ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA SCIENTIARUM MATHEMATICARUM

TOMUS 37
FASC. 1—2

SZEGED, 1975

INSTITUTUM BOLYAIANUM UNIVERSITATIS SZEGEDIENSIS

A JÓZSEF ATTILA TUDOMÁNYEGYETEM KÖZLEMÉNYEI

ACTA SCIENTIARUM MATHEMATICARUM

37. KÖTET
1—2. FÜZET

SZEGED, 1975

JÓZSEF ATTILA TUDOMÁNYEGYETEM BOLYAI INTÉZETE

ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA SCIENTIARUM MATHEMATICARUM

TOMUS 37

SZEGED, 1975

INSTITUTUM BOLYAIANUM UNIVERSITATIS SZEGEDIENSIS

A JÓZSEF ATTILA TUDOMÁNYEGYETEM KÖZLEMÉNYEI

ACTA SCIENTIARUM MATHEMATICARUM

37. KÖTET

SZEGED, 1975

JÓZSEF ATTILA TUDOMÁNYEGYETEM BOLYAI INTÉZETE

Varieties of affine modules

By B. CSÁKÁNY in Szeged

Let **R** be a ring with unit element. Any n-ary ($n>0$) polynomial $f=f(x_1, \ldots, x_n)$ of a unital right **R**-module **A** is of the form

$$x_1 \varrho_1 + \cdots + x_n \varrho_n \tag{1}$$

where $\varrho_i \in \mathbf{R}$ ($i=1, \ldots, n$). Denote by I the family of all polynomials of **A** satisfying $\sum_i \varrho_i = 1$. We can associate with **A** the algebra $\mathbf{A}^* = \langle A; I \rangle$ which will be called an *affine module over* **R**.

Affine modules were introduced by OSTERMANN and SCHMIDT in [9]; in the case when **R** is a field this notion coincides with that of the affine space over **R**, treated by MAC LANE and BIRKHOFF in [2]. In [6] GIVANT, characterizing varieties in which all algebras are free, announced that all affine spaces over a division ring (defined similarly) form such a variety.

In what follows we show that all affine modules over any ring with unit element form a variety and we give an abstract characterization (in terms of subalgebras and congruences) up to (rational) equivalence in MAL'CEV's sense (see [3], Chapter 9) for varieties of affine modules. Such varieties over commutative rings as well as over fields are also characterized. Finally, we show that any variety of affine modules determines its "ring of scalars" up to isomorphism.

The basic terminology we use is adopted from [1]. Note, however, that we will denote polynomial symbols and polynomials induced by them in the same way. Sometimes we write $(\varrho_1, \ldots, \varrho_n)$ instead of the polynomial f given by (1). The base sets of algebras **A**, **B**, ... will be denoted by A, B, ... All rings which occur in the following are supposed to have a unit element and all modules will be unital right modules. We shall denote the class of all **R**-modules by $\mathcal{M}(\mathbf{R})$, and the class of all affine modules over **R** by $\mathcal{A}(\mathbf{R})$. For any **R**-module **B** the associated affine module will always be denoted by $\mathbf{B}^*$.

Proposition. *For any ring* **R**, $\mathcal{A}(\mathbf{R})$ *is a variety.*

Proof. $\mathbf{S}(\mathscr{A}(\mathbf{R}))\subseteq\mathscr{A}(\mathbf{R})$. Let $\mathbf{A}$ be an $\mathbf{R}$-module, and suppose that $\mathbf{M}$ is a subalgebra of $\mathbf{A}^*$. Choose an $s\in M$. We show that $M_s=\{m-s\,|\,m\in M\}$ is the base set of a submodule $\mathbf{M}_s$ of $\mathbf{A}$, and $\mathbf{M}\cong\mathbf{M}_s^*\in\mathscr{A}(\mathbf{R})$. Indeed, if $a, b\in M$, $\varrho\in R$, then $(a-s)+(b-s)=(1, -1, 1)(a, s, b)-s\in M_s$ and $(a-s)\varrho=(\varrho, -\varrho, 1)(a, s, s)-s\in M_s$ hold. Further, let $m\varphi=m-s$ for any $m\in M$; then for arbitrary $\varrho_1, \dots, \varrho_n\in R$ (with sum 1) and $m_1, \dots, m_n\in M$ we have

$$(\varrho_1, \dots, \varrho_n)(m_1\varphi, \dots, m_n\varphi) = \sum_i \varrho_i m_i - \sum_i \varrho_i s = \sum_i \varrho_i m_i - s =$$

$$= ((\varrho_1, \dots, \varrho_n)(m_1, \dots, m_n))\varphi,$$

hence φ is an isomorphism of $\mathbf{M}$ onto $\mathbf{M}_s^*$.

$\mathbf{H}(\mathscr{A}(\mathbf{R}))\subseteq\mathscr{A}(\mathbf{R})$. If θ is a congruence relation (shortly: congruence) on $\mathbf{A}^*$, then θ is a congruence on $\mathbf{A}$, too: $a\equiv a_1$, $b\equiv b_1$ (θ) $(a, a_1, b, b_1\in A)$ imply $a+b= =(1, -1, 1)(a, 0, b)\equiv(1, -1, 1)(a_1, 0, b_1)=a_1+b_1(\theta)$ and $a\varrho=(\varrho, 1-\varrho)(a, 0)\equiv \equiv(\varrho, 1-\varrho)(a_1, 0)=a_1\varrho(\theta)$ for any $\varrho\in R$. Hence $\mathbf{A}^*/\theta\cong(\mathbf{A}/\theta)^*$ follows immediately.

$\mathbf{P}(\mathscr{A}(\mathbf{R}))\subseteq\mathscr{A}(\mathbf{R})$, since $\Pi(\mathbf{A}_j^*\,|\,j\in J)\cong(\Pi(\mathbf{A}_j\,|\,j\in J))^*$. This completes the proof.

Theorem 1. *A variety $\mathscr{R}$ is equivalent to $\mathscr{A}(\mathbf{R})$ for some ring $\mathbf{R}$ if and only if*

(∗) *in any algebra of $\mathscr{R}$ every subalgebra is a block of a unique congruence, and every block of any congruence is a subalgebra.*

Proof. Observe first, that condition (∗) means exactly that $\mathscr{R}$ is Hamiltonian (i.e., subalgebras are blocks of congruences; cf. [8]), idempotent (all operations are idempotent) and regular (see, e.g., [5]). Note that subalgebras and congruences are invariant under equivalence of varieties; hence to prove the necessity of condition (∗) it is enough to deal with the variety $\mathscr{A}(\mathbf{R})$ for an arbitrarily chosen ring $\mathbf{R}$.

Clearly, $\mathscr{A}(\mathbf{R})$ is idempotent. In order to show regularity we apply the characterization of regular varieties in [5]. As for the operation $(1, -1, 1)$, the identity $(1, -1, 1)(x, x, z)=z$ and the identical implication $(1, -1, 1)(x, y, z)=z\Rightarrow x=y$ are fulfilled, $\mathscr{A}(\mathbf{R})$ is regular. Finally, if $\mathbf{A}$ is an $\mathbf{R}$-module and $\mathbf{M}$ is a subalgebra of $\mathbf{A}^*$, then — as we have seen in the preceding proof — M is a block of a congruence of $\mathbf{A}$. By the definition of operations, all congruences of $\mathbf{A}$ are also congruences of $\mathbf{A}^*$. Thus M is a block of a congruence of $\mathbf{A}^*$; hence $\mathscr{A}(\mathbf{R})$ is Hamiltonian.

The proof of sufficiency needs the following lemma which is analogous to Lemma 2 in [4]:

Lemma 1. *Let $\mathscr{R}$ be a Hamiltonian, idempotent and regular variety. Suppose $\mathbf{A}\in\mathscr{R}$; let $\mathbf{B}$, $\mathbf{C}$ be subalgebras of $\mathbf{A}$ such that $B\cup C$ generates $\mathbf{A}$ and $B\cap C$ consists of a single element e. Then $\mathbf{A}\cong\mathbf{B}\times\mathbf{C}$ and there exists an isomorphism $\varphi\colon\mathbf{A}\to\mathbf{B}\times\mathbf{C}$ such that for any $b\in B$ and $c\in C$, $b\varphi=\langle b, e\rangle$ and $c\varphi=\langle e, c\rangle$ hold.*

Outline of proof. The Hamiltonian property and regularity of $\mathscr{R}$ imply that **B** and **C** determine uniquely the congruences β, resp. γ of **A**, for which they are blocks. For any $a \in A$ there exist a unique $b \in B$ and a unique $c \in C$ with $a \equiv b(\gamma)$ and $a \equiv c(\beta)$. The mapping φ defined by $a\varphi = (b, c)$ is the desired isomorphism of **A** onto $\mathbf{B} \times \mathbf{C}$. Details — *mutatis mutandis* — may be found in [4].

We prove the sufficiency by constructing a suitable ring **R** for any Hamiltonian, idempotent and regular variety $\mathscr{R}$ such that $\mathscr{A}(\mathbf{R})$ will be equivalent to $\mathscr{R}$. We establish the equivalence of these classes with the use of the following fact: varieties $\mathscr{K}$ and $\mathscr{L}$ are equivalent if and only if there exists a weak isomorphism (in the sense of Goetz [7]) between the countably generated free algebras of these classes, which induces a one-to-one correspondence between free generating sets. To make so, we need a further lemma.

Lemma 2. *Let* **R** *be an arbitrary ring. If* **F** *is a free algebra over* $\mathscr{M}(\mathbf{R})$ *with the free generating set X, then* $\mathbf{F}^*$ *is a free algebra over* $\mathscr{A}(\mathbf{R})$ *with the free generating set* $\{0\} \cup X$.

Proof. Suppose that in $\mathbf{F}^*$ the equality

$$(\varrho_1, \ldots, \varrho_m)(y_{i_1}, \ldots, y_{i_m}) = (\sigma_1, \ldots, \sigma_n)(y_{j_1}, \ldots, y_{j_n}) \tag{2}$$

holds, where $\varrho_k, \sigma_l \in R$, $\sum_k \varrho_k = \sum_l \sigma_l = 1$, and $y_{i_k}, y_{j_l} \in \{0\} \cup X$. We may assume that the y_{i_k} as well as the y_{j_l} are pairwise different. It is enough to prove that (2) holds identically in $\mathscr{A}(\mathbf{R})$.[1] If none of y_{i_k} and y_{j_l} equals $0 (\in F)$, then we may consider (2) as an equality in **F**, which holds identically in $\mathscr{M}(\mathbf{R})$, and hence in $\mathscr{A}(\mathbf{R})$, too.

Suppose now, e.g., $y_{i_1} = 0$. If none of y_{j_l} equals 0, then $y_{i_2}\varrho_2 + \cdots + y_{i_m}\varrho_m = y_{j_1}\sigma_1 + \cdots + y_{j_n}\sigma_n$ in **F**, and this equality holds identically in any **R**-module. Consider **R** as an **R**-module and substitute $1 (\in R)$ for each y_{i_k} and y_{j_l} in this equality. Then we get $\varrho_2 + \cdots + \varrho_m = \sigma_1 + \cdots + \sigma_n (= 1)$, whence $\varrho_1 = 0$. Hence it follows that (2) holds identically in $\mathscr{A}(\mathbf{R})$.

In the remainder case, let $y_{j_l} = 0$ for some l $(1 \leq l \leq n)$. Now the above consideration shows that $y_{i_2}\varrho_2 + \cdots + y_{i_m}\varrho_m = y_{j_1}\sigma_1 + \cdots + y_{j_{l-1}}\sigma_{l-1} + y_{j_{l+1}}\sigma_{l+1} + \cdots + y_{j_n}\sigma_n$ holds identically in any **R**-module and $\varrho_1 = \sigma_l$. Therefore, $a\varrho_1 + a_{i_2}\varrho_2 + \cdots + a_{i_m}\varrho_m = a_{j_1}\sigma_1 + \cdots + a_{j_{l-1}}\sigma_{l-1} + a\sigma_l + a_{j_{l+1}}\sigma_{l+1} + \cdots + a_{j_n}\sigma_n$ for arbitrary elements a, a_{i_k}, a_{j_l} (with $a_{i_k} = a_{j_l}$ whenever $y_{i_k} = y_{j_l}$) of any **R**-module. This means that (2) holds identically in $\mathscr{A}(\mathbf{R})$, completing the proof of Lemma 2.

Let $\mathbf{F}_{012}$ be a free algebra over a Hamiltonian, idempotent and regular variety $\mathscr{R}$ (which will be fixed in the sequel) with the free generating set $\{x_0, x_1, x_2\}$. Let $\mathbf{F}_{01}$ and $\mathbf{F}_{02}$ denote the subalgebras of $\mathbf{F}_{012}$ generated by $\{x_0, x_1\}$ and $\{x_0, x_2\}$, respec-

[1]) This means: "if in (2) we replace $y_{i_1}, \ldots, y_{j_n}$ by polynomial symbols $x_{i_1}, \ldots, x_{j_n}$ respectively, and polynomials by the associated polynomial symbols, then we get an identity in $\mathscr{A}(\mathbf{R})$".

tively. Then $\mathbf{F}_{01}\cup\mathbf{F}_{02}$ generates $\mathbf{F}_{012}$. On the other hand, $\mathbf{F}_{01}\cap\mathbf{F}_{02}=\{x_0\}$. Indeed, let $x\in\mathbf{F}_{01}\cap\mathbf{F}_{02}$; then there exist binary polynomials g and h over $\mathbf{F}_{012}$ such that $x=g(x_0, x_1)=h(x_0, x_2)$. The second equality holds identically in $\mathcal{R}$; hence, by idempotency, we have $x=g(x_0, x_1)=h(x_0, x_0)=x_0$. Thus, we can apply Lemma 1: $\mathbf{F}_{012}\cong\mathbf{F}_{01}\times\mathbf{F}_{02}$, and there exists an isomorphism φ such that for any binary polynomial k over $\mathbf{F}_{012}$ $\big(k(x_0, x_1)\big)\varphi=\langle k(x_0, x_1), x_0\rangle$ and $\big(k(x_0, x_2)\big)\varphi=\langle x_0, k(x_0, x_2)\rangle$.

We can find a ternary polynomial f over $\mathbf{F}_{012}$ such that $\big(f(x_0, x_1, x_2)\big)\varphi=\langle x_1, x_2\rangle$. Let $\mathbf{F}_\omega$ denote the free algebra over $\mathcal{R}$ with countable free generating set $\{x_0, x_1, \ldots\}$, and for any $x, y\in\mathbf{F}_\omega$, let $x+y=f(x_0, x, y)$. This binary algebraic function over $\mathbf{F}$ will be called addition. We show that $\langle F_\omega; +\rangle$ is an Abelian group.

First, $\langle x_1, x_2\rangle=\big(f(x_0, x_1, x_2)\big)\varphi=f(x_0\varphi, x_1\varphi, x_2\varphi)=f(\langle x_0, x_0\rangle), \langle x_1, x_0\rangle, \langle x_0, x_2\rangle)=$ $=\langle f(x_0, x_1, x_0), f(x_0, x_0, x_2)\rangle$. Hence $f(x, y, x)=f(x, x, y)=y$ is an identity in $\mathcal{R}$. Then for any $x\in\mathbf{F}_\omega$ we get $x+x_0=f(x_0, x, x_0)=x$, and similarly, $x_0+x=x$; i.e., x_0 is the zero element for the addition.

Let now $\mathbf{F}_{n0n}$ be a free algebra over $\mathcal{R}$ with free generating set $\{y_1, \ldots, y_n, x_0, x_1, \ldots, x_n\}$. Let $\mathbf{F}_{n0}$ and $\mathbf{F}_{0n}$ denote the subalgebras of $\mathbf{F}_{n0n}$ generated by $\{x_0, x_1, \ldots, x_n\}$ and $\{x_0, y_1, \ldots, y_n\}$, respectively. Lemma 1 applied to algebras $\mathbf{F}_{n0n}$, $\mathbf{F}_{n0}$ and $\mathbf{F}_{0n}$ furnishes the following fact: $\mathbf{F}_{n0n}\cong\mathbf{F}_{n0}\times\mathbf{F}_{0n}$ and there exists an isomorphism ψ such that for any $(n+1)$-ary polynomial l over $\mathbf{F}_{n0n}$ $\big(l(x_0, x_1, \ldots, x_n)\big)\psi=$ $=\langle l(x_0, x_1, \ldots, x_n), x_0\rangle$ and $\big(l(x_0, y_1, \ldots, y_n)\big)\psi=\langle x_0, l(x_0, y_1, \ldots, y_n)\rangle$ hold. This implies

$$p\big(f(x_0, x_1, y_1), \ldots, f(x_0, x_n, y_n)\big)=f\big(x_0, p(x_1, \ldots, x_n), p(y_1, \ldots, y_n)\big) \tag{3}$$

for any n-ary polynomial p over $\mathbf{F}_{n0n}$. Indeed,

$$\begin{aligned}
&p\big(f(x_0, x_1, y_1), \ldots, f(x_0, x_n, y_n)\big)=\\
&=\big(p(f(x_0\psi, x_1\psi, y_1\psi), \ldots, f(x_0\psi, x_n\psi, y_n\psi))\psi^{-1}=\\
&=\big(p(f(\langle x_0, x_0\rangle, \langle x_1, x_0\rangle, \langle x_0, y_1\rangle), \ldots, f(\langle x_0, x_0\rangle, \langle x_n, x_0\rangle, \langle x_0, y_n\rangle)\psi^{-1}=\\
&=\langle p\big(f(x_0, x_1, x_0), \ldots, f(x_0, x_n, x_0)\big), p\big(f(x_0, x_0, y_1), \ldots, f(x_0, x_0, y_n)\big)\rangle\psi^{-1}=\\
&=\langle p(x_1, \ldots, x_n), p(y_1, \ldots, y_n)\rangle\psi^{-1}=\\
&=\langle f\big(x_0, p(x_1, \ldots, x_n), x_0\big), f\big(x_0, x_0, p(y_1, \ldots, y_n)\big)\rangle\psi^{-1}=\\
&=\big(f(\langle x_0, x_0\rangle, \langle p(x_1, \ldots, x_n), x_0\rangle, \langle x_0, p(y_1, \ldots, y_n)\rangle)\big)\psi^{-1}=\\
&=\big(f(x_0\psi, (p(x_1, \ldots, x_n))\psi, (p(y_1, \ldots, y_n))\psi)\big)\psi^{-1}=\\
&=f\big(x_0, p(x_1, \ldots, x_n), p(y_1, \ldots, y_n)\big).
\end{aligned}$$

Since (3) holds identically in $\mathcal{R}$, for $p=f$ and for any $x, y, z\in\mathbf{F}_\omega$ we get

$$\begin{aligned}
x+(y+z)&=f\big(f(x_0, x_0, x_0), f(x_0, x, x_0), f(x_0, y, z)\big)=\\
&=f\big(x_0, f(x_0, x, y), f(x_0, x_0, z)\big)=(x+y)+z,
\end{aligned}$$

i.e. the addition is associative. Commutativity of addition may be checked analogously. Finally, again by (3),

$$x+f(x, x_0, x_0) = f(x_0, f(x_0, x, x_0), f(x, x_0, x_0)) =$$
$$= f(f(x_0, x_0, x), f(x_0, x, x_0), f(x_0, x_0, x_0)) = f(x, x, x_0) = x_0,$$

showing that $f(x, x_0, x_0)$ is the additive inverse of x in $\mathbf{F}_\omega$.

Let us consider the set R of all unary algebraic functions over $\mathbf{F}_\omega$ which involve no constants unless x_0. For each such function τ there exists a binary polynomial t over $\mathbf{F}_\omega$ such that $x\tau = t(x_0, x)$ for any $x \in \mathbf{F}_\omega$. We define addition and multiplication on R as follows:

$$x(\tau_1+\tau_2) = x\tau_1 + x\tau_2, \quad x(\tau_1\tau_2) = (x\tau_1)\tau_2.$$

It may be seen immediately that R is closed under these operations; furthermore, addition is associative, commutative and invertible (namely, $x(-\tau) = f(t(x_0, x), x_0, x_0)$), while multiplication is associative, left distributive and has a unit element (namely, the identical function). Right distributivity follows from (3):

$$x((\tau_1+\tau_2)\tau_3) = (x\tau_1+x\tau_2)\tau_3 = t_3(x_0, f(x_0, t_1(x_0, x), t_2(x_0, x))) =$$
$$= f(x_0, t_3(x_0, t_1(x_0, x)), t_3(x_0, t_2(x_0, x))) = (x\tau_1)\tau_3 + (x\tau_2)\tau_3 = x(\tau_1\tau_3+\tau_2\tau_3).$$

Thus, $\mathbf{R} = \langle R; +, \cdot \rangle$ is a ring with unit element. Let $\bar{R} = \{\bar{\varrho} \mid \varrho \in R\}$, and $\bar{\mathbf{R}} = \langle \bar{R}; +, \cdot \rangle$ a ring isomorphic to $\mathbf{R}$ under the one-to-one correspondence $\bar{\varrho} \leftrightarrow \varrho$.

To get the desired equivalence we show the existence of a weak isomorphism χ of the free affine module $\mathbf{G}$ over $\bar{\mathbf{R}}$ with countable generating set onto $\mathbf{F}_\omega$ which maps the free generating set of $\mathbf{G}$ onto that of $\mathbf{F}_\omega$. By Lemma 2, $\mathbf{G}$ may be given in the form $\mathbf{G} = \mathbf{F}^*$, where $\mathbf{F}$ is the free $\bar{\mathbf{R}}$-module with countable free generating set $\{x_1, x_2, \ldots\}$, and the free generators of $\mathbf{F}^*$ are $\{0, x_1, x_2, \ldots\}$; then each element of G can be written in the form $x_{i_1}\bar{\varrho}_1 + \cdots + x_{i_m}\bar{\varrho}_m$, where $\bar{\varrho}_1, \ldots, \bar{\varrho}_m$ are non-zero elements of $\bar{\mathbf{R}}$, and this representation is unique (empty sum is allowed).

