculiar which may cause some headache for the expert who wants to use the book as a reference. Nevertheless, the topics covered are familiar and they provide an independent introduction to harmonic approximation in L^p and C spaces. Both the book's strength and its weakness lies in its concise form. On the one hand this enables the author to consider several spaces and approximation methods simultaneously, on the other hand too general statements blur the necessary distinction between important and unimportant (methods, for example) and hide the differences between certain spaces (e.g. L^1 and L^p, $p>1$) that play(d) so important role in mathematics.

Very briefly the contents: Chapter 1: Approximation of functions of a single variable (Fourier series, moduli of smoothness, generalizations of Jackson's estimate and its converse, conjugate series, derivatives of functions, saturation with many examples); Chapter 2: Convolutions (equivalence of convolution processes, saturation, direct and converse theorems); Chapter 3: Multidimensional case. A 9 page historical account closes the book.

V. Totik (Szeged)

Livres reçus par la rédaction

W. Ballmann—M. Gromov—V. Schroeder, Manifolds on nonpositive curvature (Progress in Mathematics, Vol. 61), IV+263 pages, Birkhäuser Verlag, Boston—Basel—Stuttgart, 1985.

M. Barr—C. Wells, Toposes, triples and theories (Grundlehren der mathematischen Wissenschaften, Bd. 278), XIII+345 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. DM 138,—.

M. J. Beeson, Foundations of constructive mathematics. Metamathematical studies (Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Bd. 6), XXIII+466 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 168,—.

C. Camacho—A. Lins Neto, Geometric theory of foliations, V+205 pages, Birkhäuser Verlag, Boston—Basel—Stuttgart, 1985.

J. B. Conway, A course in functional analysis (Graduate Texts in Mathematics, Vol. 96), XIV+404 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 118,—.

Differential Geometric Methods in Mathematical Physics. Proceedings of an International Conference held at the Technical University of Clausthal, FRG, August 30—September 2, 1983. Edited by H.-D. Doebner, J.-D. Hennig (Lecture Notes in Mathematics, Vol. 1139), VI+337 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 51,50.

B. A. Dubrovin—A. T. Fomenko—S. P. Novikov, Modern geometry — Methods and applications, Part 2: The geometry and topology of manifolds. Translated by R. G. Burns (Graduate Texts in Mathematics, Vol. 104), XV+430 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 158,—.

Dynamical Systems and Bifurcations. Proceedings of a Workshop held in Groningen, The Netherlands, April 16—20, 1984. Edited by B. L. J. Braaksma, H. W. Broer, F. Takens, V+129 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 21,50.

E. Grosswald, Representations of integers as sums of squares, XI+251 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 148,—.

W. R. Knorr, The ancient tradition of geometric problems, IX+411 pages, Birkhäuser Verlag, Boston—Basel—Stuttgart, 1986.

H. König, Eigenvalue distribution of compact operators (Operator Theory: Advances and Applications, Vol. 16), 262 pages, Birkhäuser Verlag, Boston—Basel—Stuttgart, 1986.

O. A. Ladyzhenskaya, The boundary value problems of mathematical physics. Translated from the Russian by J. Lohwater (Applied Mathematical Sciences, Vol. 49), XXX+322 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 198,—.

S. Lang, Complex analysis. 2nd edition (Graduate Texts in Mathematics, Vol. 103), XIV+367 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 128,—.

L. Leindler, Strong approximation by Fourier series, 210 pages, Akadémiai Kiadó, Budapest, 1985.

J. Marsden—A. Weinstein, Calculus I, 2nd edition (Undergraduate Texts in Mathematics), XV+385 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 69,—.

————, **Calculus II,** 2nd edition (Undergraduate Texts in Mathematics), XV+345 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 69,—.

____________, **Calculus III,** 2nd edition (Undergraduate Texts in Mathematics), XV+341 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 69,—.

Model-Theoretic Logics. Edited by J. Barwise, S. Feferman (Perspectives in Mathematical Logic), XVIII+895 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 480,—.