Define now χ by $(x_{i_1}\bar{\varrho}_1 + \cdots + x_{i_m}\bar{\varrho}_m)\chi = x_{i_1}\varrho_1 + \cdots + x_{i_m}\varrho_m$ (at the right hand side, x_{i_k} are free generators of $\mathbf{F}_\omega$, addition and "scalars" are the above-defined algebraic functions on $\mathbf{F}_\omega$). Furthermore, let $0\chi = x_0$. Then χ maps the free generating set of $\mathbf{G}$ onto that of $\mathbf{F}_\omega$. Observe that χ is one-to-one; indeed, if

$$x_{i_1}\varrho_1 + \cdots + x_{i_m}\varrho_m = x_{j_1}\sigma_1 + \cdots + x_{j_n}\sigma_n \tag{4}$$

holds in $\mathbf{F}_\omega$, then (4) (which is a short form for the equality of two elements of $\mathbf{F}_\omega$, whose full expression involves the polynomials $f, r_1, \ldots, r_m, s_1, \ldots, s_n$ and the free generators $x_0, x_{i_1}, \ldots, x_{i_m}, x_{j_1}, \ldots, x_{j_n}$) holds identically in $\mathscr{R}$. Replace all x_{i_k} and x_{j_l}, except x_{i_1} by x_0; then, using idempotency of all r_k and s_l we get $r_1(x_0, x_{i_1}) = x_0$ unless $x_{i_1} = x_{j_l}$ for some l. But $r_1(x_0, x_{i_1}) = x_0$ holds also identically in $\mathscr{R}$, whence it follows $\varrho_1 = 0$ in $\mathbf{R}$, a contradiction. Thus we conclude that $x_{i_1} = x_{j_l}$ and $r_1(x_0, x_{i_1}) =$

$=s_l(x_0, x_{j_l})=s_l(x_0, x_{i_1})$, whence $\varrho_1=\sigma_l$ in **R**. Now a trivial induction shows that the two sides of (4) are the same.

To prove that χ is onto we use (3) in the form $p((x_1+y_1), \dots, (x_n+y_n))= =p(x_1, \dots, x_n)+p(y_1, \dots, y_n)$ (i.e., addition in $\mathbf{F}_\omega$ commutes with all polynomials). Any element of $\mathbf{F}_\omega$ can be written in the form $p(x_0, \dots, x_t)$; but

$$p(x_0, \dots, x_t) = p(x_0+x_0+\dots+x_0, x_0+x_1+x_0+\dots+x_0, \dots, x_0+\dots+x_0+x_t) =$$
$$= p(x_0, x_0, \dots, x_0)+p(x_0, x_1, x_0, \dots, x_0)+\dots+p(x_0, \dots, x_0, x_t).$$

For any i $(1\leqq i\leqq t)$ there exists a binary polynomial p_i such that

$$p(x_0, \dots, x_0, x_i, x_0, \dots, x_0) = p_i(x_0, x_i).$$

Hence

$$p(x_0, \dots, x_t) = p_1(x_0, x_1)+\dots+p_t(x_0, x_t) = x_1\pi_1+\dots+x_t\pi_t = (x_1\bar{\pi}_1+\dots+x_t\bar{\pi}_t)\chi,$$

where the unary algebraic functions π_i in **R** are defined by $x\pi_i=p_i(x_0, x)$.

To complete the proof, we need a one-to-one correspondence ζ between all polynomials **G** and $\mathbf{F}_\omega$ with the property that for any n-ary polynomial q of **G** and for arbitrary $y_1, \dots, y_n\in G$ the equality

$$(5)\qquad (q(y_1, \dots, y_n))\chi = (q\zeta)(y_1\chi, \dots, y_n\chi)$$

holds. Since polynomials of **G** are the same as (fundamental) operations, every polynomial of **G** is of the form $(\bar{\varrho}_1, \dots, \bar{\varrho}_n)$, where $\bar{\varrho}_1, \dots, \bar{\varrho}_n\in\bar{R}$, $\sum_i\bar{\varrho}_i=1$. Let $((\bar{\varrho}_1, \dots, \bar{\varrho}_n)\zeta)(z_1, \dots, z_n)=z_1\varrho_1+\dots+z_n\varrho_n$. There is an n-ary algebraic function of $\mathbf{F}_\omega$ on the right side; we show that in fact it is a polynomial. Since $\mathscr{R}$ is Hamiltonian, the subalgebra **H** of $\mathbf{F}_\omega$ generated by $\{x_1, \dots, x_n\}$ is a block for some congruence θ of $\mathbf{F}_\omega$. Then $x_1\varrho_1+\dots+x_n\varrho_n\equiv x_1\varrho_1+\dots+x_1\varrho_n=x_1(\theta)$, whence $x_1\varrho_1+\dots+x_n\varrho_n\in\mathbf{H}$. Thus, there exists an n-ary polynomial r of $\mathbf{F}_\omega$ such that $x_1\varrho_1+\dots+x_n\varrho_n=r(x_1, \dots, x_n)$. Hence $z_1\varrho_1+\dots+z_n\varrho_n=r(z_1, \dots, z_n)$ follows for any $z_1, \dots, z_n\in F_\omega$.

To show that ζ is onto and one-to-one we may proceed similarly as in the case of χ, but we must take into consideration that now the ϱ_i may equal 0. Finally we prove (5) for $q=(\bar{\varrho}_1, \dots, \bar{\varrho}_n)$ and arbitrary elements $y_i=x_1\bar{\tau}_{i1}+\dots+x_t\bar{\tau}_{it}$ $(i=1, \dots, n)$ of **G**. We have

$$(q(y_1, \dots, y_n))\chi = (x_1(\bar{\tau}_{11}\bar{\varrho}_1+\dots+\bar{\tau}_{n1}\bar{\varrho}_n)+\dots+x_t(\bar{\tau}_{1t}\bar{\varrho}_1+\dots+\bar{\tau}_{nt}\bar{\varrho}_n))\chi =$$
$$= x_1(\tau_{11}\varrho_1+\dots+\tau_{n1}\varrho_n)+\dots+x_t(\tau_{n1}\varrho_1+\dots+\tau_{nt}\varrho_n) =$$
$$= (x_1\tau_{11}+\dots+x_t\tau_{1t})\varrho_1+\dots+(x_1\tau_{n1}+\dots+x_t\tau_{nt})\varrho_n = (q\zeta)(y_1\chi, \dots, y_n\chi),$$

which was needed.

Call a variety $\mathscr{A}$ Abelian if in all algebras of $\mathscr{A}$ any two operations commute (i.e., for any m-ary g and n-ary h,

$$g(h(x_{11}, \dots, x_{1n}), \dots, h(x_{m1}, \dots, x_{mn})) = h(g(x_{11}, \dots, x_{m1}), \dots, (x_{1n}, \dots, x_{mn}))$$

is an identity in $\mathscr{A}$).

Theorem 2. *A variety $\mathscr{R}$ is equivalent to $\mathscr{A}(\mathbf{R})$ for some commutative ring* $\mathbf{R}$ *if and only if $\mathscr{R}$ is Abelian and satisfies condition* $(*)$.

Proof. On the base of Theorem 1, necessity is obvious from the description of operations on affine modules and the definition of Abelian varieties. Let now $\mathscr{R}$ be an Abelian variety satisfying $(*)$. With notations used in the proof of Theorem 1, we have to show that the ring $\mathbf{R}$ of all unary algebraic functions on $\mathbf{F}_\omega$ involving no other constants than x_0, is commutative. Let $\varrho_1, \varrho_2 \in \mathbf{R}$; then for any $x \in F_\omega$,

$$x(\varrho_1\varrho_2) = r_2(x_0, r_1(x_0, x)) = r_2(r_1(x_0, x_0), r_1(x_0, x)) =$$

$$= r_1(r_2(x_0, x_0), r_2(x_0, x)) = r_1(x_0, r_2(x, x)) = x(\varrho_2\varrho_1),$$

i.e., $\varrho_1\varrho_2 = \varrho_2\varrho_1$.

Theorem 3. *A variety $\mathscr{R}$ is equivalent to the variety of all affine modules (=affine spaces) over a field if and only if $\mathscr{R}$ is Abelian, equationally complete and satisfies condition* $(*)$.

Proof. In view of the preceding theorems, necessity is implied by Givant's result mentioned in the introduction. Let now $\mathscr{R}$ be an equationally complete Abelian variety satisfying $(*)$. It is enough to show that the function ring $\mathbf{R}$ is simple. In other words, we need the following fact: if a commutative ring with unit element, say $\mathbf{P}$, has a proper ideal $\mathbf{J}$, then the variety $\mathscr{P}$ of all affine modules over $\mathbf{P}$ has a proper (non-trivial) subvariety.

We may assume that $\mathbf{P}/\mathbf{J}$ is not isomorphic to $\mathbf{P}$. Let $\tilde{\pi}$ denote that block of the congruence determined by $\mathbf{J}$ which contains $\pi(\in P)$. With any affine module over $\mathbf{P}/\mathbf{J}$ we can associate an affine module over $\mathbf{P}$ with the same base set by defining the operations as follows: $(\pi_1, \ldots, \pi_k)(y_1, \ldots, y_k) = (\tilde{\pi}_1, \ldots, \tilde{\pi}_k)(y_1, \ldots, y_k)$. Applying the closure operators **S**, **H** and **P**, one can easily check that the affine modules over $\mathbf{P}$ obtained by such a way form a subvariety $\mathscr{P}'$ of $\mathscr{P}$. Moreover, $\mathscr{P}'$ is equivalent to the variety of all affine modules over $\mathbf{P}/\mathbf{J}$, whence, especially, follows that $\mathscr{P}'$ is non-trivial. Finally, $\mathscr{P} = \mathscr{P}'$ implies that the variety of all affine modules over $\mathbf{P}$ is equivalent to the variety of all affine modules over $\mathbf{P}/\mathbf{J}$. The following theorem shows that this is not the case, and thus $\mathscr{P}'$ is a proper subvariety of $\mathscr{P}$, qu.e.d.

Theorem 4. *If, for any rings $\mathbf{R}_1$ and $\mathbf{R}_2$, $\mathscr{A}(\mathbf{R}_1)$ and $\mathscr{A}(\mathbf{R}_2)$ are equivalent, then $\mathbf{R}_1$ and $\mathbf{R}_2$ are isomorphic.*

Proof. For $i=1, 2$; $\mathbf{R}_i$ when considered as an $\mathbf{R}_i$-module is a free $\mathbf{R}$-module with the free generator 1. Lemma 2 implies that $\mathbf{R}_i^*$ — as an affine module over $\mathbf{R}_i$ — is free in $\mathscr{A}(\mathbf{R}_i)$ with the free generating set $\{0, 1\}$. As $\mathscr{A}(\mathbf{R}_1)$ is equivalent to $\mathscr{A}(\mathbf{R}_2)$ there exists a weak isomorphism χ of $\mathbf{R}_1^*$ onto $\mathbf{R}_2^*$ such that $0\chi=0$, $1\chi=1$, with correspondence of polynomials ζ. Let, especially, $(\varrho, 1-\varrho)\zeta = (\varrho', 1-\varrho')$ for any binary polynomial $(\varrho, 1-\varrho)$ of $\mathbf{R}_1^*$. Define the mapping $\varphi: R_1 \to R_2$ by $\varrho\varphi = \varrho'$. Since ζ is one-to-one and onto, the same is valid for φ. We show that φ is an isomorphism of $\mathbf{R}_1$ onto $\mathbf{R}_2$; for this aim, it suffices to show that φ is homomorphic.

First we prove

$$(1, -1, 1)\zeta = (1, -1, 1). \tag{6}$$

Let $(1, -1, 1)\zeta = (\alpha, \beta, \gamma)$; then using (5) for $q=(1, -1, 1)$ and $y_1=1$, $y_2=y_3=0$, we obtain $\alpha=1$. Similarly we get $\beta=-1$, $\gamma=1$.

Now from (5) and (6) it follows

$$(x+y)' = \big((x+y)', 1-(x+y)'\big)(1, 0) = \big((x+y, 1-(x+y))(1, 0)\big)\chi =$$
$$= \big((1, -1, 1)((x, 1-x)(1, 0), 0, (y, 1-y)(1, 0))\big)\chi =$$
$$= (1, -1, 1)\big(((x, 1-x)(1, 0))\chi, 0\chi, ((y, 1-y)(1, 0))\chi\big) =$$
$$= (1, -1, 1)\big((x', 1-x')(1, 0), 0, (y', 1-y')(1, 0)\big) = x'+y'.$$

Finally, for any $x, y \in R_1$ we have $(xy)\chi = \big(xy + 0(1-y)\big)\chi = (y', 1-y')(x\chi, 0) = (x\chi)y'$, whence

$$(xy)' = (1\chi)(xy)' = (1xy)\chi = (1x)\chi \cdot y = (1\chi)x'y' = x'y',$$

completing the proof.

Note that the proof of theorem 3 indicates also the following result: A variety of form $\mathscr{A}(\mathbf{R})$ is equationally complete if and only if $\mathbf{R}$ is a simple ring.

References

[1] G. Grätzer, *Universal Algebra,* Van Nostrand (1968).

[2] S. Mac Lane—G. Birkhoff, *Algebra,* Macmillan (1967).

[3] A. I. Mal'cev, *The matemathematics of algebraic systems,* North-Holland (1971).

[4] B. Csákány, On the equivalence of certain classes of algebraic systems, *Acta Sci. Math.,* **23** (1962), 46—57.

[5] B. Csákány, Characterizations of regular varieties, *Acta Sci. Math.,* **31** (1970), 187—189.

[6] S. R. Givant, A representation theorem for universal classes of algebras in which all member are free, *Notices AMS,* **19**: 7 (1972), A—767.

[7] A. Goetz, On weak isomorphisms and weak homomorphisms of abstract algebras, *Coll. Math.,* **14** (1966), 163—167.

[8] L. Klukovits, Hamiltonian varieties of universal algebras, *Acta Sci. Math.,* **37** (1975), 11—15.

[9] F. Ostermann—J. Schmidt, Der baryzentrische Kalkül als axiomatische Grundlage der affinen Geometrie, *J. reine angew. Math.,* **224** (1966), 44—57.

(Received May 18, 1973)

Hamiltonian varieties of universal algebras

By L. KLUKOVITS in Szeged

A group is called Hamiltonian if its every subgroup is normal. Generalizing this notion, T. EVANS [4] introduced the Hamiltonian property of loops. He called a loop **A** Hamiltonian if its every subloop is a block of certain congruence of **A**, and proved that a variety of loops is Hamiltonian (i.e., every loop is Hamiltonian in the variety) if and only if it is a variety of Abelian groups. In this paper we shall study a natural generalization of this notion for universal algebras and describe the Hamiltonian varieties of universal algebras. Our way is independent of that of Evans and furnishes, among others, a new proof of his result, too.

Definition. A universal algebra (shortly: algebra) $\langle A; \Omega \rangle$ is called *Hamiltonian* if its every subalgebra is a block of some congruence of $\langle A; \Omega \rangle$. A variety of algebras is called Hamiltonian if every algebra is Hamiltonian in it.

This condition was applied in some earlier papers of K. SHODA [6] and B. CSÁKÁNY [3].

We shall often use the following lemma which is a special case of a theorem of MAL'CEV ([5] Theorem 5).

Lemma. *Let $\langle A; \Omega \rangle$ be an algebra and B a subset of A. The subset B is a block of some congruence of $\langle A; \Omega \rangle$ if and only if for any translation τ of* **A** *either $B\tau \subseteq B$ or $B\tau \cap B = \emptyset$ ($B\tau$ is the image of B under the mapping τ).*

The Hamiltonian varieties are characterized by the following

Theorem 1. *A variety of algebras $\mathfrak{A}$ is Hamiltonian if and only if for any n-ary polynomial symbol g there exists a ternary polynomial symbol k_g such that the identity*

$$(*) \qquad g(x_1, x_2, \ldots, x_n) = k_g(x_0, g(x_0, x_2, \ldots, x_n), x_1)$$

holds in $\mathfrak{A}$.

Proof. Let the variety $\mathfrak{A}$ be Hamiltonian and consider the free algebra $\mathbf{F}(\in\mathfrak{A})$ generated by the set $\{x_0, x_1, \ldots, x_n\}$. For any n-ary polynomial symbol g, the mapping $\tau: y \to g(y, x_2, \ldots, x_n)$ $(y \in F)$ is a translation of $\mathbf{F}$. Consider the subalgebra $\mathbf{A}$ of $\mathbf{F}$ generated by the set $\{x_0, g(x_0, x_2, \ldots, x_n), x_1\}$. Since $x_0\tau \in A$, by the lemma, we have $x_1\tau \in A$. Thus there exists a ternary polynomial symbol k_g such that the equality

$$x_1\tau = g(x_1, x_2, \ldots, x_n) = k_g\big(x_0, g(x_0, x_2, \ldots, x_n), x_1\big)$$

holds. Since $\mathbf{F}$ is a free algebra of the variety $\mathfrak{A}$ this equality is an identity in $\mathfrak{A}$.

Now, we suppose that for every n-ary polynomial symbol g of the variety $\mathfrak{A}$ there exists a ternary polynomial symbol k_g of $\mathfrak{A}$ satisfying the identity $(*)$. Let $\mathbf{D}(\in\mathfrak{A})$ be any algebra and $\mathbf{A}$ a subalgebra of $\mathbf{D}$. Consider a translation τ of $\mathbf{D}$ such that $a\tau \in A$ for some $a \in A$. This translation can be given by a polynomial symbol $g(x_1, x_2, \ldots, x_n)$: $a\tau = g(a, d_2, \ldots, d_n)$ where $d_2, \ldots, d_n \in D$. Then, using $(*)$, for any element $b(\in A)$ we have

$$b\tau = g(b, d_2, \ldots, d_n) = k_g\big(a, g(a, d_2, \ldots, d_n), b\big)$$

and therefore $b\tau \in A$. By the lemma, the proof is complete.

In theorems 2—5 we establish some basic properties of Hamiltonian algebras.

Theorem 2. *For any algebra* $\mathbf{A}$ *the following two conditions are equivalent:*

(i) $\mathbf{A}$ *is Hamiltonian,*

(ii) *any subalgebra of* $\mathbf{A}$ *generated by three elements is a block of some congruence of* $\mathbf{A}$.

Proof. Since (i)$\Rightarrow$(ii) is obvious it is enough to prove that (ii)$\Rightarrow$(i). Suppose that every subalgebra of $\mathbf{A}$ generated by three elements is a block of certain congruence of $\mathbf{A}$ but $\mathbf{A}$ has such subalgebra $\mathbf{A}_1$ which is not a block of any congruence of $\mathbf{A}$. Thus, by the lemma, there are elements a_1, a_2, a_3 in A and $\mathbf{A}$ has a translation τ such that $a_1\tau = a_2$ and $a_3\tau \notin A_1$. Now the subalgebra of $\mathbf{A}$ generated by the set of three elements $\{a_1, a_2, a_3\}$ is not a block of any congruence in view of the lemma and we have got a contradiction, which completes the proof.

Theorem 3. *The Hamiltonian property is local.*

Proof. We shall show if an algebra $\mathbf{A}$ is not Hamiltonian then it has a finitely generated subalgebra which is not Hamiltonian.

Let $\mathbf{A}$ be any algebra and $\mathbf{A}_1$ a subalgebra of $\mathbf{A}$ which is not a block of any congruence of $\mathbf{A}$. Now, by the lemma, $\mathbf{A}$ has a translation τ $\big(a\tau = g(a, a_2, \ldots, a_n)$ for every $a \in A\big)$ and A_1 has elements b, c, d such that

$$b\tau = c \quad \text{and} \quad d\tau \notin A_1.$$

Consider the subalgebra $\mathbf{A}_2$ of $\mathbf{A}$ generated by the finite set $\{b, c, d, a_2, \ldots, a_n\}$. The algebra $\mathbf{A}_1 \cap \mathbf{A}_2$ is such a subalgebra of $\mathbf{A}_2$ which is not a block of any congruence of $\mathbf{A}_2$ (τ is a translation of $\mathbf{A}_2$, too). The proof is complete.

The reader can prove in a routine way the next

Theorem 4. *Any homomorphic image and any subalgebra of a Hamiltonian algebra is Hamiltonian, too.*

In view of Birkhoff's characterization of varieties, by Theorems 3 and 4 the following question is raised: does the class of all Hamiltonian algebras of the same type form a variety? The answer is in the negative. Indeed, the Cartesian square of the quaternion group is not Hamiltonian.

Theorem 5. *In any category of Hamiltonian algebras the epimorphisms are surjections.*

Proof. Let $\mathbf{A}$ and $\mathbf{B}$ be Hamiltonian algebras. Suppose that the epimorphism $\varepsilon: \mathbf{A} \to \mathbf{B}$ is not surjective. Then $\mathbf{B}$ has a proper subalgebra $\mathbf{C}$ which is the image of $\mathbf{A}$ under the epimorphism ε. Since $\mathbf{B}$ is Hamiltonian, it has a congruence θ_c such that C is a block of θ_c. Consider the following homomorphisms α_1, α_2 from $\mathbf{B}$ into $\mathbf{B}/\theta_c$:

$$b\alpha_1 = [b]\theta_c, \quad b\alpha_2 = C$$

for all $b \in B$. Now, it is clear that $\varepsilon\alpha_1 = \varepsilon\alpha_2$. But $\alpha_1 \neq \alpha_2$ which is a contradiction.

Theorem 6. (T. EVANS [4].) *A variety $\mathfrak{A}$ of loops is Hamiltonian if and only if it is a variety of Abelian groups.*

Proof. Let the variety $\mathfrak{A}$ of loops be Hamiltonian. Then $\mathfrak{A}$ is (polynomially) equivalent to a variety $\mathfrak{R}$ of all unital right $\mathbf{R}$-modules over a ring $\mathbf{R}$ with identity element (see [3], Theorem 4). Every operation of $\mathfrak{R}$ can be written as a sum of unary operations [2] and therefore we have the identity

$$(*) \qquad x \circ y = x\alpha + y\beta$$

where "$\circ$" is the operation of the loop and $\alpha, \beta \in R$. Under this equivalence the identity element e of the loop corresponds to the zero element of $\mathbf{R}$. Substituting $x = e$ and $y = e$ respectively we have got $\alpha = \beta = 1$ (the identity element of $\mathbf{R}$). Thus the operation of the loop is associative and commutative.

In an earlier paper [7] we studied the Abelian property of universal algebras. We called the algebra $\langle A; \Omega \rangle$ Abelian, if for any operations μ and ν (m- and n-ary, erespctively) and any matrix $(a_{ij})_{nxm}$ over A the equality

$$(a_{11} \ldots a_{1m}\mu) \ldots (a_{n1} \ldots a_{nm}\mu)\nu = (a_{11} \ldots a_{n1}\nu) \ldots (a_{1m} \ldots a_{nm}\nu)\mu$$

holds. It is easy to verify that for varieties of loops, rings and lattices the Abelian and the Hamiltonian properties coincide, i.e., if a variety of loops (rings, lattices) is Hamiltonian then it is Abelian, and conversely. Therefore, a natural question can be raised: do the two properties coincide at any variety? The answer is in the negative. We can find a counter example among the varieties of unital semimodules over a semiring [2].

Theorem 7. *The variety $\mathfrak{R}$ of all unital right semimodules over a semiring* **R** *with identity element is Hamiltonian if and only if* **R** *is a ring.*

Proof. Let $\mathbf{F}\in\mathfrak{R}$ be a free algebra with the set of free generators $\{x_0, x_1, \dots, x_n\}$. Any polynomial symbol $g(x_1, x_2, \dots, x_n)$ of $\mathfrak{R}$ can be written in the form

$$g(x_1, \dots, x_n) = x_1\gamma_1 + \dots + x_n\gamma_n$$

where $\gamma_1, \dots, \gamma_n \in R$. If $\mathfrak{R}$ is Hamiltonian we have, by Theorem 1, ternary polynomial symbol $k_g(x, y, z) = x\varkappa_1 + y\varkappa_2 + z\varkappa_3$ such that in **F** the equality

$$x_1\gamma_1 + x_2\gamma_2 + \dots + x_n\gamma_n = x_0\varkappa_1 + (x_0\gamma_1 + x_2\gamma_2 + \dots + x_n\gamma_n)\varkappa_2 + x_1\varkappa_3$$

holds. Since **F** is a free algebra in $\mathfrak{R}$ this equality is an identity in $\mathfrak{R}$ and we have the following set of equations

$$(*) \qquad \varkappa_1 + \gamma_1\varkappa_2 = 0, \quad \varkappa_3 = \gamma_1, \quad \gamma_i\varkappa_2 = \gamma_i \quad (i = 2, 3, \dots, n).$$

This set of equations has to be valid for any polynomial symbol g with suitable $\varkappa_1$, $\varkappa_2$ and $\varkappa_3$. If $\gamma_i = 1$ for $i = 1, \dots, n$ we have got from $(*)$ that $\varkappa_2 = \varkappa_3 = 1$ and $\varkappa_1 + \varkappa_2 = 0$, hence it follows $\varkappa_1 = -1$, therefore **R** is a ring.

On the other hand, if **R** is a ring then the set of equations $(*)$ can be solved at any γ_i $(i = 1, \dots, n)$. Indeed, $\varkappa_1 = -\gamma_1$, $\varkappa_2 = 1$ and $\varkappa_3 = \gamma_1$ are solutions.

Theorem 8. *The variety $\mathfrak{R}$ of all unital right semimodules over a semiring* **R** *with identity element is Abelian if and only if* **R** *is a commutative semiring.*

Proof. Let the variety $\mathfrak{R}$ be Abelian and consider the following operation "$\circ$" of $\mathfrak{R}$:

$$x_1 \circ x_2 = x_1\alpha + x_2\beta,$$

where $\alpha, \beta \in R$. Since the semiring **R** under its own addition and right multiplication is a unital **R**-semimodule in $\mathfrak{R}$, by the definition of the Abelian property, we have $\alpha\beta = \beta\alpha$, using the matrix

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Such operations can be constructed by any elements α, β of R and thus we have proved that the multiplication in $\mathbf{R}$ is commutative.

The sufficiency is obvious.

Since the classes of rings and commutative semirings do not contain each other there exist Abelian and non Hamiltonian varieties and conversely.

The author expresses his thanks to B. CSÁKÁNY for his valuable suggestions during the elaboration of this theme.

References

[1] G. GRÄTZER, *Universal Algebra*, Van Nostrand (1968).
[2] B. CSÁKÁNY, Primitive classes of algebras which are equivalent to classes of semimodules and modules, *Acta Sci. Math.*, **24** (1963), 157—164. (Russian).
[3] B. CSÁKÁNY, Abelian properties of primitive classes of universal algebras, *Acta Sci. Math.*, **25** (1964), 202—208. (Russian).
[4] T. EVANS, Properties of algebras almost equivalent to identities, *J. London Math. Soc.*, **35** (1962), 53—59.
[5] A. I. MAL'CEV, On the general theory of algebraic systems, *Mat. Sbornik* (N. S.), **35** (77) (1954), 3—20. (Russian).
[6] K. SHODA, Zur Theorie der algebraischen Erweiterungen, *Osaka Math. J.*, **4** (1952), 133—143.
[7] L. KLUKOVITS, On commutative universal algebras, *Acta Sci. Math.*, **34** (1973), 171—174.

(Received June 4, 1973)

Varieties of idempotent medial quasigroups

By B. CSÁKÁNY and L. MEGYESI in Szeged

Quasigroups are algebras with three binary operations $\cdot$, $/$, and $\backslash$, called multiplication, right, and left division, respectively, which are connected by the identities

(1) $$xy/y = y\backslash yx = (x/y)y = y(y\backslash x) = x.$$

A quasigroup **Q** is *idempotent* if its multiplication is idempotent. **Q** is called *medial* if, for the multiplication, the identity

(2) $$(xy)(uv) = (xu)(yv)$$

holds. These two conditions — separately as well as jointly — were studied by several authors; see, e.g., STEIN [11] and BELOUSOV [2], [3].

In what follows we apply the results of the preceding paper [7] to characterize varieties of idempotent medial quasigroups, especially the variety of all such quasigroups and equationally complete varieties of them as well. The considerations we made are closely related with the recent investigations of MITSCHKE and WERNER [10]; as a matter of fact, the groupoids involved in [10] are equivalent to special idempotent medial quasigroups.

We will use the conventions of [7] without further references. We write abc instead of $(ab)c$; more generally, the absence of parentheses in any product indicates that multiplication must be performed from left to right even in the case when exponents occur; e.g., $a(bc^2)d$ denotes $\big(a((bc)c)\big)d$. Let **P** denote the ring of all rational functions of form $\frac{f(x)}{x^k(1-x)^l}$, where $f(x)\in\mathbf{Z}[x]$ and k, l are non-negative integers.

Theorem 1. *The variety $\mathcal{P}$ of all idempotent medial quasigroups is equivalent to the variety of all affine modules over* **P**. *Any variety $\mathcal{R}$ of idempotent medial quasigroups is equivalent to the variety of all affine modules over some homomorphic image of* **P**.

Proof. To prove that $\mathcal{R}$ is equivalent to $\mathcal{A}(\mathbf{R})$ for *some* commutative ring $\mathbf{R}$, it is enough to show that $\mathcal{R}$ is regular, idempotent, Abelian and Hamiltonian. Indeed, in this case $\mathcal{R}$ satisfies the conditions of Theorem 2 in [7].

Any variety of quasigroups is regular [6]. As Stein observed [11], in any quasigroup the idempotency of multiplication implies the idempotency of both divisions; hence $\mathcal{R}$ is idempotent. Again by [11], from mediality of multiplication follows the mediality of divisions, and so each fundamental operation in $\mathcal{R}$ commutes with itself; in order to prove that $\mathcal{R}$ is Abelian it remains to show that they commute with each other. Using (1) and (2) we obtain

$$x/y\cdot u/v = (x/y\cdot u/v)(yv)/yv = xu/yv,$$

and similarly we get the other two desired identities.

Let $\mathbf{Q}\in\mathcal{R}$ and consider an arbitrary subquasigroup $\mathbf{A}$ of $\mathbf{Q}$. Then the distinct sets of form $Aq=\{aq\,|\,a\in A\}$, where q is a fixed element of Q, furnish a partition of Q. Indeed, suppose $Ab\cap Ac\neq\emptyset$ $(b, c\in Q)$. We have to prove $Ab\subseteq Ac$. There exist a_1, a_2 A such that $a_1b=a_2c$. Take an a_3 from A; then

$$a_3b = (a_3/a_1)b = \big((a_3/a_1)b\big)(a_1b) = \big((a_3/a_1)b\big)(a_1b\backslash a_2c) = \big((a_3/a_1)(a_1\backslash a_2)\big)c;$$

i.e., $Ab\subseteq Ac$. Now the mediality implies that this partition is compatible with the quasigroup operations, showing that A is a congruence class in $\mathbf{Q}$. Thus, the Hamiltonian property of $\mathcal{R}$ is established.

Thus, $\mathcal{R}$ is equivalent to $\mathcal{A}(\mathbf{R})$ for some $\mathbf{R}$. We have to prove that $\mathbf{R}$ is a homomorphic image of $\mathbf{P}$. The set R equipped with the ring addition and right multiplications is a free $\mathbf{R}$-module with the free generator 1. By Lemma 2 in [7], the associated affine module $\mathbf{R}^*$ is free in $\mathcal{A}(\mathbf{R})$ with the free generating set $\{0, 1\}$. Let $\mathbf{F}_2$ denote the free idempotent medial quasigroup with the same free generating set. Then there exists a weak isomorphism $\varphi\colon \mathbf{F}_2\to\mathbf{R}^*$ such that $0\varphi=0$, $1\varphi=1$. Denote by ζ the one-to-one correspondence of the polynomials of $\mathbf{F}_2$ and $\mathbf{R}^*$ under this weak isomorphism.

Take $(\cdot)\zeta=(x, x')$. Then $1=1\cdot 1=(x, x')(1, 1)=x+x'$, whence $x'=1-x$. If $(/)\zeta=(u, u')$ then $1=(1/0)0=(1u+0u')x+0(1-x)=ux$, and, by idempotency of the right division, $u'=1-u$. If $(\backslash)\zeta=(v, v')$, then we get $v(1-x)=1$, $v'=1-v$ analogously. Observe that for any $f(x)\in\mathbf{Z}[x]$, and non-negative integers k, l, the ring $\mathbf{R}$ contains the product $f(x)u^kv^l$. On the other hand, using the commutativity of $\mathbf{R}$ and the equations $ux=v(1-x)=1$, an induction (on the number of fundamental operations occuring in the expression of elements of $\mathbf{F}_2$ over $\{0, 1\}$) shows that every element of $(\mathbf{F}_2\varphi=)\mathbf{R}$ may be written in the form $f(x)u^kv^l$. Hence there exists a homomorphism of $\mathbf{P}$ onto $\mathbf{R}$ $\left(\text{namely, } \dfrac{f(x)}{x^k(1-x)^l}\to f(x)u^kv^l\right)$, proving the second part of the theorem.

Now we can assume that $\mathscr{P}$ is equivalent to $\mathscr{A}(\mathbf{R}_0)$ for some homomorphic image $\mathbf{R}_0$ of $\mathbf{P}$. It is clear from the proof of Theorem 3 in [7] that $\mathscr{A}(\mathbf{R}_0)$ is equivalent to some subvariety of $\mathscr{A}(\mathbf{P})$. But $\mathscr{A}(\mathbf{P})$ itself is equivalent to some variety of idempotent medial quasigroups. Indeed, the polynomials

$$(3)\qquad (x, 1-x),\quad \left(\frac{1}{x}, 1-\frac{1}{x}\right),\quad \left(\frac{1}{1-x}, 1-\frac{1}{1-x}\right),$$

considered as multiplication and divisions, satisfy (1); further, an induction (on the arity) shows that all polynomials of any affine module over $\mathbf{P}$ may be expressed as polynomials over (3). Thus, $\mathbf{P}$ is also a homomorphic image of $\mathbf{R}_0$, whence, using the fact that $\mathbf{P}$ is Noetherian, it follows $\mathbf{R}_0 \cong \mathbf{P}$, qu.e.d.

Corollary 1. *There exist countably many varieties of idempotent medial quasigroups.*

Theorem 2. *The equationally complete varieties of idempotent medial quasigroups coincide up to equivalence with the varieties of affine modules over finite fields except $GF(2)$.*

Proof. In virtue of the remark at the end of [7], the varieties of quasigroups in question are equivalent to varieties of affine modules over simple quotient rings of $\mathbf{P}$. Such quotient rings are fields; we prove that they are finite. Observe that $\mathbf{P}$ is a homomorphic image of the polynomial ring $\mathbf{Z}[x_1, x_2, x_3]$, because the last one is free with the free generating set $\{x_1, x_2, x_3\}$ in the variety of commutative rings with unit element. It is known, that any maximal ideal in $\mathbf{Z}[x_1, x_2, x_3]$ has a finite index there (see [4], p. 68.). Hence the same holds for $\mathbf{P}$. Thus, the quotient fields of $\mathbf{P}$ are finite, indeed.

On the other hand, any finite field $\mathbf{K}$ consisting of at least three elements, is a homomorphic image of $\mathbf{P}$, because the correspondence $0\to 0$, $1\to 1$, $x\to\alpha$ (where α is a multiplicative generator of $\mathbf{K}$) may be extended to a homomorphism of $\mathbf{P}$ onto $\mathbf{K}$. The trivial fact that no polynomials of affine modules over GF(2) may be essentially binary, completes the proof.

Corollary 2. *There exist countably many equationally complete varieties of idempotent medial quasigroups.*

Theorem 2 enables us to axiomatize equationally complete varieties of idempotent medial quasigroups. Let $\mathbf{K}$ be an arbitrary finite field consisting of $q(>2)$ elements. Take a generating element α of the multiplicative group of $\mathbf{K}$. Let k be the unique integer between 0 and $q-1$ for which $\alpha^k=(1-\alpha)^{-1}$ holds; let, furthermore, for $i=1,\dots,q-2$ the integer $i\sigma$ $(0<i\sigma<q-1)$ defined by the equation $\alpha^{i\sigma}=\alpha^{i+1}-\alpha+1$. This definition fails for $i\equiv-(k+1)$ $(\mathrm{mod}\,(q-1))$ if $2|q$ and for $i\equiv-\left(\frac{q-1}{2}+k+1\right)$ $(\mathrm{mod}\,(q-1))$ if $2\nmid q$, and so the mapping σ has a domain con-

taining $q-3$ numbers; it is one-to-one and its range does not include $q-1-k$, but $(q-1-k)\sigma$ exists always unless the domain of σ is empty.

Theorem 3. *The variety $\mathcal{K}$ of idempotent medial quasigroups determined by the further identities*

$$(6) \qquad x/y = xy^{q-2},$$

$$(7) \qquad y\backslash x = xy^k,$$

$$(8) \qquad xy^i x = xy^{i\sigma} \quad \text{if} \quad 1 \leqq i \leqq q-2 \quad \text{and} \quad i\sigma \text{ is defined},$$

$$(9) \qquad xy^i x = y \quad \text{if} \quad 1 \leqq i \leqq q-2 \quad \text{and} \quad i\sigma \text{ is undefined},$$

is equationally complete and equivalent to $\mathcal{A}(\mathbf{K})$.

Proof. Any affine module $\mathbf{A}$ over $\mathbf{K}$ considered as a quasigroup with multiplication and divisions

$$(10) \qquad (\alpha, 1-\alpha), \quad (\alpha^{-1}, 1-\alpha^{-1}), \quad ((1-\alpha)^{-1}, 1-(1-\alpha)^{-1})$$

belongs to $\mathcal{K}$. Indeed, a routine computation shows that $\mathbf{A}$ is idempotent, medial, and the identities (6)—(9) are satisfied in it; furthermore, the familiar induction used in this paper, gives that all polynomials of $\mathbf{A}$ may be expressed as polynomials over (10). It remains to prove that $\mathcal{K}$ is equationally complete.

Observe first that (6) and (7) implies the identities

$$(6') \qquad xy^{q-1} = x,$$

$$(7') \qquad yxy^k = x.$$

Only (7′) needs a verification. Using several times the identity

$$(11) \qquad (yx)y = y(xy)$$

(a consequence of the idempotency and mediality) we get $yxy^k = y(xy^k) = y(y\backslash x) = x$.

We establish the equational completeness of $\mathcal{K}$ by proving that any algebra $\mathbf{A}_n$ in $\mathcal{K}$, with a minimal generating set of n elements, is determined uniquely up to isomorphism. $\mathbf{A}_1$ consists of a single element. Let $\mathbf{A}_2$ be generated by the set $\{x, y\}$. We show that A_2 consists exactly of the elements

$$(12) \qquad y, x, xy, \ldots, xy^{q-2}.$$

For this aim we show that the product of any two elements from (12) occurs in (12) (since, in virtue of (6)—(7), divisions in $\mathbf{A}_2$ can be expressed by multiplication). This requires some computations which may be surveyed on the following table:

	y	x	xy^{t_2}
y	*	(13)	(15)
x	*	*	(16)
xy^{t_1}	*	*	(17)

Here asterisk means that product of the leading members indicating the considered row and column obviously occurs in (12); the numbers in brackets refer to the computations what follow:

(13) $$yx \overset{(6')}{=} yxy^{q-1} = yxy^k y^{q-1-k} \overset{(7')}{=} xy^{q-1-k}.$$

Hence also

(14) $$xy^t x^2 = xy^{q-1-k}$$

follows in the case when $t\sigma$ is undefined.

(15) $$y(xy^t) \overset{(11)}{=} yxy^t \overset{(6')}{=} yxy^k y^{q-1-k+t} \overset{(7')}{=} xy^{q-1-k+t}.$$

(16) $$x(xy^t) \overset{(6')}{=} x(xy^t)x^k x^{q-1-k} \overset{(7')}{=}$$

$$= xy^t x^{q-1-k} = \begin{cases} xy^{t\sigma} x^{q-1-k-1} & \text{by (8) for } t\sigma \text{ defined,} \\ y & \text{by (9) for } t\sigma \text{ undefined and } k=q-2, \\ xy^{q-1-k} x^{q-1-k-2} & \text{by (14) in the remainder case.} \end{cases}$$

We can iterate, if it is necessary, the last step of (16) until finally we get an expression of form y or $xy^{t'}$. The computation of $(xy^{t_1})(xy^{t_2})$ will be divided into three parts according to the cases $t_1>t_2$, $t_1=t_2(=t)$ and $t_1<t_2$.

(17_1) $$(xy^{t_1})(xy^{t_2}) \overset{(2)}{=} xy^{t_1-t_2}xy^{t_2} = \begin{cases} xy^{(t_1-t_2)\sigma+t_2} & \text{by (8) for } (t_1-t_2)\sigma \text{ defined,} \\ y & \text{by (9) for } (t_1-t_2)\sigma \text{ undefined.} \end{cases}$$

(17_2) $$(xy^t)(xy^t) = xy^t.$$

(17_3) $$(xy^{t_1})(xy^{t_2}) \overset{(2)}{=} x(xy^{t_2-t_1})y^{t_1} \overset{(16)}{=} \begin{cases} xy^{(t_2-t_1)'+t_1} & \text{or} \\ yy^{t_1} = y. \end{cases}$$

Furthermore, the elements (12) are pairwise distinct. Indeed, $y=xy^t$ $(0<t<q-1)$ implies $y=yy^{q-1-t}=xy^{q-1}=x$ by (6′), in contrary to the assumption. From the regularity of $\mathscr{K}$, no other pairs of elements in (12) may equal. Thus we showed that $\mathbf{A}_2$ consists of the q distinct elements (12) and its multiplication table is uniquely defined.

Suppose, by induction, that $\mathbf{A}_n$ $(n \geqq 2)$ is unique, and let the minimal generating set of $\mathbf{A}_{n+1}$ be $\{x_0, x_1, \ldots, x_n\}$. Then $[x_0, x_1]$ and $[x_1, \ldots, x_n]$ are isomorphic to $\mathbf{A}_2$ and $\mathbf{A}_n$, respectively. Clearly, $[x_0, x_1] \cup [x_1, \ldots, x_n]$ generates $\mathbf{A}_{n+1}$. On the other hand, $[x_0, x_1] \cap [x_1, \ldots, x_n] = x_1$, since if $x \in [x_0, x_1] \cap [x_1, \ldots, x_n]$ holds for $x \neq x_1$, then $[x, x_1] \cong \mathbf{A}_2 \cong [x_0, x_1]$, whence $[x, x_1] = [x_0, x_1]$, i.e., $[x_0, x_1] \subseteq [x_1, \ldots, x_n]$, denying the minimality of $\{x_0, x_1, \ldots, x_n\}$. Hence we can apply Lemma 1 from [7]: $\mathbf{A}_{n+1} \cong \cong \{x_0, x_1] \times [x_1, \ldots, x_n] \cong \mathbf{A}_2 \times \mathbf{A}_n$, and so $\mathbf{A}_{n+1}$ is unique up to isomorphism. Thus, $\mathscr{K}$ is equationally complete, ending the proof of the Theorem.

Corollary 3. *Equationally complete varieties of idempotent medial quasigroups are equivalent to varieties of groupoids.*

Remarks 1. The varieties $\mathcal{G}(n, k)$ of groupoids, discussed in [10], are also, in fact, equivalent to varieties of idempotent medial quasigroups. Indeed, as it is shown there, $\mathcal{G}(n, k)$ is equivalent to $\mathcal{A}(\mathbf{R}(n, k))$, where $\mathbf{R}(n, k)=\mathbf{Z}[x]/(x^n-1, x^k+x-1)$. Now, for any natural numbers $k<n$, $\mathbf{R}(n, k)$ is a homomorphic image of $\mathbf{P}$ under the homomorphism $\frac{f(x)}{x^u(1-x)^v} \to f(r)r^{(n-1)u+(n-k)v}$, where $r=x+(x^n-1, x^k+x-1)$ in $\mathbf{R}(n, k)$. Hence $\mathcal{G}(n, k)$ is equivalent to a subvariety of $\mathcal{P}$; i.e., it is equivalent to some variety $\mathcal{P}_{n,k}$ of idempotent medial quasigroups. Note that $\mathcal{P}_{n,k}$ may be axiomatized by the identities $x/y=xy^{n-1}$, $y\backslash x=xy^{n-k}$.

2. The solution of Plonka's problem (Corollary 7 in [10]) can be derived from the above considerations as well. Let $\mathcal{G}$ be the variety of groupoids satisfying the identities $x^2=x$, $x(yx)=y$ and $xyz=zyx$. The last identity implies the mediality; defining x/y by yx and $y\backslash x$ by xy, $\mathcal{G}$ becomes a variety of quasigroups, which is clearly equivalent to $\mathcal{G}$. By Theorem 1, $\mathcal{G}$ is equivalent to $\mathcal{A}(\mathbf{R})$ for some ring $\mathbf{R}$, generated by an element α, such that the operation $(\alpha, 1-\alpha)$ of $\mathcal{A}(\mathbf{R})$ corresponds to the multiplication of $\mathcal{G}$. Then Plonka's second and third identities, rewritten with the aid of α, give $\alpha^2=1-\alpha$ and $\alpha(1-\alpha)=1$, and this implies that $\mathbf{R}\cong GF(4)$; i.e., $\mathcal{G}$ is equivalent to $\mathcal{A}(GF(4))$.

3. The characterization of medial Steiner triple systems (Corollary 8 in [10]) as affine modules over $GF(3)$ is even the special case $\mathbf{K}=GF(3)$ of Theorem 3. For related results, see [1] and [9].