Nonlinear Analysis and Optimization. Proceedings of the International Conference held in Bologna, Italy, May 3—7, 1982. Edited by C. Vinti (Lecture Notes in Mathematics, Vol. 1107), V+214 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1984. — DM 31,50.

B. Oksendal, Stochastic differential equations. An introduction with applications (Universitext), XIII+205 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 42,—.

Orders and their Applications. Proceedings of a Conference held in Oberwolfach, West Germany, June 3—9, 1984. Edited by I. Reiner, K. W. Roggenkamp (Lecture Notes in Mathematics, Vol. 1142), X+306 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 45,—.

Ordinary and Partial Differential Equations. Proceedings of the Eighth Conference held at Dundee, Scotland, June 25—29, 1984. Edited by B. D. Sleeman, R. J. Jarvis (Lecture Notes in Mathematics, Vol. 1151), XIV+357 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 51,50.

Probability in Banach Spaces V. Edited by A. Beck, R. Dudley, M. Hahn, J. Knelbs and M. Marcus (Lecture Notes in Mathematics, Vol. 1153), VI+460 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 64,—.

M. H. Protter—C. B. Morrey, Intermediate calculus. 2nd edition (Undergraduate Texts in Mathematics), X+650 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 128,—.

Recursion Theory Week. Proceedings of a Conference held in Oberwolfach, West Germany, April 15—21, 1984. Edited by H.-D. Ebbinghaus, G. H. Müller, G. E. Sacks (Lecture Notes in Mathematics, Vol. 1141), IX+418 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 57,—.

Representations of Lie Groups and Lie Algebras. Edited by A. A. Kirillov, 225 pages, Akadémiai Kiadó, Budapest, 1985.

M. Rosenblatt, Stationary sequences and random fields, 258 pages, Birkhäuser Verlag, Boston—Basel—Stuttgart, 1985.

N. Z. Shor, Minimization methods for non-differentiable functions. Translated from the Russian by K. C. Kiwiel, A. Ruszczynski (Springer Series in Computational Mathematics, Vol. 3), VIII+162 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 84,—.

C. Smorynski, Self-reference and modal logic (Universitext), XII+333 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 88,—.

G. A. Sod, Numerical methods in fluid dynamics, IX+446 pages, Cambridge University Press, Cambridge—London—New York, 1985. — £ 30.00.

F. H. Soon, Student's guide to calculus by J. Marsden and A. Weinstein, Vol. 1, XIV+312 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 48,—.

Stability Problems for Stochastic Models. Edited by V. V. Kalashnikov and V. M. Zolotarev (Lecture Notes in Mathematics, Vol. 1155), VI+450 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 64,—.

Stochastic Analysis and Applications. Proceedings of the International Conference held at Swansea, April 11—15, 1983. Edited by A. Truman, D. Williams (Lecture Notes in Mathematics, Vol.

1095), V+199 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1984. — DM 31,50.

A. Terras, Harmonic analysis on symmetric spaces and applications I, XV+341 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 138,—.

Theoretical Approaches to Turbulence. Edited by D. L. Dwoyer, M. Y. Hussaini, R. G. Voigt (Applied Mathematical Sciences, Vol. 58), XII+373 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 118,—.

A. N. Tikhonov—A. B. Vasileva—A. G. Sveshnikov, Differential equations. Translated from the Russian by A. B. Sossinskij (Springer Series in Soviet Mathematics), VIII+238 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 98,—.

Topics in the Theoretical Bases and Applications of Computer Science. Proceedings of the 4th Hungarian Computer Science Conference Győr, Hungary, July 8—10, 1985. Edited by M. Arató, I. Kátai, L. Varga, X+514 pages, Akadémiai Kiadó, Budapest, 1986.

Universal Algebra and Lattice Theory. Edited by S. D. Corner (Lecture Notes in Mathematics, Vol. 1149), VI+286 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 38,50.