4. Algebras with one ternary operation τ which commutes with itself and satisfies the identity

$$\tau(x, x, y) = \tau(x, y, x) = \tau(y, x, x) = y \tag{18}$$

were discussed by Aliev [1], who called them S^*-algebras. Aliev's results jointly with Givant's characterization of varieties in which all members are free [8] imply that the variety $\mathcal{S}^*$ of all S^*-algebras is equivalent to $\mathcal{A}(GF(2))$. This fact can be deduced also from our considerations as follows. Obviously, $\mathcal{S}^*$ is idempotent and Abelian; further the defining identities involve that the S^*-algebras are essentially flocks with commutative covering groups ([5], p. 40), whence $\mathcal{S}^*$ is regular and Hamiltonian. Then Theorem 2 in [7] shows that $\mathcal{S}^*$ is equivalent to $\mathcal{A}(\mathbf{R})$ for some commutative ring $\mathbf{R}$. Now the routine discussion of the identities (18) furnishes that $\mathbf{R}$ is generated by its unit element, and $1=-1$ in $\mathbf{R}$. Hence $\mathbf{R}\cong GF(2)$.

References

[1] I. S. O. ALIEV, On the minimal variety of symmetric algebras, *Algebra i Logika*, **5**: 6 (1966), 5—14. (Russian)

[2] V. D. BELOUSOV, *Foundations of the theory of quasigroups and loops*, Nauka (1967). (Russian)

[3] V. D. BELOUSOV, Transitive distributive quasigroups, *Ukr. Mat. Ž.*, **10** (1958), 13—22. (Russian)

[4] N. BOURBAKI, *Éléments de Mathématique XXX, Algèbre commutative*; Hermann, Paris 1964.

[5] R. H. BRUCK, *A survey of binary systems*, Springer (1958).

[6] B. CSÁKÁNY, Characterizations of regular varieties, *Acta Sci. Math.*, **31** (1970), 187—189.

[7] B. CSÁKÁNY, Varieties of affine modules, *Acta Sci. Math.*, **37** (1975), 3—10.

[8] S. R. GIVANT, A representation theorem for universal classes of algebras in which all members are free, *Notices AMS*, **19**: 7 (1972), p. A—767.

[9] G. GRÄTZER, P. PADMANABHAN, On idempotent, commutative and nonassociative groupoids, *Proc. Amer. Math. Soc.*, **28**: 1 (1971), 75—80.

[10] A. MITSCHKE, H. WERNER, On groupoids representable by vector spaces over finite fields, *Archiv der Math.*, **24** (1973), 14—20.

[11] S. K. STEIN, On the foundations of quasigroups, *Trans. Amer. Math. Soc.*, **85** (1957), 228—256.

(Received June 5, 1973)

Varieties in which congruences and subalgebras are amicable

By B. CSÁKÁNY in Szeged

In earlier articles [6], [8] we proved: If in each algebra of the variety $\mathscr{A}$ any subalgebra is a block of a unique congruence, and

$$\begin{Bmatrix}\text{every congruence has a unique block which is a subalgebra}\\ \text{all block of any congruence are subalgebras}\end{Bmatrix}$$

then $\mathscr{A}$ is equivalent to the variety of all

$$\begin{Bmatrix}\text{unital right modules}\\ \text{affine modules}\end{Bmatrix}$$

over some ring with unit element.

These results suggest that it may be fruitful to investigate those varieties in which there exists a similar but more general connection between congruences and subalgebras. Such a connection can be introduced in the following way.

Let M be a non-void set, $\mathfrak{S}$ a set of its subsets and Σ a set of equivalences of M. We say that $\mathfrak{S}$ and Σ are *amicable*, if every $S \in \mathfrak{S}$ is a block of some $\sigma \in \Sigma$ and every $\sigma \in \Sigma$ has a block which belongs to $\mathfrak{S}$. Uniqueness of the corresponding equivalences and blocks is not required. If, especially, **M** is an algebra, $\mathfrak{S}$ the set of its subalgebras and Σ the set of congruences of **M**, then in the above case we say shortly that in **M** the congruences and subalgebras are amicable. Finally, if the same is fulfilled in each algebra of a variety $\mathscr{A}$, we say that in $\mathscr{A}$ congruences and subalgebras are amicable.

Following KUROŠ ([2], § 14; see also [11]), we call a variety $\mathscr{A}$ Abelian, if in all algebras of $\mathscr{A}$ any two operations commute. Our result consists of a full description of equationally complete Abelian varieties with the property in the title.

Theorem. *A variety $\mathscr{A}$ is an equationally complete Abelian variety in which congruences and subalgebras are amicable if and only if $\mathscr{A}$ is equivalent to one of the following varieties:*

(a) *varieties of vector spaces over fields,*

(b) *the variety of pointed sets,*

(c) *varieties of affine spaces over fields* (see [3], Ch. XII, and [8]);

(d) *the variety of sets.*

Corollary. *An Abelian variety is categorically free (i.e., exhausted by its free algebras) if and only if it is an equationally complete variety in which congruences and subalgebras are amicable.*

As a preparation of the proof, we formulate several lemmas.

Lemma 1. *In any Abelian algebra the set of all idempotent elements*[1]) *forms a subalgebra.*

Indeed, let f and g be n-ary, resp. m-ary polynomials on the Abelian algebra **A**; further, let $a_1, \ldots, a_n$ be idempotent elements of **A**. Since f and g commute, we have $g(f(a_1, \ldots, a_n), \ldots, f(a_1, \ldots, a_n)) = f(g(a_1, \ldots, a_1), \ldots, g(a_n, \ldots, a_n)) = f(a_1, \ldots, a_n)$, i.e., $f(a_1, \ldots, a_n)$ is also idempotent.

Lemma 2. *In any algebra a subset closed with respect to endomorphisms generates a fully invariant congruence.*

Let **A** be an arbitrary algebra, M a subset of A, and denote by the sign $\sim$ the congruence of **A** generated by M (i.e., the smallest congruence of **A** under which all elements of M are congruent). Then, for $a, b \in A$, $a \sim b$ means that there exist elements $a = a_0, a_1, \ldots, a_k = b$ such that for suitable translations (i.e., unary algebraic functions) $\tau_1, \ldots, \tau_k$ of **A** and elements $m_{10}, \ldots, m_{k0}, m_{11}, \ldots, m_{k1} \in M$ the equations $m_{ij}\tau_i = a_{i-1+j}$ $(i = 1, \ldots, k;\ j = 0, 1)$ hold. For any $x \in A$ and for $i = 1, \ldots, k$ let the image of x under τ_i defined by $t_i(x, c_{i1}, \ldots, c_{il_i})$, where t_i is a polynomial of **A** and $c_{i1}, \ldots, c_{il_i} \in A$. Suppose that M is closed with respect to endomorphisms of **A**. For any such endomorphism φ denote by τ_i^φ the translation $x \to t_i\ (x, c_{i1}\varphi, \ldots, c_{il_i}\varphi)$. Then for $a\varphi = a_0\varphi, a_1\varphi, \ldots, a_k\varphi = b\varphi$, for $\tau_1^\varphi, \ldots, \tau_k^\varphi$, and for the elements $m_{ij}\varphi \in M$ we have $(m_{ij}\varphi)\tau_i^\varphi = t_i(m_{ij}\varphi, c_{i1}\varphi, \ldots) = (t_i(m_{ij}, c_{i1}, \ldots))\varphi = a_{i-1+j}\varphi$, whence $a\varphi = b\varphi$, which was needed.

The following fact is familiar:

Lemma 3. *A free algebra in an equationally complete variety has no other fully invariant congruences than the trivial ones.*

Lastly, we recall a useful result of KLUKOVITS [12]:

Lemma 4. *A variety $\mathscr{A}$ (of type τ) is Hamiltonian (*i.e., *in any algebra of $\mathscr{A}$ every subalgebra is a block of some congruence) if and only if for any n-ary polynomial symbol f (of type τ) there exists a ternary polynomial symbol h_f (of type τ) such that in $\mathscr{A}$ the identity*

$$(1) \qquad f(x_1, \ldots, x_n) = h_f(x_0, x_1, f(x_0, x_2, \ldots, x_n))$$

holds.

---

[1]) We call an element of an algebra **A** *idempotent* if it forms a one-element subalgebra of **A**. A class of algebras is *idempotent* if its every algebra consists of idempotent elements only.

Proof of the theorem. Sufficiency is obvious. To prove the necessity, let us consider an equationally complete Abelian variety $\mathscr{A}$ in which congruences and subalgebras are amicable. The last condition means exactly that $\mathscr{A}$ is Hamiltonian and any algebra in $\mathscr{A}$ has at least one idempotent element. We shall distinguish two cases.

I. $\mathscr{A}$ is not idempotent.

Let $\mathbf{F}_\omega$ be the $\mathscr{A}$-free algebra with countable free generating set. The idempotent elements of $\mathbf{F}_\omega$ form a proper subset M in F_ω. By Lemma 1, M is a subalgebra in $\mathbf{F}_\omega$. Obviously, M is closed under endomorphisms of $\mathbf{F}_\omega$. Since $\mathscr{A}$ is Hamiltonian, M is a block of the congruence generated by itself in $\mathbf{F}_\omega$. Hence this congruence has at least two blocks. On the other hand, this congruence is fully invariant by Lemma 2, and, using Lemma 3, we get that our congruence is just the equality. It follows that $\mathbf{F}_\omega$ has a unique idempotent element 0. Then there exist an essentially nullary polynomial whose value is 0 in $\mathbf{F}_\omega$; denote it also by 0. Now we shall distinguish two subcases.

a) For some $n>1$, $\mathscr{A}$ has an essentially n-ary polynomial.

Suppose that n is the minimal among such natural numbers; we show that $n=2$. Denote by $\mathbf{F}_n$ the $\mathscr{A}$-free algebra freely generated by the set $\{x_1, \dots, x_n\}$ and let f be an essentially n-ary polynomial. Since n is minimal, $f(0, \varepsilon_n^2, \dots, \varepsilon_n^n)$ — where ε_n^i denotes the i-th n-ary projection — is essentially not more than unary and so for some i $(2 \leqq i \leqq n)$ $f(0, x_2, \dots, x_n) \in [x_i]$ holds, i.e., for a suitable unary f_i we have $f(0, x_2, \dots, x_n) = f_i(x_i)$. Applying Lemma 4, we get

$$f(x_1, \dots, x_n) = h_f(0, x_1, f(0, x_2, \dots, x_n)) = h_f(0, x_1, f_1(x_i)) \in [x_1, x_i],$$

whence f is essentially binary. In what follows we write f multiplicatively.

Let $\mathbf{F}_2$ be the $\mathscr{A}$-free algebra with free generators x and y. Define on F_2 an equivalence $\sim$ as follows: for $a, b \in F_2$, let $a \sim b$ if $a \cdot 0 = b \cdot 0$. This relation is a fully invariant congruence on $\mathbf{F}_2$. Indeed, for any m-ary operation g and $a_1, \dots$ $\dots, a_m, b_1, \dots, b_m \in F_2$ from $a_i \sim b_i$ $(i=1, \dots, m)$ it follows (using that f and g commute):

$$(2) \qquad g(a_1, \dots, a_m) \cdot 0 = g(a_1, \dots, a_m) \cdot g(0, \dots, 0) = \\ = g(a_1 \cdot 0, \dots, a_m \cdot 0) = g(b_1 \cdot 0, \dots, b_m \cdot 0) = g(b_1, \dots, b_m) \cdot 0,$$

whence $g(a_1, \dots, a_m) \sim g(b_1, \dots, b_m)$. Further, if $a, b \in F_2$ and σ is any endomorphism of $\mathbf{F}_2$, then $a \sim b$ implies

$$(3) \qquad a\sigma \cdot 0 = a\sigma \cdot 0\sigma = (a \cdot 0)\sigma = (b \cdot 0)\sigma = b\sigma \cdot 0,$$

i.e., $a\sigma \sim b\sigma$.

On the basis of Lemma 3, $\sim$ is trivial. Suppose that it is the complete relation; then 0 is a right zero element with respect to f. Let f^* denote the polynomial $\varepsilon_2^2 \cdot \varepsilon_2^1$.

Using Lemma 4, we get

$$xy = f^*(y, x) = h_{f^*}(0, y, f^*(0, x)) = h_{f^*}(0, y, x\cdot 0) = h_{f^*}(0, y, 0),$$

a contradiction since f is essentially binary. Hence it follows that $\sim$ is the equality relation on F_2. This means that the mapping $\varphi_1\colon F_2\to F_2$ defined by $a\varphi_1 = a\cdot 0$ is $1-1$. Moreover, φ_1 maps F_2 onto itself. Indeed, as (2) and (3) show, the image of F_2 under φ_1 is a fully invariant subalgebra in $\mathbf{F}_2$, whence, by Lemma 2 and 3, this image is either $\{0\}$ or F_2. The first case infer that $\mathscr{A}$ is trivial. Thus, $F_2\varphi_1 = F_2$; i.e., $\varphi_1\colon F_2\to F_2$ is a bijection. We can get in an analogous way that the mapping $\varphi_2\colon F_2\to F_2$ defined by $a\varphi_2 = 0\cdot a$ is also a bijection.

Let $f^{-1}(x, y)$ be the unique element of F_2 for which $f^{-1}(x, y)\varphi_1 = x$ holds. Then $f^{-1}(x, y)\cdot 0 = x$ is an identity in $\mathscr{A}$, whence $f^{-1}(x, 0)\cdot 0 = x$ follows. We get similarly a binary polynomial ${}^{-1}f$ satisfying $0\cdot {}^{-1}f(0, x) = x$. Now we take the polynomial $f^{-1}(\varepsilon_2^1, 0)\cdot {}^{-1}f(0, \varepsilon_2^2)$; it will be called addition and denoted additively. We see that 0 is the unit element with respect to addition.

Next we prove that in $\mathscr{A}$ the direct and the $\mathscr{A}$-free products of two algebras coincide. As it was proved in [5] (Theorem 1), this fact jointly with the existence of 0 in $\mathscr{A}$ implies that $\mathscr{A}$ is equivalent to the variety of all unital right semimodules over some associative semiring R with unit element. Let $\mathbf{A}, \mathbf{B}\in\mathscr{A}$; then $\mathbf{A}\times\mathbf{B}$ is generated by the union of its subalgebras $(\mathbf{A}, \mathbf{0}) = \{(a, 0)\,|\,a\in A\}$ and $(\mathbf{0}, \mathbf{B}) = \{(0, b)\,|\,b\in B\}$; furthermore, $(\mathbf{A}, \mathbf{0})\cong\mathbf{A}$ and $(\mathbf{0}, \mathbf{B})\cong\mathbf{B}$. Consider an arbitrary algebra $\mathbf{C}\in\mathscr{A}$ and homomorphisms $\psi\colon (A, 0)\to C$, $\chi\colon (0, B)\to C$. We have to prove that ψ and χ admit a common homomorphic extension $\eta\colon \mathbf{A}\times\mathbf{B}\to\mathbf{C}$. Define η by means $(a, b)\eta = (a, 0)\psi + (0, b)\chi$. Obviously, η is an extension of ψ and χ. On the other hand, for any m-ary polynomial g and elements $a_1, \dots, a_m\in A$, $b_1, \dots, b_m\in B$ we have

$$g((a_1, b_1), \dots, (a_m, b_m))\eta = (g(a_1, \dots, a_m), g(b_1, \dots, b_m))\eta = (g(a_1, \dots, a_m), 0)\psi +$$
$$+ (0, g(b_1, \dots, b_m))\chi = g((a_1, 0), \dots, (a_m, 0))\psi + g((0, b_1), \dots, (0, b_m))\chi =$$
$$= g((a_1, 0)\psi, \dots, (a_m, 0)\psi) + g((0, b_1)\chi + \dots + (0, b_m)\chi) =$$
$$= g((a_1, 0)\psi + (0, b_1)\chi, \dots, (a_m, 0)\psi + (0, b_m)\chi) = g((a_1, b_1)\eta, \dots, (a_m, b_m)\eta),$$

i.e., η is a homomorphism.

Thus, $\mathscr{A}$ is equivalent to the variety of all unital right semimodules over a semiring $\mathbf{R}$. Then the Hamiltonian property of $\mathscr{A}$ guarantees that $\mathbf{R}$ is an associative ring, and, as semimodules over rings are modules, $\mathscr{A}$ is equivalent to the variety of unital right modules over the ring $\mathbf{R}$ (see [12], Theorem 7). Now, the Abelian property and the equational completeness of $\mathscr{A}$ together imply, that $\mathbf{R}$ is a field and $\mathscr{A}$ is equivalent to the variety of all vector spaces over $\mathbf{R}$ (see [6], § 2).

b) For $n > 1$, $\mathscr{A}$ has no essentially n-ary polynomials.

Let $\mathbf{F}_2$ be again the $\mathscr{A}$-free algebra freely generated by x and y. Define on $\mathbf{F}_2$ an equivalence $\sim$ as follows: for $a, b \in F_2$, let $a \sim b$ if $[a] \cap \{x, y\} = [b] \cap \{x, y\}$. We shall prove that $\sim$ is a fully invariant congruence on $\mathbf{F}_2$.

Since all operations in $\mathscr{A}$ are essentially no more than unary, the set of translations of $\mathbf{F}_2$ is the same as that of its (polynomial) operations. The last ones commute pairwise, whence it follows that all translations of $\mathbf{F}_2$ are endomorphisms. Thus, it is enough to prove that $\sim$ is invariant under endomorphisms.

Let $C_x = \{a \mid a \in F_2,\ [a] \cap \{x, y\}\} = \{x\}$. Define C_y similarly; and let $C_0 = \{a \mid a \in F_2,\ [a] \cap \{x, y\} = \emptyset\}$. Then all the blocks of $\sim$ are C_x, C_y, C_0 and none of them may be void. Indeed, if $[a] \cap \{x, y\} = \{x, y\}$, then let, e.g., $a = t(x)$, where t is a polynomial. For suitable polynomial r we have $r(a) = y$, whence $r(t(x)) = y$, showing that $\mathscr{A}$ is trivial, a contradiction. On the other hand, $x \in C_x$, $y \in C_y$ and $0 \in C_0$. Remark that $C_x \subseteqq [x]$ and $C_y \subseteqq [y]$.

In the following, l, k, q, r, s, t, u denote (unary) polynomials. Consider an arbitrary endomorphism φ of $\mathbf{F}_2$. First we show that φ maps C_0 into itself. Let $l(x) \in C_0$ and suppose $l(x)\varphi \in C_x$. Then for a suitable k we have $k(l(x)\varphi) = x$, whence $k(l(x\varphi)) = x$. If $x\varphi = q(x)$, then, by the Abelian property, $k(q(l(x))) = k(l(q(x))) = x$ holds showing that $l(x) \in C_x$, a contradiction; and if $x\varphi = q(y)$, then $k(l(q(y))) = x$ and $\mathscr{A}$ is trivial, in contrast to the assumption. Supposing that $l(x)\varphi \in C_y$ we get a contradiction analogously.

Let now $l(x) \in C_x$ and suppose $l(x)\varphi \in C_x$. Consider an arbitrary element $r(x)$ from C_x; we must prove that $r(x)\varphi \in C_x$. For suitable s, t we have $s(l(x\varphi)) = x$ and $t(r(x)) = x$. Hence $s(l(t(r(x)\varphi))) = s(l(t(r(x\varphi)))) = t(r(s(l(x\varphi)))) = x$, and thus $r(x)\varphi \in C_x$. Suppose that $l(x)\varphi \in C_y$ and $u(l(x)\varphi) = y$. Let r and t be as above; then $u(l(t(r(x)\varphi))) = t(r(u(l(x)\varphi))) = t(r(y)) = y$, whence $r(x)\varphi \in C_y$. These considerations show also that $l(x)\varphi \in C_0$ implies $r(x)\varphi \in C_0$.

We got that $\sim$ is a fully invariant congruence in $\mathbf{F}_2$ with three blocks. By virtue of Lemma 3, $\sim$ is the equality, and so $F_2 = \{x, y, 0\}$, i.e., $\mathscr{A}$ has no other operations than 0. Hence $\mathscr{A}$ is the variety of pointed sets.

II. $\mathscr{A}$ is idempotent.

Let us consider for a moment the case in which, for some $n > 1$, $\mathscr{A}$ has an essentially n-ary (polynomial) operation. Suppose that n is minimal; it can be shown that $n \leqq 3$. For this aim it suffices to repeat the consideration we made at the beginning of section a) with the only deviation that we must write x_2 instead of 0.

Hence we shall distinguish three subcases.

α) $\mathscr{A}$ has an essentially binary polynomial.

Let f be such a polynomial; we shall write it multiplicatively. Again $\mathbf{F}_2$ denotes the $\mathscr{A}$-free algebra with free generators x and y. Introduce a relation $\sim$ on F_2: for $a, b \in F_2$, let $a \sim b$ if there exist elements $u, a_1, b_1 \in F_2$ such that $a = ua_1$, $b = ub_1$ hold. Obviously, $\sim$ is reflexive and symmetric; we show that it is also transitive. It suffices to prove that if $ab=cd$ $(a, b, c, d \in F_2)$ then for any $p \in F_2$ the equation

$$ap = cz \tag{4}$$

has a solution for z in F_2. From Lemma 4 we get

$$rs = h_f(s, r, ss) = h_f(s, r, s)$$

and

$$(rs)t = h_f(r, rs, rt) = h_f(rr, rs, rt) = h_f(r, r, r) \cdot h_f(r, s, t) = r \cdot h_f(r, s, t).$$

Using these equalities as well as idempotency and permutability of operations in $\mathscr{A}$ one can compute ap as follows:

$$\begin{aligned} ap &= h_f(b, a, bp) = h_f(b, a, h_f(p, b, p)) = \\ &= h_f(h_f(b, b, b), h_f(a, a, a), h_f(p, b, p)) = \\ &= h_f(h_f(b, a, p), h_f(b, a, b), h_f(b, a, p)) = (ab) \cdot h_f(b, a, p) = \\ &= (cd) \cdot h_f(b, a, p) = c \cdot h_f(c, d, h_f(b, a, p)). \end{aligned}$$

Thus, $z=h_f(c, d, h_f(b, a, p))$ is a solution of (4). Hence $\sim$ is an equivalence. Moreover, $\sim$ is a fully invariant congruence on $\mathbf{F}_2$; indeed, for any m-ary polynomial g and elements $a_i, b_i, u_i \in F_2$ $(i=1, \ldots, m)$ we have $g(u_1 a_1, \ldots, u_m a_m) = g(u_1, \ldots, u_m) \cdot g(a_1, \ldots, a_m) \sim g(u_1, \ldots, u_m) \cdot g(b_1, \ldots, b_m) = g(u_1 b_1, \ldots, u_m b_m)$, and for arbitrary endomorphism φ of $\mathbf{F}_2$ from $a \sim b$ it follows $a\varphi = u\varphi \cdot a_1 \varphi \sim u\varphi \cdot b_1 \varphi = b\varphi$.

By Lemma 3, the congruence $\sim$ is trivial, and, since f is essentially binary, $\sim$ is the complete relation. Hence $x \sim y$ in $\mathbf{F}_2$. This means that, for a suitable binary polynomial l, in $\mathbf{F}_2$ the equality $x \cdot l(x, y) = y$ holds. Furthermore, $l(x, xy) = l(xx, xy) = l(x, x) \cdot l(x, y) = x \cdot l(x, y) = y$ is also fulfilled. An analogous consideration shows that, for some binary polynomial r, the equalities $r(x, y) \cdot y = x$, $r(xy, y) = x$ hold.

Since these equalities may be considered as identities in $\mathscr{A}$, we see that the algebras in $\mathscr{A}$ are quasigroups with respect to polynomials f, l, r as multiplication, left and right division, respectively. Hence $\mathscr{A}$ is a regular variety [7]. Now Theorem 3 in [8] gives that $\mathscr{A}$ is equivalent to the variety of affine spaces over some field.

β) $\mathscr{A}$ has no essentially binary polynomials, but it has an essentially ternary polynomial.

Let f be essentially ternary and consider the polynomial $t = h_f(\varepsilon_3^3, \varepsilon_3^2, \varepsilon_3^1)$. We show that in $\mathscr{A}$ the identity $h_t(x, y, x) = h_t(x, x, y) = y$ holds (i.e., $\mathscr{A}$ is a normal variety). Take the $\mathscr{A}$-free algebra $\mathbf{F}_3$ with free generators x, y and z. By the assumption, $h_f(\varepsilon_3^1, \varepsilon_3^1, \varepsilon_3^2)$ is essentially at most unary, and by the idempotency, it is a projection. But $f(x, y, z) = h_f(x, x, f(x, y, z))$ shows that $h_f(\varepsilon_3^1, \varepsilon_3^1, \varepsilon_3^2) = \varepsilon_3^1$ is impossible. Hence $h_f(\varepsilon_3^1, \varepsilon_3^1, \varepsilon_3^2) = \varepsilon_3^2$, and $h_t(x, y, x) = h_t(x, y, t(x, x, x)) = t(y, x, x) = h_f(x, x, y) = y$.

On the other hand, t is also essentially ternary. Indeed, in the opposite case h_f were a projection, which is impossible because of (1). Repeating the consideration made for h_f before, we get $h_t(x, x, y) = y$.

Introducing now the binary algebraic operation $a+b=h_t(x_0, a, b)$ on the countably generated $\mathscr{A}$-free algebra $\mathbf{F}_\omega(=\langle x_0, x_1, \ldots\rangle)$, we can process similarly as in the proof of Theorem 1 in [8] to prove that $\mathscr{A}$ is equivalent to the variety of affine modules over some ring $\mathbf{R}$. Note that the main identity marked with (3) in [8] is an immediate consequence of the Abelian property of $\mathscr{A}$ here. Moreover, $\mathscr{A}$ is equivalent to the variety of affine spaces over the *field* $\mathbf{R}$, because $\mathscr{A}$ is equationally complete and Abelian (see Theorem 4 in [8]).

γ) For $n>1$, $\mathscr{A}$ has no essentially n-ary polynomials.

Then, evidently, $\mathscr{A}$ is equivalent to the variety of sets. The proof is complete.

Corollary follows directly from GIVANT's characterization of categorically free varieties [10] and our theorem.

Remarks 1. As we have seen, in varieties of modules as well as of affine modules the congruences and subalgebras are amicable. This is the case also in varieties of modules over semigroups (see [1], p. 55) with unit and zero element. Groups, rings and lattices furnish no other varieties with the considered property (abelian groups and zero rings are equivalent to modules).

2. Section β) together with Remark 4 in [9] enables us to give another characterization for ALIEV's variety of S^*-algebras [4]. Namely, if an equationally complete Abelian variety $\mathscr{S}$, in which congruences and subalgebras are amicable, has no binary polynomials, but has an essentially at least ternary polynomial, then $\mathscr{S}$ is equivalent to the variety of S^*-algebras.

References

[1] P. M. COHN, *Universal Algebra*, Harper & Row (1956).

[2] A. G. KUROS, *General Algebra* (Lecture Notes), Moscow State University (1970). (Russian)

[3] S. MAC LANE, G. BIRKHOFF, *Algebra*, Macmillan (1967).

[4] I. S. O. ALIEV, On the minimal variety of symmetric algebras, *Algebra i Logika*, **5**: **6** (1966), 5—14. (Russian)

[5] B. CSÁKÁNY, Primitive classes of algebras which are equivalent to classes of semi-modules and modules, *Acta Sci. Math.*, **24** (1963), 157—164. (Russian)

[6] B. CSÁKÁNY, Abelian properties of primitive classes of universal algebras, *Acta Sci. Math.* **25** (1964), 202—208. (Russian)

[7] B. CSÁKÁNY, Characterizations of regular varieties, *Acta Sci. Math.*, **31** (1970), 187—189.

[8] B. CSÁKÁNY, Varieties of affine modules, *Acta Sci. Math.*, **37** (1975), 3—10.

[9] B. CSÁKÁNY—L. MEGYESI, Varieties of idempotent medial quasigroups, *Acta Sci. Math.*, **37** (1975), 17—23.

[10] S. R. GIVANT, A representation theorem for universal classes of algebras in which all members are free, *Notices AMS*, **19** (1972), A—767.

[11] L. KLUKOVITS, On commutative universal algebras, *Acta Sci. Math.*, **34** (1973), 171—174.

[12] L. KLUKOVITS, Hamiltonian varieties of universal algebras, *Acta Sci. Math.*, **37** (1975), 11—15.

(Received September 28, 1973)

On affine spaces over prime fields

By B. CSÁKÁNY in Szeged

The aim of this note to prove a result for affine spaces over arbitrary prime fields like the Grätzer—Padmanabhan characterization theorem of affine spaces over $GF(3)$. Our terminology and notation are the standard ones (see [1]) excepting that the identical mapping of any set will be considered as an essentially unary operation which permits to give a more concise form for the succeeding propositions. Under this agreement, $p_1(\mathbf{A})$ — the number of essentially unary polynomials — equals 1 for any idempotent algebra.

Following PLONKA [6], for any group $\mathbf{G}=\langle G; +\rangle$ the algebra $\langle G; I\rangle$, where I denotes the set of all idempotent polynomials of $\mathbf{G}$, is called the idempotent reduct of $\mathbf{G}$. Concerning this notion we shall need the fact that idempotent reducts of abelian groups of exponent p are exactly the affine spaces over $GF(p)$; furthermore, the free affine space over $GF(p)$ with an n-element free generating set is the same as the idempotent reduct of $\mathbf{Z}_p^{n-1}$, where $\mathbf{Z}_p$ is the group of order p.

The characterization theorem we mentioned above (i.e., the join of Theorems 2 and 3 in [5]) may be formulated as follows:

A groupoid $\mathbf{A}$ is equivalent to an affine space over $GF(3)$ if and only if

$$(3, k) \qquad p_k(\mathbf{A}) = \frac{1}{3}(2^k-(-1)^k)$$

holds for $k=1, 2, 3, 4$. In this case $(3, k)$ remains valid for all non-negative integers k.

Our result is the following.

Theorem. *Let p be an arbitrary prime. An algebra $\mathbf{A}=\langle A;f\rangle$, where f is at most quaternary, is equivalent to an affine space over $GF(p)$ if and only if*

$$(p, k) \qquad p_k(\mathbf{A}) = \frac{1}{p}((p-1)^k-(-1)^k)$$

holds for $k=1,2,3,4$, and

(p^*) *there exists no subalgebra $\mathbf{B}$ in $\mathbf{A}$ with $1<|B|<p$. In this case (p, k) remains valid for all non-negative integers k.*

Proof. Let $\mathscr{V}$ be the variety generated by **A** and, for any natural k, denote by $\mathbf{F}_k$ the free algebra over $\mathscr{V}$ with the free generating set $\{x_0, \ldots, x_{k-1}\}$. Suppose that **A** is equivalent to an affine space over $GF(p)$. The variety of all affine spaces over $GF(p)$ is equationally complete; hence it is equivalent to $\mathscr{V}$. Thus, for every natural k, $\mathbf{F}_k$ is equivalent to the idempotent reduct of $\mathbf{Z}_p^{k-1}$, implying $|F_k|=p^{k-1}$. The formula

$$(\alpha) \qquad |F_k| = \sum_{i=0}^{k} \binom{k}{i} p_i(\mathbf{A})$$

(see [4], p. 38.) gives

$$p_k(\mathbf{A}) = \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i}|F_i| = \frac{1}{p}((p-1)^k-(-1)^k),$$

which was needed. Further, any subalgebra of **A** is also equivalent to an affine space over $GF(p)$, which clearly cannot have q elements for $1<q<p$.

To prove the sufficiency, first we remark that $(p, 1)$ and $(p, 3)$ jointly imply that f is at least binary and **A** is idempotent. Now, if $p=2$, using Urbanik's description of idempotent algebras ([7], Theorem 4) we get that **A** is equivalent to an affine space over $GF(2)$, moreover, f is essentially ternary.

Suppose $p>2$. By (α), $(p, 1)$ and $(p, 2)$ we have $|F_2|=p$. Let **B** a minimal subalgebra of **A** having at least two elements. By (p^*), we have $|B|\geqq p$. Since **B** is generated by two elements, it is a homomorphic image of $\mathbf{F}_2$, whence $|B|=p$ and $\mathbf{B}\cong\mathbf{F}_2$. Thus, the proper subalgebras of $\mathbf{F}_2$ are exactly the one-element ones.

Next we show that $\mathbf{F}_2^2(=\mathbf{F}_2\times\mathbf{F}_2)$ is generated by the set $S=\{\langle x_1, x_0\rangle, \langle x_0, x_0\rangle, \langle x_0, x_1\rangle\}$. Let $\langle g_1(x_0, x_1), g_2(x_0, x_1)\rangle$ be an arbitrary element of F_2^2. Consider an essentially binary polynomial h of $\mathbf{F}_2$. Then

$$\langle x_0, h(x_0, x_1)\rangle (= h(\langle x_0, x_0\rangle, \langle x_0, x_1\rangle)) \in [S],$$

$$\langle h(x_1, x_0), h(x_0, x_1)\rangle (= h(\langle x_1, x_0\rangle, \langle x_0, x_1\rangle)) \in [S].$$

Now, $h(x_1, x_0)\neq x_0$; hence $[\langle h(x_1, x_0), h(x_0, x_1)\rangle, \langle x_0, h(x_0, x_1)\rangle](\subseteq [S])$ contains p elements, i.e., all elements of F_2^2 with second component $h(x_0, x_1)$, and thus $\langle f(x_0, x_1), h(x_0, x_1)\rangle \in [S]$. Analogously, $\langle g_1(x_0, x_1), x_0\rangle \in [S]$, whence $\langle g_1(x_0, x_1), g_2(x_0, x_1)\rangle \in [S]$ follows.

Let $\varphi\colon F_3\to F_2^2$ that homomorphism for which $x_0\varphi=\langle x_0, x_0\rangle$, $x_1\varphi=\langle x_1, x_0\rangle$, $x_2\varphi=\langle x_0, x_1\rangle$ holds. Then φ is onto. Hence there exists an essentially ternary polynomial m of $\mathbf{F}_3$ satisfying $(m(x_0, x_1, x_2))\varphi=\langle x_1, x_1\rangle$. But

$$(m(x_0, x_1, x_2))\varphi = \langle m(x_0, x_1, x_0), m(x_0, x_0, x_1)\rangle,$$

whence we get that the identity

$$(\beta) \qquad m(x_0, x_1, x_0) = m(x_0, x_0, x_1) = x_1$$

holds in $\mathscr{V}$. This implies

$$(\gamma_3) \qquad \big(m(x_0, f_1(x_0, x_1), f_2(x_0, x_2))\big)\varphi = \langle f_1(x_0, x_1), f_2(x_0, x_1)\rangle$$

for any binary polynomials f_1, f_2.

Observe that $|F_3|=p^2=|F_2^2|$. Thus φ is an isomorphism; i.e., $\mathbf{F}_3 \cong \mathbf{F}_2^2$. We show that $\mathbf{F}_4 \cong \mathbf{F}_2^3$ is valid too. Since $|F_4|=|F_2^3|(=p^3)$, it is enough to show that the homomorphism $\psi\colon F_4 \to F_2^3$ for which

$$x_0\psi = \langle x_0, x_0, x_0\rangle, \quad x_1\psi = \langle x_1, x_0, x_0\rangle, \quad x_2\psi = \langle x_0, x_1, x_0\rangle, \quad x_3\psi = \langle x_0, x_0, x_1\rangle$$

holds, is surjective. Applying (β), we get

$$(\gamma_4) \qquad \big(m(x_0, m(x_0, f_1(x_0, x_1), f_2(x_0, x_2)), f_3(x_0, x_3))\big)\psi = \\ = \langle f_1(x_0, x_1), f_2(x_0, x_1), f_3(x_0, x_1)\rangle$$

for any binary polynomials f_1, f_2, f_3. Hence ψ is onto, indeed.

Now, let 0 be an arbitrary element of A. Introduce the binary algebraic function $+$ on A, called addition and defined by $a+b=m(0, a, b)$ for all $a, b \in A$. We claim that $\langle A; +\rangle$ is an abelian group of exponent p. Using (β) as well as the isomorphisms φ and ψ it follows

$$m\big(x_0, x_1, m(x_0, x_2, x_3)\big) = \langle x_1, x_1, x_1\rangle\psi^{-1} = m\big(x_0, m(x_0, x_1, x_2), x_3\big)$$

in $\mathbf{F}_4$ and

$$m(x_0, x_1, x_2) = \langle x_0, x_1, x_1\rangle\varphi^{-1} = m(x_0, x_2, x_1)$$

in $\mathbf{F}_3$, implying associativity, resp. commutativity of the addition. From (β) we get $a+0=0+a=a$ for any $a \in A$. Further,

$$m\big(x_0, x_1, m(x_2, x_0, x_0)\big) = \langle x_1, m(x_1, x_0, x_0)\rangle\varphi^{-1} = m(x_2, x_1, x_0)$$

holds in $\mathbf{F}_3$, whence for any $a \in A$ we have $a+m(a, 0, 0)=m(a, a, 0)=0$; i.e., $m(a, 0, 0)$ is the additive inverse for a. Finally, let $a \in A$, $a \neq 0$. Then every element of the subgroup by a in $\langle A; +\rangle$ is contained in the subalgebra $\mathbf{C}$ of $\mathbf{A}$ generated by $\{a, 0\}$. Since $\langle C; +\rangle$ is also a subgroup of $\langle A; +\rangle$ and $|C|=p$, the order of a equals p in $\langle A; +\rangle$, proving our claim.

For arbitrary $a, b, c \in A$,

$$(\delta) \qquad m(a, b, c) = -a+b+c$$

holds. Indeed, let $\theta\colon F_4 \to A$ the homomorphism for which $x_0\theta=0$, $x_1\theta=a$, $x_2\theta=b$, $x_3\theta=c$. Then, using (γ_4), we get

$$m(a, b, c) = \big(m(x_1, x_2, x_3)\big)\theta = \langle m(x_1, x_0, x_0), x_1, x_1\rangle\psi^{-1}\theta = \\ = \big(m(x_0, m(x_0, m(x_1, x_0, x_0), x_2), x_3)\big)\theta = -a+b+c.$$

In view of (δ) and Lemma 1 in [6], $\langle A; m\rangle$ is equivalent to an affine space over $GF(p)$.

The completing step is to prove that $\langle A; f\rangle$ is equivalent to $\langle A; m\rangle$. For this aim, it suffices to show that f is a polynomial of $\langle A; m\rangle$. Assume first that f is binary. The binary polynomials $q_0, \ldots, q_{p-1}$ of A, defined by $q_0 = e_1^2$ (i.e., the second binary projection) and $q_k = m(e_0^2, q_{k-1}, e_1^2)$ for $k > 0$, are, by definition, polynomials of $\langle A; m\rangle$, too. Moreover, they are pairwise different, since, by (δ), for any $a, b \in A$ and $k = 0, \ldots, p-1$ the equality $q_k(a, b) = -ka + (k+1)b$ holds. But **A** has exactly p binary polynomials, whence $f = q_i$ follows for some i $(0 \leqq i < p)$. Thus, f is a polynomial of $\langle A; m\rangle$. Finally, let f be n-ary with $2 < n \leqq 4$. Then (γ_n) shows that f is generated by m and some binary polynomials of **A**. Just we saw, however, that binary polynomials of **A** are generated by m. Hence, f is a polynomial of $\langle A; m\rangle$, q.e.d.

Remarks. 1. Our theorem is not a generalization of the Grätzer—Padmanabhan theorem, because the last one contains no assumption on the power of subalgebras in **A**. In fact, groupoids satisfying (3,1)—(3,4) cannot have two-element subgroupoids, as the identity (15) in [5] shows. In other words, (3,1)—(3,4) together imply (3*) for any groupoid **A**. It is an open problem whether (p*) follows from (p, 1)—(p, 4) for some (possibly for all) primes $p > 3$.

2. The method we used allows some minor generalizations of our theorem. Thus, we can take any algebra $\langle A; F\rangle$ instead of $\langle A; f\rangle$ where the arities of operations from F do not exceed 4. Moreover, if we require (p, k) for $k = 0, \ldots, n$ then it suffices to assume that all operations from F are at most n-ary. Hence it follows that an arbitrary algebra **A** satisfying (p*) and (p, k) for every non-negative integer k, is equivalent to an affine space over $GF(p)$.

References

[1] G. GRÄTZER, *Universal Algebra*, Van Nostrand (1968).

[2] S. MAC LANE—G. BIRKHOFF, *Algebra* Macmillan (1967).

[3] B. CSÁKÁNY, Varieties of affine modules, *Acta Sci. Math.*, **37** (1975), 3—10.

[4] G. GRÄTZER, Composition of functions, *Proc. Conf. on Universal Algebra*, pp. 1—106, Queen's Univ. (Kingston, Ont., 1970).

[5] G. GRÄTZER—R. PADMANABHAN, On idempotent, commutative and nonassociative groupoids *Proc. Amer. Math. Soc.*, **28** (1971), 75—80.

[6] J. PŁONKA, On the arity of idempotent reducts of groups, *Coll. Math.*, **21** (1970), 35—37.

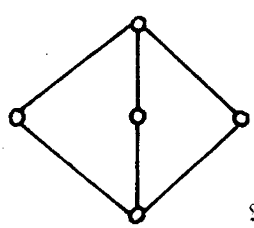
[7] K. URBANIK, On algebraic operations in idempotent algebras, *Coll. Math.*, **13** (1965), 129—157.

(Received November 24, 1973)

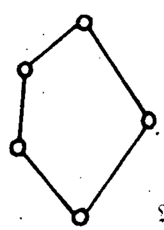
Equational classes which cover the class of distributive lattices

By E. FRIED in Budapest

Introduction. It is well-known that there are exactly two equational classes of lattices which cover the class of all distributive lattices. These are the classes generated by $\mathfrak{M}_5$ and by $\mathfrak{N}_5$ (see Fig. 1) and one of them is always contained in any equational class of lattices containing properly the class of all distributive lattices.



$\mathfrak{M}_5$



$\mathfrak{N}_5$

Fig. 1

The class of *weakly associative lattices* (in short: WALs) contains two other equational classes which also cover the class of all distributive lattices.

It has been a conjecture since the introduction of WALs in 1970, that there are no other equational classes of WALs which cover the class of all distributive lattices. The aim of this paper is to prove the existence of an equational class of WALs different from the class of all distributive lattices which does not contain the four equational classes in question.

Preliminaries. An algebra $\mathfrak{A}=\langle A; \vee, \wedge\rangle$ is a WAL if the two binary operations are idempotent and commutative and over the two absorption identities the two weak associativities hold:

$$\{(x\vee z)\wedge(y\vee z)\}\wedge z = \{(x\wedge z)\vee(y\wedge z)\}\vee z = z.$$

The relations $x=x\wedge y$ and $y=x\vee y$ are equivalent and will be denoted by $x\leqq y$ ($x<y$ means $x\leqq y$ and $x\neq y$). The relation $\leqq$ is reflexive and antisymmetrical and

$x \vee y$ and $x \wedge y$ are the least upper bound and the greatest lower bound of x and y, respectively. In such a way one can define WALs just as lattices in the transitive case. We shall denote $a < b$ by an arrow which goes from a to b.

Fig. 2 shows two WALs both of which are subdirectly irreducible. They are typical, for they show the two possibilities when $a < b < c$ does not imply $a < c$. It is not to hard to prove that both of the equational classes generated by them cover the class of all distributive lattices.

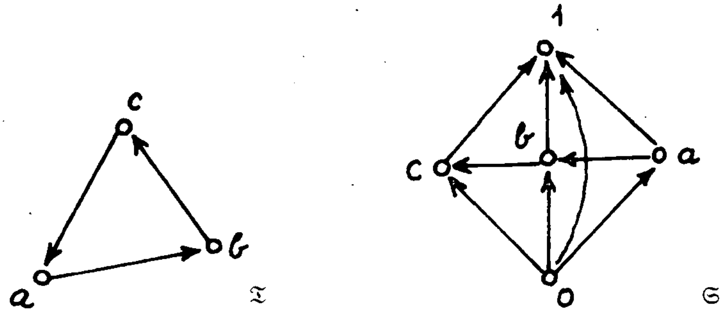


Fig. 2

A WAL $\mathfrak{A} = \langle A; \vee, \wedge \rangle$ has the unique bound property (further on UBP) if, for different $a, b \in A$, $a \leqq c$ and $b \leqq c$ imply $c = a \vee b$, and $d \leqq a$ and $d \leqq b$ imply $d = a \wedge b$. It was proven in [2] that $\mathfrak{A}$ has the UBP if and only if it is subdirectly irreducible and it satisfies the congruence extension property if and only if each subalgebra of $\mathfrak{A}$ is a simple one.

The construction of the desired class. For the construction we need two propositions.

Proposition 1. *There exists a* WAL *having the* UBP *and containing none of* $\mathfrak{M}_5$, $\mathfrak{N}_5$, $\mathfrak{T}$ *and* $\mathfrak{S}$.