R. L. Vaught, Set theory, X+141 pages, Birkhäuser Verlag, Boston—Basel—Stuttgart, 1985.

Vertex Operators in Mathematics and Physics. Edited by J. Lepowski, S. Mandelstam, I. M. Singer (Mathematical Sciences Research Institute Publications, Vol. 3), XIV+482 pages, Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985. — DM 98,—.

M. Zamansky, Approximation des fonctions, VII+93 pages, Hermann, Paris, 1985. — 160 F.

TOMUS L—1986—50. KÖTET

Bibliographie

Advances in Probability Theory: Limit Theorems and Related Topics. — Asymptotic Analysis II — Surveys and New Trends. — J. P. AUBIN—A. CELLINA, Differential Inclusions. — M. J. BEESON, Foundations of Constructive Mathematics, Mathematical Studies. — G. W. BLUMAN, Problem Book for First Year Calculus. — K. W. CHANG—F. A. HOWES, Nonlinear Singular Perturbation Phenomena: Theory and Applications. — Convex Analysis and Optimization. — J. B. CONWAY, A Course in Functional Analysis. — J. B. CONWAY, Functions of One Complex Variable. — J. DIESTEL, Sequences and Series in Banach Spaces. — Differential Geometry and Complex Analysis. — H. E. EDWARDS, Galois Theory. — L. EULER, Elements of Algebra. — L. R. FOULDS, Combinatorial Optimization for Undergraduates. — D. S. FREED—K. K. UHLENBECK, Instantons and Four-Manifolds. — J. K. HALE—L. T. MAGALHÃES—W. M. OLIVA, An Introduction to Infinite Dimensional Dynamical Systems: Geometric Theory. — Infinite-Dimensional Systems. — D. KLETZING, Structure and Representation of Q-Groups. — M. A. KRASNOSEL'SKIĬ—P. P. ZABREĬKO, Geometrical Methods of Nonlinear Analysis. — Lie Group Representations III. — Linear and Complex Analysis Problem Book. — D. H. LUECKING—L. A. RUBEL, Complex Analysis: A Functional Analysis Approach. — B. MALGRANGE, Lectures on the Theory of Functions of Several Complex Variables. — J. MARSDEN—A. WEINSTEIN, Calculus I—II—III. — T. MATOLCSI, A Concept of Mathematical Physics: Models for Space-Time. — V. A. MOROZOV, Methods for Solving Incorrectly Posed Problems. — J. D. MURRAY, Asymptotic Analysis. — Nonlinear Analysis and Optimization. — Y. OKUYAMA, Absolute Summability of Fourier Series and Orthogonal Series. — D. P. PARENT, Exercises in Number Theory. — Probability Theory on Vector Spaces III. —

ACTA SCIENTIARUM MATHEMATICARUM

LIST OF PAPERS IN THE ALPHABETICAL ORDER OF THE NAMES OF AUTHORS

TOM. 1 (1922)—TOM. 50 (1986)

A

B

C

D

F

H

I

J

K

L

M

N

O

P

RÉDEI, L., Ein neuer Beweis des quadratischen Reziprocitätssatzes .... **1** (1922/23), 134—138

——— Ein kombinatorischer Satz .... **7** (1934/35), 39—43

——— Über den Fundamentalsatz der Abelschen Gruppen von endlicher Ordnung .... **10** (1941/43), 109—111

——— Zur Gaußischen Theorie der Reduktion binärer quadratischer Formen....... **10** (1941/43), 134—140

——— Bemerkung zu einer Arbeit von R. Fueter über die Klassenkörpertheorie .... **11** (1946/48), 37—38

——— Über einige merkwürdige Polynome in endlichen Körpern mit zahlentheoretischen Beziehungen .... **11** (1946/48), 39—54

——— Zur Theorie der Gleichungen in endlichen Körpern....... **11** (1946/48), 63—70

——— Über eindeutig umkehrbare Polynome in endlichen Körpern.... **11** (1946/48), 85—92