Proof. Let Q be the field of rationals and let α be a zero of the irreducible polynomial $f(x) = x^3 + 3x + 1$. Let us denote by $a\alpha^2 + b\alpha + c$ the element (a, b, c) of the two-dimensional projective plane over Q $(a, b, c \in Q)$. Let, for $\beta, \gamma \in Q(\alpha)$, $\beta > \gamma$ mean the existence of a linear polynomial $r(x)$ over Q such that $\beta = \gamma \cdot r(\alpha)$. It was proven in [3] that in this manner we arrive at a WAL $\mathfrak{A}$ satisfying UBP. Thus, $\mathfrak{A}$ cannot contain a three-element chain, i.e., $\mathfrak{A}$ does not contain any of $\mathfrak{M}_5$, $\mathfrak{N}_5$, and $\mathfrak{S}$. $f'(x) = 3x^2 + 3 > 0$ implies that $x^3 + 3x + p$ has for no rational p two, hence three, rational roots. Let, now, $\beta < \gamma < \delta < \varepsilon$ in $Q(\alpha)$, i.e., $\varepsilon = \beta \cdot r_1(\alpha) \cdot r_2(\alpha) \cdot r_3(\alpha)$, where the $r_i(x)$-s are linear polynomials over Q. As $x^3 + 3x + p$ is never a product of three linear factors over Q the element $r_1(\alpha) \cdot r_2(\alpha) \cdot r_3(\alpha)$ does not belong to Q.

Hence, β and ε are different elements of the projective plane, i.e., $\mathfrak{A}$ does not contain $\mathfrak{T}$, either.

Remark. This method does not work more for finite fields. Let a, b, and c be elements of the finite field K. The polynomial $f(x)=x^3+ax^2+bx+c$ orders to each element u of K the element $f(u)$ of K. If $f(u)$ runs over K then $f(x)+v$ is for no v in K irreducible. When the method gives us a WAL then $f(x)$ must be irreducible. Hence, in this case there must exist different u_1, u_2 in K such that $f(u_1)=f(u_2)=v$. Thus, the polynomial $f(x)-v$ is the product of three linear polynomials, say $r_1(x)$, $r_2(x)$, $r_3(x)$, i.e., for the zero α of $f(x)$ we have $1<r_1(\alpha)<r_1(\alpha)\cdot r_2(\alpha)<r_1(\alpha)\cdot r_2(\alpha)\cdot r_3(\alpha)=v$. Since 1 and v are the same points of the projective plane this WAL must contain $\mathfrak{T}$.

Let $\mathfrak{A}$ be a WAL satisfying UBP and not containing any subalgebra isomorphic to $\mathfrak{T}$. These two properties mean that for the elements $a<b<c$ in $\mathfrak{A}$ the elements a and c are incomparable, i.e., neither $a\leqq c$ nor $c\leqq a$ are valid. Such a WAL we shall call a *scattering* WAL.

Proposition 2. *Homomorphic images, subalgebras and primeproducts of scattering* WALs *are scattering, too.*

Proof. The first statement is implied by the simpleness of scattering WALs. The second statement is obvious. Since the class of scattering WALs is a first order class, the third statement is also valid.

Theorem. *The equational class generated by the scattering* WALs *does not contain any of the given four classes.*

Proof. It was proven in [1] that the congruence-lattice of any WAL is a distributive one. The homomorphic images of subalgebras of primeproducts of scattering WALs are, by Proposition 2, scattering WALs. Thus, applying the well-known result of Jónsson (Theorem 3.3 in [5]) we have that the equational class in question does not contain other subdirectly irreducible WALs. Since $\mathfrak{M}_5$, $\mathfrak{N}_5$, $\mathfrak{T}$ and $\mathfrak{S}$ are subdirectly irreducible the theorem is proven.[1])

Problems. The theorem, of course, does not mean the existence of a new equational class covering the class of distributive lattices. It is possible that this class is not covered by any equational subclass of the constructed above. We state some problems concerning this question.[2])

---

[1]) This proof was shortened by W. A. Lampe in Honolulu.

[2]) In the meantime, Problem 1 was solved by R. Freese in Honolulu. The lattice of the equational classes of WALs is dual to an algebraic lattice. Since the class of distributive lattices is finitely based this class is a compact element of the lattice of classes. Thus, each maximal chain between the class of all distributive lattices and of all scattering WALs contains an element which covers the class of all distributive lattices. Hence, the existence of a fifth covering class is proven.

1. Is there any scattering WAL $\mathfrak{A}$ having no nontrivial subalgebra which is not isomorphic to $\mathfrak{A}$?

2. Are there any finite scattering WALs? (The existence of such a WAL would imply that the answer of problem 1 is affirmative.)

3. Is there any equational class of WALs different from the class of all distributive lattices which does not contain either scattering WALs or any of the given four WALs?

References

[1] E. Fried, Tournaments and nonassociative lattices, *Ann. Univ. Sci. Budapest*, Sect. Math., 13 (1970), 151—164.
[2] E. Fried, Subdirect irreducible weakly associative lattices with congruence extension property, *Ann. Unio. Sci Budapest*, Sect. Math., **17** (1974), 59—68.
[3] E. Fried—V. T. Sós, Weakly associative lattices and projective planes *Algebra Universalis*, **5** (1975), 62—67.
[4] G. Grätzer, *Lattice theory, first concepts and distributive lattices*, Freeman and Co. (1971).
[5] B. Jónsson, Algebras whose congruence lattices are distributive, *Math. Scand.*, **21** (1967), 110—121.

(Received April 24, 1974)

Результантная матрица и ее обобщения
I. Результантный оператор матричных полиномов

И. Ц. ГОХБЕРГ и Г. ХАЙНИГ (Кишинев, СССР)

Пусть $a(\lambda)=a_0+a_1\lambda+\dots+a_n\lambda^n$ и $b(\lambda)=b_0+b_1\lambda+\dots+b_m\lambda^m$ — два полинома с коэффициентами из $\mathbf{C}^1$. Результантом этих полиномов называется определитель следующей матрицы:

$$R(a,b)=\begin{bmatrix} a_0 & a_1 & \dots & a_n & \dots & & \\ & a_0 & a_1 & \dots & a_n & \dots & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & \dots & & \\ & b_0 & b_1 & \dots & b_m & \dots & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & & b_0 & b_1 & \dots & b_m \end{bmatrix}\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \end{matrix}$$

Как известно,

$$\det R(a,b)=a_n^n b_m^m \prod_{j=1}^{n}\prod_{k=1}^{m}(\lambda_j(a)-\lambda_k(b)),$$

где $\lambda_j(a)$ $(j=1,2,\dots,n)$ — полный набор корней полинома $a(\lambda)$. В частности, полиномы $a(\lambda)$ и $b(\lambda)$ имеют хотя бы один общий корень в том и только том случае, когда результант $\det R(a,b)$ обращается в нуль (см., например, [1]). Известен следующий более полный результат (см., например, [2, 3]): число общих корней многочленов $a(\lambda)$ и $b(\lambda)$ (с учетом их кратности) равно числу $m+n-\operatorname{rang} \mathrm{R}(a,b)$. Эта связь непосредственно вытекает из следующего предложения.

Теорема 0. 1. *Пусть $\lambda_l(l=1,2,\dots,l_0)$ — все различные общие корни полимонов $a(\lambda)$ и $b(\lambda)$ и k_l — кратность общего корня λ_l.*

Тогда система векторов

$$H_k(\lambda_l)=\left(\binom{p}{k}\lambda_l^{p-k}\right)_{p=0}^{m+n-1}\quad (\in \mathbf{C}^{m+n};\ l=1,2,\dots,l_0;\ k=0,1,\dots,k_l-1)$$

образует базис подпространства $\operatorname{Ker} R(a, b)$, *в частности,*

$$\sum_{l=0}^{l_0} k_p = \dim \operatorname{Ker} R(a, b). \tag{0.1}$$

В настоящей статье устанавливаются различные обобщения этой теоремы.

В первой части этой статьи исследуется результантный оператор для матричных полиномов. В отличие от скалярного случая оказалось, что этот оператор как правило определяется прямоугольной матрицей.

Эта часть состоит из пяти параграфов. Первые два носят вспомогательный характер. В третьем доказывается основная теорема, из которой, в частности, вытекает теорема 0.1. В четвертом и пятом параграфах приводятся примеры приложений основной теоремы.

Во второй части статьи будут изложены континуальные аналоги результатов этой статьи.

Авторы начали эти исследования под влиянием бесед с М. Г. Крейном. М. Г. Крейн любезно обратил внимание авторов на связи, существующие между кругом этих вопросов и результатами об обращении конечных теплицевых матриц и их континуальных аналогов [4, 5].

Авторы приносят М. Г. Крейну искреннюю благодарность.

§ 1. Лемма о кратных расширениях систем векторов

1. Пусть L обозначает некоторое линейное пространство и L^m — линейное пространство всех векторов вида $f=(f_j)_{j=0}^{m-1}$ с компонентами $f_j \in L$. Пусть $\mathfrak{F}=\{\varphi_{jk}: k=0, 1, \ldots, k_j-1; j=1, 2, \ldots, j_0\}$ — система векторов из L и λ_0 — некоторое комплексное число. Систему векторов

$$\mathfrak{F}^m(\lambda_0) = \{\Phi_{jk}(\lambda_0)\colon k = 0, 1, \ldots, k_j-1; j = 1, 2, \ldots, j_0\} \text{ из } L^m, \text{ где}$$

$$\Phi_{jk}(\lambda_0) = \left(\varphi_{jk}^p(\lambda_0)\right)_{p=0}^{m-1} \quad \text{и} \quad \varphi_{jk}^p(\lambda_0) = \sum_{s=0}^{p} \binom{p}{s} \lambda_0^{p-s} \varphi_{j,k-s} \tag{1.1}$$

назовем m-кратным расширением системы $\mathfrak{F}$ относительно λ_0. Легко видеть, что для векторов $\Phi_{jk}(\lambda_0)$ имеют место равенства

$$\varphi_{jk}^p(\lambda_0) = \frac{d^p}{dt^p} e^{\lambda_0 t} \left(\varphi_{jk} + \frac{t}{1!} \varphi_{j,k-1} + \ldots + \frac{t^k}{k!} \varphi_{j0}\right)\Bigg|_{t=0}. \tag{1.2}$$

Имеет также место следующая рекуррентная формула:

$$\varphi_{jk}^{p+1}(\lambda_0) = \lambda_0 \varphi_{jk}^p(\lambda_0) + \varphi_{jk-1}^p(\lambda_0) \quad (k = 0, 1, \ldots, k_j-1;\ j = 1, 2, \ldots, j_0), \tag{1.3}$$

в которой полагается $\varphi^p_{j,-1}(\lambda_0)=0$. В самом деле, из равенства (1.1) вытекает, что

$$\varphi^{p+1}_{jk}(\lambda_0)-\lambda_0\varphi^p_{jk}(\lambda_0)=\sum_{s=0}^{p+1}\left(\binom{p+1}{s}\lambda_0^{p-s+1}\varphi_{j,k-s}(\lambda_0)-\binom{p}{s}\lambda_0^{p-s+1}\varphi_{j,k-s}(\lambda_0)\right)$$
$$=\sum_{s=0}^{p+1}\binom{p}{s-1}\lambda_0^{p-s+1}\varphi_{j,k-s}(\lambda_0).$$

Таким образом,

$$\varphi^{p+1}_{jk}(\lambda_0)-\lambda_0\varphi^p_{jk}(\lambda_0)=\sum_{s=0}^{p}\binom{p}{s}\lambda_0^{p-s}\varphi_{j,k-1-s}(\lambda_0)=\varphi^p_{j,k-1}(\lambda_0).$$

Из формулы (1.3) без труда выводится следующая более общая формула:

(1.4) $$\varphi^{p+r}_{jk}(\lambda_0)=\sum_{s=0}^{p}\binom{r}{s}\lambda_0^{r-s}\varphi^p_{j,k-s}(\lambda_0)\quad(r=1,2,\ldots).$$

В самом деле, для $r=1$ формула (1.4) совпадает с (1.3). Пусть равенство (1.4) верно. Тогда

$$\varphi^{p+r+1}_{jk}(\lambda_0)=\lambda_0\varphi^{p+r}_{jk}(\lambda_0)+\varphi^{p+r}_{j,k-1}(\lambda_0)=$$
$$=\sum_{s=0}^{r}\left(\binom{r}{s}\lambda_0^{r+1-s}\varphi^p_{j,k-s}(\lambda_0)-\binom{r}{s-1}\lambda_0^{r+1-s}\right)\varphi_{j,k-s}(\lambda_0)$$

и, следовательно,

$$\varphi^{p+r+1}_{jk}(\lambda_0)=\sum_{s=0}^{r+1}\binom{r+1}{s}\lambda_0^{r+1-s}\varphi^p_{j,k-s}(\lambda_0).$$

2. В дальнейшем существенную роль играет следующее предложение.

Лемма 1.1. *Пусть* $\Lambda=\{\lambda_1,\lambda_2,\ldots,\lambda_l\}$ *— система различных комплексных чисел и* $\mathfrak{F}_l$ $(l=1,2,\ldots,l_0)$ *— системы векторов из* L:

$$\mathfrak{F}_l=\{\varphi_{jk,l}\colon k=0,1,\ldots,k_{jl}-1;\ j=1,2,\ldots,j_l\}.$$

Если при каждом $l=1,2,\ldots,l_0$ *система векторов* $\varphi_{j0,l}$ $(j=1,2,\ldots,j_l)$ *линейно независима и число* m *удовлетворяет условию*

(1.5) $$m\geqq\sum_{l=1}^{l_0}\max_{j=1,2,\ldots,j_l}k_{jl}$$

то система векторов

$$\mathfrak{F}^m(\Lambda)=\bigcup_{l=1}^{l_0}\mathfrak{F}^m_l(\lambda_l)\,^{1)}$$

является также линейно независимой.

---

[1]) Здесь и в дальнейшем мы через $\bigcup_{l=1}^{l_0}\mathfrak{F}^m_l(\lambda_l)$ обозначим систему (!)

$$\{\Phi_{jk,l}(\lambda_l)\colon k=0,1,\ldots,k_{jl}-1;\ j=1,2,\ldots,j_l;\ l=1,2,\ldots,l_0\}.$$

Доказательство. Очевидно, в доказательстве достаточно ограничиться случаем, когда

$$m = \sum_{l=1}^{l_0} \max_{j=1,2,\ldots,j_l} k_{jl}.$$

Введем в рассмотрение операторные матрицы

$$\Pi_r(\lambda) = \|\pi_{st}^r I\|_{s,t=1}^{m-1} \quad (r = 0, 1, \ldots, m-1)$$

где

$$\pi_{st}^r = \begin{cases} \delta_{st} & (s \leqq r) \\ (-\lambda)^{s-t}\begin{pmatrix} s-r \\ t-r \end{pmatrix} & (s > r) \end{cases}$$

и I — единичный оператор в пространстве L. Выясним теперь, как оператор $\Pi_r(\lambda)$ действует на векторы $\Phi_{jk}(\lambda_l) = (\varphi_{jk,l}^p(\lambda_l))_{p=0}^{m-1}$ системы $\mathfrak{F}^m(\Lambda)$. В первую очередь отметим, что оператор $\Pi_r(\lambda)$ не меняет первые $r+1$ компоненты вектора $\Phi_{jk,l}(\lambda_l)$.

Рассмотрим системы векторов

(1.6) $\quad \mathfrak{G}_r^m(\lambda, \lambda_l) = \{P_r\Pi_r(\lambda)\Phi_{jk,l}(\lambda_l)\colon k = 0, 1, \ldots, k_{jl}-1;\ j = 1, 2, \ldots, j_l\}$

где

$$P_r = \underbrace{\begin{bmatrix} 0 \ldots 0 & I & 0 \\ \vdots \quad\ \vdots & & \ddots \\ 0 \ldots 0 & 0 & I \end{bmatrix}}_{m} \Big\} m-r,$$

$$l = 1, 2, \ldots, l_0 \quad \text{и} \quad r = 0, 1, \ldots, m-1.$$

Докажем, что каждая из этих систем векторов является $(m-r)$ — кратным расширением относительно $\lambda_l - \lambda$ соответствующей системы векторов

$$\mathfrak{G}_r(\lambda_l) = \{\varphi_{jk,l}^r(\lambda_l)\colon k = 0, 1, \ldots, k_{jl}-1;\ j = 1, 2, \ldots, j_l\}.$$

Положим

$$(\psi_{jk,l}^p)_{p=0}^{m-1-r} = P_r\Pi_r(\lambda)\Phi_{jk,l}(\lambda_l).$$

Тогда

$$\psi_{jk,l}^p = \sum_{s=r}^{p+r}(-\lambda)^{p+r-s}\begin{pmatrix} p \\ s-r \end{pmatrix}\varphi_{jk,l}^s(\lambda_l) = \sum_{u=0}^{p}(-\lambda)^u\begin{pmatrix} p \\ u \end{pmatrix}\varphi_{jk,l}^{p+k-u}(\lambda_l).$$

В силу (1.4)

$$\varphi_{jk,l}^{p-u+r}(\lambda_l) = \sum_{s=0}^{p-u}\lambda_l^{p-u-s}\begin{pmatrix} p-u \\ s \end{pmatrix}\varphi_{j,k-s,l}^r(\lambda_l),$$

следовательно,

$$\psi_{jk,l}^p = \sum_{u=0}^{p}\sum_{s=0}^{p-u}\lambda_l^{p-u-s}(-\lambda)^u\begin{pmatrix} p \\ u \end{pmatrix}\begin{pmatrix} p-u \\ s \end{pmatrix}\varphi_{j,k-s,l}^r.$$

Учитывая, что

$$\binom{p-u}{s}\binom{p}{u}=\binom{p-s}{u}\binom{p}{s}$$

получим

$$\psi^p_{jk,l}=\sum_{s=0}^{p}\sum_{u=0}^{p-s}\lambda_l^{p-u-s}(-\lambda)^u\binom{p-s}{u}\binom{p}{s}\varphi^r_{j,k-s,l}(\lambda_l).$$

Таким образом,

$$\psi^p_{jk,l}=\sum_{s=0}^{p}(\lambda_l-\lambda)^{p-s}\binom{p}{s}\varphi^r_{j,k-s,l}(\lambda_l);$$

Последнее и означает, что система векторов $\mathfrak{G}^m_r(\lambda,\lambda_l)$ является $(m-r)$-кратным расширением системы $\mathfrak{G}^m_r(\lambda,\lambda_l)$ относительно $\lambda_l-\lambda$.

Рассмотрим систему $\mathfrak{F}^{(1)}_m(\lambda_l)$ векторов

$$\Phi^{(1)}_{jk}(\lambda_l)=\Pi_0(\lambda)\,\Phi_{jk,l}(\lambda_l)\quad (k=0,1,\dots,k_{jl}-1;\, j=1,2,\dots,j).$$

Из предыдущих рассуждений вытекает, что система $\mathfrak{F}^{(1)}_m(\lambda_l)$ представляет собой m-кратное расширение системы $\mathfrak{F}_l$ $(l=1,2,\dots,l_0)$ относительно $\lambda_l-\lambda_1$. В частности, векторы $\Phi^{(1)}_{jk}(\lambda_1)$ имеют вид

$$\Phi^{(1)}_{jk}(\lambda_1)=\begin{bmatrix}\varphi_{jk,1}\\ \vdots\\ \varphi_{j0,1}\\ 0\\ \vdots\\ 0\end{bmatrix}\quad (k=0,1,\dots,k_{j1}-1;\ j=1,2,\dots,j_1).$$

Образуем теперь систему $\mathfrak{F}^{(2)}_m(\lambda_l)$ векторов $\Phi^{(2)}_{jk}(\lambda_l)=\Pi_{\varkappa_1}(\lambda_2-\lambda_1)\,\Phi^{(1)}_{jk}(\lambda_l)$ $(k=0,1,\dots,k_{jl}-1;\, j=1,2,\dots,l_0)$, где $\varkappa_1=\max\limits_{j=1,2,\dots,j_1}k_{j1}$. Тогда система векторов $P_{\varkappa_1}\Phi^{(2)}_{jk}(\lambda_l)$ представляет собой $(m-\varkappa_1)$-кратное расщирение векторов $\varphi^{\varkappa_1}_{jk,l}(\lambda_l-\lambda_1)$ относительно $\lambda_l-\lambda_1-(\lambda_2-\lambda_1)=\lambda_l-\lambda_2$. В частности, $P_{\varkappa_1}\Phi^{(2)}_{jk}(\lambda_1)=0$, а векторы $P_{\varkappa_1}\Phi^{(2)}_{jk}(\lambda_2)$ имеют вид

$$P_{\varkappa_1}\Phi^{(2)}_{jk}(\lambda_2)=\begin{bmatrix}*\\ \vdots\\ *\\ (\lambda_2-\lambda_1)^{\varkappa_1}\varphi_{jk,2}\\ 0\\ \vdots\\ 0\end{bmatrix}\leftarrow k$$

где звездочкой заменены векторы, которые в дальнейшем не играют роли.

Продолжим этот процесс так далее: по системе $\mathfrak{F}^{(s)}_m(\lambda_l)$ векторов $\Phi^{(s)}_{jk}(\lambda_l)$ $(k=0,1,\dots,k_{jl}-1;\ j=1,\dots,j_l)$ построим систему $\mathfrak{F}^{(s+1)}_m(\lambda_l)$ векторов $\Phi^{(s+1)}_{jk}(\lambda_l)=$

$=\Pi_{\varkappa_s}(\lambda_{s+1}-\lambda_s)\Phi_{jk}^{(s)}$, где $\varkappa_s=\sum_{l=1}^{s}\max_{j=1,2,\ldots,j_s}k_{jl}$. Для векторов $P_{\varkappa_s}\Phi_{jk}^{(s+1)}(\lambda_l)$, где $l=1, 2, \ldots, s$, имеют место равенства $P_{\varkappa_s}\Phi_{jk}^{(s+1)}(\lambda_l)=0$, а векторы $P_{\varkappa_s}\Phi_{jk}^{(s+1)}(\lambda_{s+1})$ имеют вид

$$\begin{bmatrix} * \\ \vdots \\ * \\ (\lambda_{s+1}-\lambda_s)^{\varkappa_s}\varphi_{jk,s+1} \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow k \quad (k=0, 1, \ldots, k_{j,s+1}-1;\ j=1, 2, \ldots, j_{s+1}).$$

Наконец, построим системы $\mathfrak{F}_m^{(l_0)}(\lambda_l)$ $(l=1, 2, \ldots, l_0)$. Для векторов этой системы $P_{\varkappa_{l_0-1}}\Phi_{jk}^{(l_0)}(\lambda_l)=0$ при $l\neq l_0$, а векторы $P_{\varkappa_{l_0-1}}\Phi_{jk}^{(l_0)}(\lambda_{l_0})$ имеют вид

$$\begin{bmatrix} * \\ \vdots \\ * \\ (\lambda_{l_0}-\lambda_{l_0-1})^{\varkappa_{l_0-1}}\varphi_{jk,l_0} \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow k \tag{1.7}$$

Докажем теперь, что система векторов

$$\mathfrak{F}_m^{(l_0)}(\Lambda) \doteq \bigcup_{l=1}^{l_0}\mathfrak{F}_m^{(l_0)}(\lambda_l)$$

линейно независима. Пусть

$$\sum_{l=1}^{l_0}\sum_{j=1}^{j_l}\sum_{k=0}^{k_{jl}-1}\alpha_{jkl}\Phi_{jk}^{(l_0)}(\lambda_l)=0.$$

Тогда

$$\sum_{j,k,l}\alpha_{jkl}P_{\varkappa_{l_0-1}}\Phi_{jk}^{(l_0)}(\lambda_l)=\sum_{j=1}^{j_{l_0}}\sum_{k=0}^{k_{jl}-1}\alpha_{jkl_0}P_{\varkappa_{l_0-1}}\Phi_{jk}^{(l_0)}(\lambda_{l_0})=0.$$

Так как векторы $P_{\varkappa_{l_0-1}}\Phi_{jk}^{(l_0)}(\lambda_{l_0})$ имеют вид (1.7) и векторы φ_{j0,l_0} $(j=1, 2, \ldots, j_l)$ линейно независимы, то

$$\alpha_{jkl_0}=0 \quad (k=0, 1, \ldots, k_{jl_0}-1;\ j=1, 2, \ldots, j_{l_0}).$$

Таким образом,

$$\sum_{l=1}^{l_0-1}\sum_{j=1}^{j_l}\sum_{k=0}^{k_{jl}-1}\alpha_{jkl}\Phi_{jk}^{(l_0)}(\lambda_l)=0.$$

Применяя к этому равенству оператор $P_{\varkappa_{l_0-2}}$, получим, что $\alpha_{jk,l_0-1}=0$ $(k=0, 1, \dots, k_{jl_0-1}-1; j=1, \dots, j_{l_0-1})$. Продолжая этот процесс аналогичным образом, получим, что $\alpha_{jks}=0$ $(k=0, 1, \dots, k_{js}-1; j=1, 2, \dots, j_s)$ для $s=l_0-2, l_0-3, \dots, 1$. Из линейной независимости системы $\mathfrak{F}_m^{(l_0)}(\Lambda)$ вытекает линейная независимость системы $\mathfrak{F}^m(\Lambda)$.

Лемма доказана.

Без труда можно убедиться в том, что даже в случае $L=\mathbf{C}^1$ условие (1.5) существенно в формулировке леммы 1.1.

3. Из леммы 1.1 выводится следующая

Лемма 1.2. *Пусть $\Lambda=\{\lambda_1, \lambda_2, \dots, \lambda_{l_0}\}$ — множество комплексных чисел и $\mathfrak{F}_l$ $(l=1, 2, \dots, l_0)$ — система векторов из L:*

$$\mathfrak{F}_l = \{\varphi_{jk,l}\colon k = 0, 1, \dots, k_{jl}-1;\ j = 1, 2, \dots, j_l\}.$$

Если число m удовлетворяет условию (1.5) *и*

$$\sum_{l=1}^{l_0} \sum_{j=1}^{j_l} \sum_{k=0}^{k_{jl}-1} \alpha_{jkl}\Phi_{jk,l}(\lambda_l) = 0 \quad (\alpha_{jkl}\in\mathbf{C}^1), \tag{1.6}$$

то

$$\Phi_{k,l}(\lambda_l) = \sum_j \alpha_{jkl}\Phi_{jk,l}(\lambda_l) = 0 \quad (k = 0, 1, \dots, \max_j k_{jl}-1;\ l = 1, 2, \dots, l_0),$$

где суммирование распространяется на все индексы j, для которых $k_{jl}\geqq k$.

Доказательство. Образуем систему

$$\mathfrak{G}_l = \Big\{\varphi_{k,l} = \sum_j \alpha_{jkl}\varphi_{jk,l}\colon \varphi_{0,l}\neq 0;\ k = 0, 1, \dots, \max_j k_{jl}-1\Big\} \quad (l = 1, 2, \dots, l_0)$$

и предположим, что она непуста. Тогда, очевидно, система $\mathfrak{G}_l^m=\{\Phi_{k,l}(\lambda_l)\colon k=0, 1, \dots, \max_j k_{jl}-1\}$ является m-кратным расширением системы $\mathfrak{G}_l$. Применяя к системе $\mathfrak{G}=\bigcup_{l=1}^{l_0}\mathfrak{G}_l$ лемму 1.1, получим, что система векторов $\Phi_{k,l}(\lambda_l)$ линейно независима. Последнее противоречит равенству (1.7). Таким образом, $\mathfrak{G}_l=\emptyset$, что означает $\varphi_{0,l}=0$ $(l=1, 2, \dots, l_0)$.

Теперь образуем системы

$$\mathfrak{G}_{l,1} = \Big\{\varphi_{k,l}^{(1)} = \varphi_{k+1,l}\colon \varphi_{1,l}\neq 0,\ k = 0, 1, \dots, \max_j k_{jl}-2\Big\} \quad (l = 1, 2, \dots, l_0).$$

Как легко видеть, m-кратное расширение системы $\mathfrak{G}_{l,1}$ состоит из векторов $\Phi_{k+1,l}(\lambda_l)=\Phi_{k,l,1}(\lambda_l)$ $(\varphi_{1,l}\neq 0;\ k=0, \dots, \max_j k_{jl}-2)$. Следовательно, применяя снова лемму 1.1, получим $\mathfrak{G}_{1,l}=\emptyset$, что означает $\varphi_{1,l}=0$ $(l=1, 2, \dots, l_0)$.

Продолжая этот процесс далее, получим $\varphi_{r,l}=0$ $(l=1, 2, \dots, l_0)$ для $r=2, 3, \dots, \max_{j,l} k_{jl}-1$.

Лемма доказана.

§ 2. Вспомогательные предложения

1. Пусть d — натуральное число и $A(\lambda)=A_0+\lambda A_1+\dots+\lambda^n A_n$ матричный пучок с коэффициентами $A_k\in L(\mathbf{C}^d)$. [2]) Всюду в дальнейшем будем предполагать, что матрица A_n обратима.

Число $\lambda_0\in\mathbf{C}^1$ называется характеристическим числом пучка $A(\lambda)$ если $\det A(\lambda_0)=0$. Если для некоторого вектора $\varphi_0\in\mathbf{C}^d$ $(\varphi_0\neq 0)$ имеет место равенство $A(\lambda_0)\varphi_0=0$, то вектор φ_0 называется собственным вектором пучка $A(\lambda)$, отвечающим числу λ_0. Цепочка векторов $\varphi_0, \varphi_1, \dots, \varphi_r$ называется цепочкой (длины $r+1$) из собственного и присоединенных векторов, если имеют место равенства

$$(2.1)\quad A(\lambda_0)\varphi_k+\frac{1}{1!}\left(\frac{d}{d\lambda}A\right)(\lambda_0)\varphi_{k-1}+\dots+\frac{1}{k!}\left(\frac{d^k}{d\lambda^k}A\right)(\lambda_0)\varphi_0=0 \quad (k=0, 1, \dots, r).$$

Пусть λ_0 — характеристическое число пучка $A(\lambda)$. Без труда доказывается, что в ядре матрицы $A(\lambda_0)$ можно построитъ базис $\varphi_{10}, \varphi_{20}, \dots, \varphi_{r0}$ со следующим свойством:

Для каждого вектора φ_{j0} существует цепочка присоединенных векторов $\varphi_{j1}, \varphi_{j2}, \dots, \varphi_{j,k_j-1}$, где $k_1\geqq k_2\geqq\dots\geqq k_r$ и число $k_1+k_2+\dots+k_r$ равно кратности нуля функции $\det A(\lambda)$ в точке λ_0.

Числа k_j $(j=1, 2, \dots, r)$ называются частными кратностями характеристического числа λ_0, а система $\varphi_{j0}, \varphi_{j1}, \dots, \varphi_{j,k_j-1}$ $(j=1, 2, \dots, r)$ — канонической системой собственных и присоединенных векторов пучка $A(\lambda)$, отвечающих характеристическому числу λ_0.

Лемма 2.1. *Пусть $\Lambda=\{\lambda_1, \lambda_2, \dots, \lambda_l\}$ — полный набор всех различных характеристических чисел пучка $A(\lambda)=A_0+\lambda A_1+\dots+\lambda^n A_n$ с коэффициентами $A_k\in L(\mathbf{C}^d)$ и пусть*

$$\mathfrak{F}_l=\{\varphi_{jk,l}\colon k=0, 1, \dots, k_{jl}-1;\ j=1, 2, \dots, j_l\} \quad (l=1, 2, \dots, q)$$

— каноническая система собственных и присоединенных векторов пучка $A(\lambda)$, отвечающих характеристическому числу λ_l.

Тогда при любом натуральном m система [3])

$$\mathfrak{F}^{m+n}(\Lambda)=$$

$$=\bigcup_{l=1}^{l_0}\mathfrak{F}_l^{m+n}(\lambda_l)=\left\{\Phi_{jk,l}(\lambda_l)=\left(\varphi_{jk,l}^p(\lambda_l)\right)_{p=0}^{m-1}\colon j=1, \dots, j_l;\ k=0, \dots, k_{jl}-1\right\}$$

---

[2]) Через $L(\mathbf{C}^d)$ обозначается пространство квадратных матриц порядка d.

[3]) Напомним, что система $\mathfrak{F}^{m+n}(\lambda_l)$ является $(m+n)$-кратным расширением системы $\mathfrak{F}$ относительно λ_l (см. определние в § 1).

является базисом ядра оператора

$$\mathscr{A}_m = \left.\begin{bmatrix} A_0 & A_1 \dots A_n & \dots & 0 \\ \vdots & A_0 \dots A_{n-1} & A_n & \vdots \\ & \ddots & \ddots \quad \ddots & \\ 0 & \dots & A_0 \dots A_{n-1} & A_n \end{bmatrix}\right\} m$$

действующего из $\mathbf{C}^{(m+n)d}$ *в* $\mathbf{C}^{md}$.

Доказательство. Докажем сначала, что равенство

$$\sum_{p=r}^{n+r} A_{p-r}\varphi^p_{jk,l}(\lambda_l) = 0 \quad (j=1, 2, \dots, j_l) \tag{2.2}$$

верно для $k=0$ и любого r. В самом деле, так как $\varphi^p_{j0,l}(\lambda_l) = \lambda_l^p \varphi_{j0,l}$, то

$$\sum_{p=r}^{n+r} A_{p-r}\varphi^p_{j0,l}(\lambda_l) = \sum_{p=r}^{n+r} \lambda_l^p A_{p-r}\varphi_{j0,l} = \lambda_l^r A(\lambda_l)\varphi_{j0,l} = 0.$$

Предположим, что равенство (2.2) верно для любого r и $k=k_0$. Тогда оно верно и для $k=k_0+1$ и любого r. В самом деле, по предположению имеем

$$0 = \sum_{p+r}^{n+r} A_{p-r}\varphi^p_{jk_0,l}(\lambda_l) = \lambda_l \sum_{p=r}^{n+r}\sum_{s=0}^{p}\binom{p}{s}\lambda_l^{p-s}A_{p-r}\varphi_{j,k_0-s,l}$$
$$= \sum_{p=r}^{n+r}\sum_{s=0}^{p}\binom{p}{s-1}\lambda_l^{p-s}A_{p-r}\varphi_{j,k_0+1-s,l}.$$

Отсюда вытекает, что

$$\sum_{p=r}^{n+r} A_{p-r}\varphi^p_{j,k_0+1}(\lambda_0) = \sum_{p=r}^{n+r}\sum_{s=0}^{p}\left(\binom{p}{s}\lambda_l^{p-s}A_{p-r}\varphi_{j,k_0+1-s,l} - \binom{p}{s-1}\lambda_l^{p-s}A_{p-r}\varphi_{j,k_0+1-s,l}\right)$$
$$= \sum_{p=r}^{n+r}\sum_{s=1}^{p-1}\binom{p-1}{s-1}\lambda_l^{p-s}A_{p-r}\varphi_{j,k_0+1-s,l}$$
$$= \sum_{p=r-1}^{n+r-1} A_{p-(r-1)}\varphi^p_{jk_0,l}(\lambda_l) = 0.$$

Таким образом, доказано, что для любого $k=0, 1, \dots, k_{jl}-1$ и любого $r=0, 1, \dots, m-1$ имеет место равенство (2.2). Отсюда вытекает, что $\Phi_{jk,l}(\lambda_l) \in \operatorname{Ker}\mathscr{A}_m$.

Система $\mathfrak{F}^{m+n}(\Lambda)$ состоит из nd векторов. Согласно лемме 1.1 эта система линейно независима. С другой стороны, очевидно,

$$\dim\operatorname{Ker}\mathscr{A}_m = (m+n)d - md = nd.$$

Таким образом, $\operatorname{Ker}\mathscr{A}_m = \operatorname{lin}\mathfrak{F}^{m+n}(\Lambda)$. [4])

Лемма доказана.

---

[4]) Через $\operatorname{lin}\mathfrak{F}$ обозначается линейная оболочка системы векторов $\mathfrak{F}$.

2. Лемма 2.2. *Пусть*

$$\mathfrak{F}_l = \{\varphi_{jk,l}\colon k = 0, 1, \ldots, k_{jl}-1;\ j = 1, 2, \ldots, j_l\} \quad (l = 1, 2, \ldots, q)$$

— система векторов из пространства $\mathbf{C}^d$ *и* $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$ *— конечное множество комплексных чисел. Пусть далее* $\mathfrak{F}_l^{m+n}(\lambda_l)$ $(m+n)$*-кратное расширение системы* $\mathfrak{F}_l$ *относительно* λ_l *и вектор*

$$\Omega = \sum_{l=1}^{q} \sum_{j=1}^{j_l} \sum_{k=0}^{k_{jl}-1} \alpha_{jkl} \Phi_{jk,l}(\lambda_l) \quad (\in \mathbf{C}^{(m+n)d}),$$

где $\alpha_{jkl} \in \mathbf{C}^1$ *принадлежит ядру оператора* $\mathscr{A}_m$. *Если число* m *удовлетворяет условию*

$$m \geqq \sum_{l=1}^{q} \max_j k_{jl},\ ^{5})$$

то все векторы

$$\Omega_{k,l} = \sum_j \alpha_{jkl} \Phi_{jk,l}(\lambda_l) \quad (k = 0, 1, \ldots, \max k_{jl} - 1;\ l = 1, \ldots, q) \tag{2.3}$$

где суммирование распространяется на все индексы j, *для которых* $k_{jl} \geqq k$ *принадлежат ядру оператора* $\mathscr{A}_m$.

Доказательство. Положим

$$\psi_{jk,l} = \sum_{p=0}^{n} A_p \varphi^p_{jk,l}(\lambda_l),$$

$$\mathfrak{G}_l = \{\psi_{jk,l}\colon j = 1, 2, \ldots, j_l;\ k = 0, 1, \ldots, k_{jl}-1\} \quad (l = 1, 2, \ldots, q)$$

и

$$\tilde{\Psi}_{jk,l} = (\psi^p_{jk,l})_{p=0}^{m-1} \overset{\text{def}}{=} \mathscr{A}_m \Phi_{jk,l}(\lambda_l).$$

Докажем, что система $\tilde{\mathfrak{G}}_l = \{\tilde{\Psi}_{jk,l}\colon k=0, 1, \ldots, k_{jl}-1;\ l=1, 2, \ldots, q\}$ представляет собой m-кратное расширение отностительно λ_l системы $\mathfrak{F}_l$, т.е. $\mathfrak{F}_l^m(\lambda_l) = \tilde{\mathfrak{G}}_l$.

Имеет место равенство

$$\psi^s_{jk,l} = \sum_{p=s}^{s+n} A_{p-s} \varphi^p_{jk,l}(\lambda_l) = \sum_{p=0}^{n} A_p \varphi^{p+s}_{jk,l}(\lambda_l).$$

В силу (1.4)

$$\varphi^s_{jk,l} = \sum_{p=0}^{n} \sum_{u=0}^{s} \binom{s}{u} \lambda_l^{s-u} \varphi^p_{j,k-u,l}(\lambda_l).$$

Следовательно,

$$\psi^s_{jk,l} = \sum_{p=0}^{n} \sum_{u=0}^{s} \binom{s}{u} \lambda_l^{s-u} A_p \varphi^p_{j,k-u,l}(\lambda_l) = \sum_{u=0}^{s} \binom{s}{u} \lambda_l^{s-u} \psi_{j,k-u,l}.$$

Отсюда вытекает, что $\tilde{\psi}^s_{jk,l} = \psi^s_{jk,l}(\lambda_l)$ и $\tilde{\Psi}_{jk,l} = \Psi_{jk,l}(\lambda_l)$.

---

[5]) Отметим, что это условие заведомо выполняется, если $m \geqq nd$.

Пусть

$$\Omega = \sum_{l=1}^{q} \sum_{j=1}^{j_l} \sum_{k=0}^{k_{jl}-1} \Phi_{jk,l}(\lambda_l) \in \operatorname{Ker} \mathcal{A}_m.$$

Тогда

$$\mathcal{A}_m \Omega = \sum_{l=1}^{q} \sum_{j=1}^{j_l} \sum_{k=0}^{k_{jl}-1} \alpha_{jkl} \tilde{\Psi}_{jk,l}.$$

В силу леммы 1.2 отсюда вытекает

$$\sum_j \alpha_{jkl} \tilde{\Psi}_{jk,l} = 0 \quad (k = 0, 1, \dots, k_{jl}-1;\ l = 1, 2, \dots, q),$$

где, суммирование происходит по всем j, для которых $k_{jl} \geqq k$.

Лемма доказана.

Отметим, что в условиях леммы 2.2 может оказаться, что все векторы $\Phi_{jk,l}(\lambda_l)$ не принадлежат ядру оператора $\mathcal{A}_m$ для любого m. В этом можно убедиться на следующем примере.

Рассмотрим при $d=2$ пучок $A(\lambda) = A_0 + \lambda I$, где

$$A_0 = \begin{Vmatrix} -1 & 0 \\ 0 & 1 \end{Vmatrix}.$$

Положим $\Lambda = \{1, -1\}$, $\mathfrak{F}_1 = \{\varphi_{10}\}$, $\mathfrak{F}_2 = \{\varphi_{20}\}$, где $\varphi_{10} = (0; 1)$ и $\varphi_{20} = (1; -1)$. Пусть m — произвольное натуральное число. Тогда, очевидно, система $\mathfrak{F}_1^m(1)$ состоит из единственного вектора $\Phi_{10,1}(1) = (\underbrace{0, 1, 0, 1, \dots, 0, 1}_{2m})$, а система $\mathfrak{F}_2^m(-1)$ — из вектора $\Phi_{20,2}(-1) = (\underbrace{-1, 1, -1, 1, \dots, -1, 1}_{2m})$. Оператор $\mathcal{A}_m$ в рассматриваемом случае определяется равенством

$$\mathcal{A}_m = \left.\begin{bmatrix} A_0 & I & \dots & 0 \\ \vdots & A_0 & I & \vdots \\ & & \ddots \quad \ddots & \\ 0 & \dots & A_0 & I \end{bmatrix}\right\} m$$

Легко видеть, что $\mathcal{A}_m(\Phi_{10,1}(1) + \Phi_{20,2}(-1)) = 0$, в то время как $\mathcal{A}_m \Phi_{10,1}(1) \neq 0$ и $\mathcal{A}_m \Phi_{20,2}(-1) \neq 0$.

3. Лемма 2.3. *Пусть* $\mathfrak{F} = \{\varphi_k : k = 0, 1, \dots, k_0\}$ [6]) — *система векторов из* $\mathbf{C}^d$ *и* $\mathfrak{F}^m = \{\Phi_k(\lambda_0) = (\varphi_k^p(\lambda_0))_{p=0}^{m-1}\}$ — *ее* m*-кратное расширение относительно* $\lambda_0 (\in \mathbf{C}^1)$. *Если* $m > k_0$ *и вектор* $\Phi_{k_0}(\lambda_0)$ *принадлежит ядру оператора* $\mathcal{A}_m$, *то* λ_0 *является характеристическим числом пучка* $A(\lambda)$, *а* $\varphi_0, \varphi_1, \dots, \varphi_{k_0}$ *представляет собой цепочку из собственного и присоединенных векторов.*

[6]) Здесь индекс k соответствует второму индексу векторов из определения m-кратного расширения.

Доказательство: Пусть $\psi_k = \sum_{p=0}^{n} A_p \varphi_k^p$. Повторяя соответствующее место из доказательства леммы 2.2, покажем, что система $\tilde{\mathfrak{G}} = \{\mathscr{A}_m \Phi_k(\lambda_0):\ k = 0, 1, \ldots, k_0\}$ является m-кратным расширением системы $\mathfrak{G} = \{\psi_k : k = 0, 1, \ldots, k_0\}$. Следовательно, согласно (1.3) имеет место равенство

$$\psi_{p+1}^k = \lambda_0 \psi_k^p + \psi_{k-1}^p,$$

где $\mathscr{A}_m \Phi_k(\lambda_0) = (\psi_k^p)_{p=0}^{m-1}$.

Поскольку $\psi_{k_0}^p = 0$ $(p = 0, 1, \ldots, m-1)$ и $m > k_0$, то отсюда вытекает, что $\psi_k = 0$ для $k = 0, 1, \ldots, k_0$. Последнее означает, что

$$0 = \sum_{p=0}^{n} A_p \varphi_k^p = \sum_{p=0}^{n} \sum_{r=0}^{p} \binom{p}{r} \lambda_0^{p-r} A_p \varphi_{k-r}.$$

Так как

$$\left(\frac{d^r}{d\lambda^r} A\right)(\lambda) = r! \sum_{p=0}^{n} \binom{p}{r} \lambda^{p-r} A_p,$$

то

$$0 = \sum_{r=0}^{k} \frac{1}{r!} \left(\frac{d^r}{d\lambda^r} A\right)(\lambda_0) \varphi_{k-r} \quad (k = 0, 1, \ldots, k_0).$$

Это означает, что $\varphi_0, \varphi_1, \ldots, \varphi_{k_0}$ является цепочкой из собственного и присоединенных векторов пучка $A(\lambda)$, соответствующей характеристическому числу λ_0.