——— Über die Gleichungen dritten und vierten Grades in endlichen Körpern....... **11** (1946/48), 96—105

——— Bemerkung zu meiner Arbeit „Über die Gleichungen dritten und vierten Grades in endlichen Körpern“ .... **11** (1946/48), 184—190

——— Elementarer Beweis und Verallgemeinerung einer Reziprozitätsformel von Dedekind....... **12 B** (1950), 236—239

——— Vereinfachter Beweis des Satzes von Minkowski—Hajós....... **13** (1949/50), 21—35

——— Über die Wertverteilung des Jacobischen Symbols....... **13** (1949/50), 242—246

——— Die Verallgemeinerung der Schreierschen Erweiterungstheorie... **14** (1951/52), 252—273

——— Die Existenz eines ungeraden quadratischen Nichtrestes mod p im Intervall $1, \sqrt{p}$ .... **15** (1953/54), 12—19

——— Über die Ringe mit gegebenem Modul....... **15** (1953/54), 251—254

——— Äquivalent der Sätze von Kronecker—Hensel und von Szekeres für die Ideale des Polynomringes einer Unbestimmten über einem kommutativen Hauptidealring mit Primzerlegung .... **17** (1956), 198—202

——— Über die algebraischzahlentheoretische Verallgemeinerung eines elementarzahlentheoretischen Satzes von Zsigmondy....... **19** (1958), 98—126

——— Eine Bemerkung über die endlichen einstufig nichtkommutativen Gruppen .... **19** (1958), 127—128

——— Ein spezieller Diskriminantensatz über Polynome .... **20** (1959), 234—237

——— Die einstufig nichtregulären Ringe....... **20** (1959), 238—244

——— Über die quadratischen Zahlkörper mit Primzerlegung .... **21** (1960), 1—3

——— Ein Überdeckungssatz für endliche abelsche Gruppen im Zusammenhang mit dem Hauptsatz von Hajós .... **26** (1965), 55—62

——— Einige Teilbarkeitskriterien....... **34** (1973), 345—348

——— see SZÉP, J.

RÉDEI, L. und STEINFELD, O., Gegenseitige Schreiersche Gruppenerweiterungen .... **15** (1953/54), 243—250

RÉDEI, L. und STOHR, A., Über ein spezielles schiefes Produkt in der Gruppentheorie .... **15** (1953/54), 7—11

RÉDEI, L. und SZELE, T., Die Ringe „ersten Ranges“ .... **12 A** (1950), 18—29

RÉDEI, L. und SZÉP, J., Verallgemeinerung der Theorie des Gruppenproduktes von Zappa—Casadio .... **16** (1955), 165—170

RÉDEI, L. und WEINERT, H. J., Ein Gleichverteilungssatz für Systeme homogener Linearformen .... **27** (1966), 41—44

——— Verallgemeinerung eines Satzes über homogene Linearformen ... **27** (1966), 45—48

S

T

TANDORI, K., Über die Cesàrosche Summierbarkeit der orthogonalen Reihen .... 14 (1951/52), 85—95
——— Über die Konvergenz singulärer Integrale .... 15 (1953/54), 223—230
——— Über die Divergenz der Fourierreihen .... 15 (1953/54), 236—239
——— Über die starke Summation von Fourierreihen .... 16 (1955), 65—73
——— Über orthogonale Reihen .... 16 (1955), 74—76
——— Über die orthogonalen Funktionen. I. .... 18 (1957), 57—130
——— Über die orthogonalen Funktionen. II (Summation) .... 18 (1957), 149—168
——— Über die orthogonalen Funktionen. III (Lebesguesche Funktionen) 18 (1957), 169—178
——— Über die orthogonalen Funktionen. IV .... 19 (1958), 18—25
——— Über die orthogonalen Funktionen. V (Genaue Weylsche Multiplikatorfolgen) .... 20 (1959), 1—13
——— Über die orthogonalen Funktionen. VI (Eine genaue Bedingung für die starke Summation) .... 20 (1959), 14—18
——— Über die orthogonalen Funktionen. VII (Approximationssätze).. 20 (1959), 19—24
——— Bemerkung zur Divergenz der trigonometrischen Reihen .... 20 (1959), 25—32
——— Über die orthogonalen Funktionen. VIII (Eine notwendige Bedingung für die Konvergenz) .... 20 (1959), 245—251
——— Bemerkung zu einem Satz von G. Alexits .... 21 (1960), 12—14
——— Ein Summationssatz für Orthogonalreihen mit monotoner Koeffizientenfolge .... 21 (1960), 15—18
——— Über die orthogonalen Funktionen. IX (Absolute Summation)... 21 (1960), 292—299
——— Bemerkung zu einem Satz von A. N. Kolmogoroff .... 22 (1961), 133—135
——— Über die orthogonalen Funktionen. X .... 23 (1962), 185—221
——— Über die Konvergenz der Orthogonalreihen .... 24 (1963), 139—151
——— Über die Konvergenz der Orthogonalreihen. II .... 25 (1964), 219—232
——— Über ein Problem von S. B. Stetschkin .... 26 (1965), 75—78
——— Bemerkung zur Konvergenz der Orthogonalreihen .... 26 (1965), 249—252
——— Über die Divergenz der Wahlshschen Reihen .... 27 (1966), 261—263
——— Ergänzung zu einem Satz von S. Kaczmarz .... 28 (1967), 147—156
——— Bemerkung zur Divergenz der Fourierreihen .... 28 (1967), 281—283
——— Berichtigung zur Arbeit „Über die starke Summation von Fourierreihen" .... 29 (1968), 351—352
——— Über die Reflexivität gewisser Banachräume .... 30 (1969), 39—42
——— Ein Divergenzsatz für Fourierreihen .... 30 (1969), 43—48
——— Über die unbedingte Konvergenz der Orthogonalreihen .... 32 (1971), 11—40
——— Über das Maximum der Summen orthogonaler Funktionen ..... 32 (1971), 317—326
——— Bemerkung über die Konvergenz der Orthogonalreihen .... 34 (1973), 393—399
——— Eine Abschätzung des Maximums der Partialsummen von Orthogonalreihen .... 36 (1974), 169—180
——— Bemerkungen zur Konvergenz der Reihen nach multiplikativen Funktionensystemen .... 38 (1976), 167—170
——— Einfacher Beweis eines Satzes von B. S. Kašin .... 39 (1977), 175—178
——— Bemerkung zu einem Satz von S. Kaczmarz .... 42 (1980), 171—173
——— Über einem Satz von Alexits und Sharma .... 42 (1980), 175—182
——— Beitrag zur Konvergenz der Orthogonalreihen .... 43 (1981), 127—130
——— Beitrag zu den Arbeiten „Bemerkung zu einem Satz von S. Kaczmarz" und „Über einen Satz von Alexits und Sharma" .... 44 (1982), 307—311

U

V

W

Д

К

Л

М

Х

Ч

OBITUARIES

86-2044 — Szegedi Nyomda — Felelős vezető: Surányi Tibor igazgató

INDEX

ACTA SCIENTIARUM MATHEMATICARUM

SZEGED (HUNGARIA), ARADI VÉRTANÚK TERE 1

On peut s'abonner à l'entreprise de commerce des livres et journaux „Kultúra" (1061 Budapest, I., Fő utca 32)

ISSN 0324-6523 Acta Univ. Szeged
ISSN 0001 6969 Acta Sci. Math.

INDEX: 26024

86-2044 — Szegedi Nyomda — F. v.: Surányi Tibor igazgató

Felelős szerkesztő és kiadó: Leindler László
A kézirat a nyomdába érkezett: 1986. április 29.
Megjelenés: 1987.

Példányszám: 1000. Terjedelem: 18,2 (A/5) ív
Készült monószedéssel, íves magasnyomással,
az MSZ 5601-24 és az MSZ 5602-55 szabvány szerint