Лемма доказана.

§ 3. Основная теорема

1. Пусть

$$A(\lambda) = A_0 + \lambda A_1 + \cdots + \lambda^n A_n \quad \text{и} \quad B(\lambda) = B_0 + \lambda B_1 + \cdots + \lambda^m B_m$$

— два матричных пучка с коэффициентами $A_j, B_k \in \mathbf{C}^d$ $(j = 0, 1, \ldots, n;\ k = 0, 1, \ldots, m)$. Пусть φ_0 — общее характеристическое число пучков $A(\lambda)$ и $B(\lambda)$ и

$$\mathfrak{K} = \operatorname{Ker} A(\lambda_0) \cap \operatorname{Ker} B(\lambda_0).$$

Пусть $\varphi_0, \varphi_1, \ldots, \varphi_r$ — цепочка собственного и присоединенных векторов одновременно для пучков $A(\lambda)$ и $B(\lambda)$, соответствующая характеристическому числу λ_0. Число $r+1$ называется длиной этой цепочки. Наибольшая длина такой цепочки, начинающейся вектором φ_0, назовем рангом общего собственного вектора φ_0 и обозначим через $\operatorname{rang}(\lambda_0, \varphi_0)$.

В подпространстве $\mathfrak{K}$ выберем базис $\varphi_{10}, \varphi_{20}, \ldots, \varphi_{j_0 0}$, ранги векторов которого обладают следующими свойствами: k_1 является максимальным из чисел $\operatorname{rang}(\lambda_0, \varphi)$ $(\varphi \in \mathfrak{K})$, а k_j $(j = 2, 3, \ldots, j_0)$ является максимальным из чисел rang (λ_0, φ) для всех векторов прямого дополнения к lin $\{\varphi_{10}, \varphi_{20}, \ldots, \varphi_{j-1,0}\}$ в $\mathfrak{K}$, содержащего φ_{j0}.

Легко видеть, что число rang (λ_0, φ_0) для любого вектора $\varphi_0 \in \mathfrak{K}$ равно одному из чисел k_j $(j=1, 2, \ldots, j_0)$. Следовательно, числа k_j $(j=1, 2, \ldots, j_0)$ определяются однозначно пучками $A(\lambda)$ и $B(\lambda)$.

Обозначим через $\varphi_{j1}, \varphi_{j2}, \ldots, \varphi_{j,k_j-1}$ соответствующую общую для $A(\lambda)$ и $B(\lambda)$ цепочку присоединенных векторов к собственному вектору φ_{j0} $(j=1, 2, \ldots, j_0)$.

Систему

$$\varphi_{j0}, \varphi_{j1}, \ldots, \varphi_{j,k_j-1} \quad (j = 1, 2, \ldots, j_0)$$

назовем канонической системой общих собственных и присоединенных векторов пучков $A(\lambda)$ и $B(\lambda)$, отвечающих характеристическому числу λ_0, а число

$$\nu(A, B, \lambda_0) \stackrel{\text{def}}{=} \sum_{j=1}^{j_0} k_j$$

назовем общей кратностью характеристического числа λ_0 пучков $A(\lambda)$ и $B(\lambda)$.

2. Пучкам $A(\lambda)$ и $B(\lambda)$ и целому числу $w > \max\{n, m\}$ сопоставим оператор

$$R_w(A, B) = \left[\begin{matrix} A_0 & A_1 \ldots A_n & & \ldots & 0 \\ \vdots & A_0 \ldots A_{n-1} & A_n & & \vdots \\ & \ddots & \ddots & \ddots & \\ 0 & \ldots & A_0 & \ldots\ A_{n-1} & A_n \\ B_0 & B_1 \ldots B_m & & \ldots & 0 \\ \vdots & B_0 \ldots B_{m-1} & B_m & & \vdots \\ & \ddots & \ddots & \ddots & \\ 0 & \ldots & B_0 & B_{m-1} & B_m \end{matrix}\right] \begin{matrix} \left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\} w-n \\ \left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\} w-m \end{matrix}$$

действующий из пространства $\mathbf{C}^{wd}$ в $\mathbf{C}^{(2w-m-n)d}$.

Условимся $R_w(A, B)$ называть результантным оператором или результантной матрицей пучков $A(\lambda)$ и $B(\lambda)$.

Теорема 3.1. *Пусть*

$$(3.1) \qquad A(\lambda) = A_0 + \lambda A_1 + \cdots + \lambda^n A_n \quad \text{и} \quad B(\lambda) = B_0 + \lambda B_1 + \cdots + \lambda^m B_m$$

— два матричных пучка $(A_j, B_k \in \mathbf{C}^d)$ *с обратимыми старшими коэффициентами* A_n *и* B_m; $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_l\}$ *— множество всех (различных) общих характеристических чисел пучков* $A(\lambda)$ *и* $B(\lambda)$ *и*

$$\mathfrak{F}_l = \{\varphi_{jk,l} \colon k = 0, 1, \ldots, k_{jl} - 1;\ j = 1, 2, \ldots, j_l\} \quad (l = 1, 2, \ldots, q)$$

— каноническая система общих собственных и присоединенных векторов пучков $A(\lambda)$ *и* $B(\lambda)$, *отвечающих характеристическому числу* λ_l.

Если выполняется условие

$$w \geqq \min\{n+md,\ m+nd\}\ ^{7)}, \tag{3.2}$$

то система

$$\mathfrak{F}^w(A) = \bigcup_{l=1}^{q} \mathfrak{F}_l^w(\lambda_l)$$

является базисом подпространства $\operatorname{Ker} R_w(A, B)$.

В частности, при условии (3.1) *имеет место равенство*

$$\nu(A, B) = \dim \operatorname{Ker} R_w(A, B) \quad \text{где} \quad \nu(A, B) = \sum_{l=1}^{q} \nu(A, B, \lambda_l).$$

Доказательство. Без ограничения общности можно предполагать, что $m \geqq n$.

Из леммы 2.1 вытекает, что $\mathfrak{F}^w(A) \subset \operatorname{Ker} \mathscr{A}_{w-n}$ и $\mathfrak{F}^w(A) \subset \operatorname{Ker} \mathscr{B}_{w-n}$, следовательно, $\mathfrak{F}^w(A) \subset \operatorname{Ker} R_w(A, B) = \operatorname{Ker} \mathscr{A}_{w-n} \cap \operatorname{Ker} \mathscr{B}_{w-m}$.

Пусть теперь $\Omega \in \operatorname{Ker} R_w(A, B)$. Тогда $\Omega \in \operatorname{Ker} \mathscr{A}_{w-n}$ и в силу леммы 2.1 Ω можно представить в виде

$$\Omega = \sum_{l=1}^{q} \sum_{j=1}^{j_l} \sum_{k=0}^{k_{jl}-1} \alpha_{jkl} \Phi_{jk,l}(\lambda_l),$$

где $\qquad \mathfrak{F}_l^w(A) = \{\Phi_{jk,l}(\lambda_l) \colon j = 1, 2, \ldots, j_l;\ k = 0, 1, \ldots, k_{jl}-1\}.$

Отсюда в силу леммы 2.2 вытекает, что

$$\Omega_k(\lambda_l) = \sum_j \alpha_{jkl} \Phi_{jk,l}(\lambda_l) \in \operatorname{Ker} \mathscr{B}_{w-m}$$

при $k=0, 1, \ldots, k_{jl}-1$, $l=1, 2, \ldots, q$, где суммирование происходит по всем j, для которых $k_{jl} \geqq k$. Согласно лемме 2.3 векторы

$$\omega_{kr}(\lambda_l) = \sum_j \alpha_{jkl} \varphi_{jr}(\lambda_l) \quad (r = 0, 1, \ldots, k;\ k = 0, 1, \ldots, k_l - 1;\ k_l = \max_j k_{jl})$$

образуют цепочку из собственного и присоединенных векторов пучка $B(\lambda)$. Так как, кроме того, векторы $\omega_{kr}(\lambda_l)$ $(r=0, 1, \ldots, k)$ также представляют собой цепочку из собственного и присоединенных векторов пучка $A(\lambda)$ мы пришли к выводу, что векторы $\Omega_k(\lambda_l)$ можно представить в виде линейной комбинации

---

[7]) Легко видеть, что приводимое доказательство теоремы остается в силе, если условие (3.1) заменить следующим менее стеснительным условием

$$w \geqq \min\left\{n + \sum_{l=1}^{q} \max_j k_{jl}(B);\ m + \sum_{l=1}^{q} \max_j k_{jl}(A)\right\} \tag{3.2'}$$

где $\{k_{jl}(C) \colon j=1, \ldots, j_l(C)\}$-набор частных кратностей пучка $C(\lambda)$.

векторов из $\mathfrak{F}^w(A)$. Следовательно, вектор Ω является линейной комбинацией векторов из $\mathfrak{F}^w(A)$.

Теорема доказана.

Следствие 3.1. *Пучки $A(\lambda)$ и $B(\lambda)$ из* (3.1) *имеют общее характеристическое число λ_0 и общий собственный вектор, отвечающий λ_0 в том и только том случае, когда ранг результантной матрицы $R_w(A, B)$ при $w \geqq \min\{md+n; nd+m\}$ меньше максимального.*

3. Теорема 0.1, сформулированная во введении, без труда выводится из теоремы 3.1. Классическая результантная матрица $R(a, b)$, приведенная во введении, очевидно, совпадает с $R_{m+n}(a, b)$. В этом случае (при $d=1$), очевидно, условие (3.2) выполняется. Следовательно, $\operatorname{Ker} R(a, b)$ состоит из линейной оболочки векторов

$$\Phi_k(\lambda_l) = \left((\varphi_k^p(\lambda_l))\right)_{p=0}^{m+n-1}, \quad \text{где} \quad \varphi_k^p(\lambda_l) = \sum_{s=0}^{k} \binom{p}{s} \lambda_l^{p-s}.$$

Так как

$$\Phi_k(\lambda_l) = \sum_{s=0}^{k} H_s(\lambda_l) \quad \text{и} \quad H_k(\lambda_l) = \Phi_k(\lambda_l) - \Phi_{k-1}(\lambda_l),$$

то отсюда непосредственно вытекает справедливость теоремы 0.1.

В случае $d>1$ для классической результантной матрицы, т.е. для $R_{m+n}(A, B)$, можно лишь утверждать следующее:

$$\operatorname{Ker} R_{m+n}(A, B) = \operatorname{Ker} \mathscr{A}_m \cap \operatorname{Ker} \mathscr{B}_n$$

и

$$\nu(A, B) \leqq \dim \operatorname{Ker} R_{m+n}(A, B).$$

Эти соотношения непосредственно вытекают из леммы 2.1.

Приведем еще одно утверждение для классической результантной матрицы при $d \neq 1$.

Пусть $\mathfrak{F}(\lambda_l, A)$ $(\mathfrak{F}(\mu_l, B))$ — каноническая система собственных и присоединенных векторов пучка $A(\lambda)$ $(B(\lambda))$, отвечающих характеристическому числу $\lambda_l(\mu_l)$. Тогда число $\dim \operatorname{Ker} R_{m+n}(A, B)$ равно коразмерности подпространства

$$\operatorname{lin} \mathfrak{F}^{m+n}(A) \cup \mathfrak{F}^{m+n}(B), \quad \text{где} \quad \mathfrak{F}^{m+n}(A) = \bigcup_l \mathfrak{F}^{m+n}(\lambda_l, A), \quad \mathfrak{F}^{m+n}(B) = \bigcup_l \mathfrak{F}^{m+n}(\mu_l, B).$$

В частности, оператор $R_{m+n}(A, B)$ обратим в том и только том случае, когда система $\mathfrak{F}^{m+n}(A) \cup \mathfrak{F}^{m+n}(B)$ полна в $\mathbf{C}^{(m+n)d}$.

Легко видеть, что для $w=m+n$ при $d>1$ условие (3.2′) выполняется только в некоторых частных случаях. Условие (3.2) (и соответствующее условие (3.2′)) теоремы 3.1 является существенным, для классической результантной матрицы теорема 3.1, вообще говоря, не имеет места. В этом можно убедиться на следующем примере.

Пусть

$$A(\lambda) = \begin{bmatrix} 1+\lambda & 0 \\ -1 & -1+\lambda \end{bmatrix} \quad \text{и} \quad B(\lambda) = \begin{bmatrix} 1+\lambda & 1 \\ 1 & 1+\lambda \end{bmatrix}.$$

Тогда ядро результантной матрицы $R_2(A, B)$ состоит из множества векторов $(-1, 1, 1, 0)t$ $(t \in \mathbf{C}^1)$. С другой стороны, пучок $A(\lambda)$ имеет характеристические числа ± 1, а пучок $B(\lambda)$ имеет характеристические числа $0, -2$. Таким образом, $\nu(A, B) = 0$, а $\dim \operatorname{Ker} R_2(A, B) = 1$.

§ 4. Приложения

Приведем два приложения результатов из § 3.

1. Начнем с обобщения метода исключения неизвестного из системы двух уравнений с двумя неизвестными (см., например, [1], гл. 11, § 54).

Пусть $A(\lambda, \mu)$ и $B(\lambda, \mu)$ — матричные пучки двух переменных

$$A(\lambda, \mu) = \sum_{j=0}^{n} \sum_{k=0}^{m} \lambda^j \mu^k A_{jk}$$

$$\qquad (\lambda, \mu \in \mathbf{C}^1;\ A_{jk}, B_{jk} \in L(\mathbf{C}^d)).$$

$$B(\lambda, \mu) = \sum_{j=0}^{q} \sum_{k=0}^{p} \lambda^j \mu^k B_{jk}$$

Рассмотрим следующую систему уравнений:

$$(4.1) \qquad A(\lambda, \mu)\varphi = 0, \quad B(\lambda, \mu)\varphi = 0$$

с неизвестными числами λ и μ и неизвестным вектором $\varphi \in \mathbf{C}^d$ $(\varphi \neq 0)$. Сделаем следующие предположения:

а) для некоторого $\mu = \mu_0 \in \mathbf{C}^1$ система (4.1) не имеет решения;

б) определители $\det \sum_{k=0}^{m} \mu^k A_{nk}$ и $\det \sum_{k=0}^{p} \mu^k B_{qk}$ не равны тождественно нулю;

в) определители $\det \sum_{j=0}^{n} \lambda^j A_{jm}$ и $\det \sum_{j=0}^{p} \lambda^j B_{jp}$ не равны тождественно нулю.

Пусть выполнены условия а) и б). Запишем пучки $A(\lambda, \mu)$ и $B(\lambda, \mu)$ по степеням переменной λ:

$$A(\lambda, \mu) = A_0(\mu) + \lambda A_1(\mu) + \cdots + \lambda^n A_n(\mu)$$

$$B(\lambda, \mu) = B_0(\mu) + \lambda B_1(\mu) + \cdots + \lambda^q B_q(\mu)$$

где $A_j(\mu) = \sum_{k=0}^{m} \mu^k A_{jk}$ и $B_j(\mu) = \sum_{k=0}^{p} \mu^k B_{jk}$, и положим

$$R_w(\mu) = \begin{bmatrix} A_0(\mu) & A_1(\mu) \dots A_n(\mu) & & \dots & 0 \\ \vdots & A_0(\mu) \dots A_{n-1}(\mu) & & A_n(\mu) & \vdots \\ & \ddots & & \ddots \quad \ddots & \\ 0 & \dots & A_0(\mu) & \dots \; A_{n-1}(\mu) & A_n(\mu) \\ B_0(\mu) & B_1(\mu) \dots B_m(\mu) & & \dots & 0 \\ \vdots & B_0(\mu) \dots B_{m-1}(\mu) & & B_m(\mu) & \vdots \\ & \ddots & & \ddots & \\ 0 & \dots & B_0(\mu) & \dots \; B_{m-1}(\mu) & B_m(\mu) \end{bmatrix}$$

Пусть M_0 (конечное) множество нулей функции $\det A_n(\mu) B_q(\mu)$. Если w обладает свойством

$$w \geqq \min\{nd+q;\; qd+n\},$$

то для всех $\mu \notin M_0$ можно применить следствие 3.1. Следовательно, множество точек μ, для которых существует решение системы (4.1), состоит из точек множества M_1 чисел $\mu_0 \notin M_0$, для которых

$$\text{(4.2)} \qquad \operatorname{rang} R_w(\mu_0) < w$$

и, быть может, некоторых точек из множества M_0.

Подставляя в (4.1) вместо переменной μ точки μ_0 множества $M_0 \cup M_1$, получим

$$\text{(4.3)} \qquad \left.\begin{aligned} A(\lambda, \mu_0)\varphi &= 0 \\ B(\lambda, \mu_0)\varphi &= 0 \end{aligned}\right\} \quad (\mu_0 \in M_0 \cup M_1).$$

Этим путем разыскание решений системы (4.1) сведено к разысканию решений системы с одним неизвестным числом и одним неизвестным вектором.

Предположим теперь, что кроме условий а) и б), выполняется еще условие в). Тогда описанный процесс можно повторить, поменяв местами переменные μ и λ. Пусть Λ_0 — множество всех нулей функции

$$\det\left(\sum_{j=0}^{n} \lambda^j A_{jm}\right)\left(\sum_{j=0}^{p} \lambda^j B_{jp}\right).$$

Множество чисел λ, для которых система (4.1) имеет решение, состоит из множества Λ_1 всех точек λ_0, для которых

$$\text{(4.4)} \qquad \operatorname{rang} \tilde{R}_w(\lambda_0) < w \; [8]$$

и, быть может, некоторых точек из множества Λ_0.

[8] $\tilde{R}_w(\lambda)$ определяется подобно $R_w(\mu)$.

Таким образом, осталось решить системы уравнений

$$\left.\begin{aligned} A(\lambda_0, \mu_0)\varphi = 0 \\ B(\lambda_0, \mu_0)\varphi = 0 \end{aligned}\right\} \tag{4.5}$$

где λ_0 пробегает множество $\Lambda_0 \cup \Lambda_1$, а μ_0 пробегает множество $M_0 \cup M_1$.

2. Рассмотрим однородные дифференциальные уравнения

$$A_n\left(\frac{d^n}{dt^n}\varphi\right)(t) + \cdots + A_1\left(\frac{d}{dt}\varphi\right)(t) + (A_0\varphi)(t) = 0 \tag{4.6}$$

$$B_m\left(\frac{d^m}{dt^m}\psi\right)(t) + \cdots + B_1\left(\frac{d}{dt}\psi\right)(t) + (B_0\psi)(t) = 0 \tag{4.7}$$

где $A_j, B_k \in L(\mathbf{C}^d)$ и матрицы A_n и B_m обратимы. Этим уравнениям отвечают матричные пучки $A(\lambda) = \sum_{k=0}^{n} \lambda^k A_k$ и $B(\lambda) = \sum_{k=0}^{m} \lambda^k B_k$.

Имеется тесная связь между решениями уравнения (4.6) с собственными и присоединенными векторами пучка $A(\lambda)$. Общее решение уравнения является линейной комбинацией вектор-функций вида

$$\varphi(t) = e^{\lambda_0 t}\left(\frac{t^k}{k!}\varphi_0 + \cdots + \frac{t}{1!}\varphi_{k-1} + \varphi_k\right) \tag{4.8}$$

где $\varphi_0, \varphi_1, \ldots, \varphi_k$ пробегают все цепочки из собственного и присоединенных векторов пучка $A(\lambda)$. Таким образом, из теоремы 3.1 непосредственно вытекает следующая теорема.

Теорема 4.1. *Пусть* $\mathfrak{K}$ *— подпространство общих решений уравнений* (4.6) *и* (4.7). *Если число* w *удовлетворяет условию*

$$w \geqq \min\{nd+m, md+n\},$$

то имеет место равенство

$$\dim \mathfrak{K} = \dim \operatorname{Ker} R_w(A, B).$$

С помощью этой теоремы и метода из п. 1 можно указать способ для решения системы дифференциальных уравнений, зависящих от параметра μ вида

$$\left.\begin{aligned} A_n(\mu)\left(\frac{d^n}{dt^n}\varphi\right)(t) + \cdots + A_1(\mu)\left(\frac{d}{dt}\varphi\right)(t) + A_0(\mu)\varphi(t) = 0 \\ B_m(\mu)\left(\frac{d^m}{dt^m}\varphi\right)(t) + \cdots + B_1(\mu)\left(\frac{d}{dt}\varphi\right)(t) + B_0(\mu)\varphi(t) = 0 \end{aligned}\right\},$$

где $A_k(\mu)$ и $B_k(\mu)$ — матричные пучки.

Рассмотрим еще одну задачу. Пусть даны $m+n$ векторов χ_k $(k=0, 1, \ldots, m+n-1)$ из пространства $\mathbf{C}^d$. Будем искать все пары функций $(\varphi(t), \psi(t))$, где

$\varphi(t)$ — решение уравнения (4.6), а $\psi(t)$ — решение уравнения (4.7), которые удовлетворяют начальным условиям

(4.9) $$\frac{d^k}{dt^k}(\varphi(t)+\psi(t))\Big|_{t=0} = \chi_k \quad (k=0, 1, \ldots, m+n-1).$$

Эта задача имеет для любого набора векторов χ_k $(k=0, 1, \ldots, m+n-1)$ единственное решение в том и только том случае, когда классическая результантная матрица $R_{m+n}(A, B)$ обратима.

В самом деле, построим для каждого решения $\varphi(t)$ уравнения (4.6) ($\psi(t)$ уравнения (4.7)) вектор-функцию

$$\Phi(t) = \left(\left(\frac{d^k}{dt^k}\varphi\right)(t)\right)_{k=0}^{m+n-1} \quad \left(\Psi(t) = \left(\left(\frac{d^k}{dt^k}\psi\right)(t)\right)_{k=0}^{m+n-1}\right).$$

Полагая $X=(\chi_k)_{k=0}^{m+n-1}$, видим, что начальные условия (4.9) принимают вид

$$\Phi(0)+\Psi(0) = X.$$

Если вектор-функция $\varphi(t)$ пробегает все решения уравнения (4.6) ($\psi(t)$ — все решения (4.7)), то из равенства (1.2) непосредственно вытекает, что векторы $\Phi(0)$ ($\Psi(0)$) пробегают систему векторов $(m+n)$-кратного расширения $\mathfrak{F}^{m+l}$ ($\mathfrak{G}^{m+l}$) систем из собственных и присоединенных векторов пучка $A(\lambda)$ (пучка $B(\lambda)$). Следовательно, задача имеет для любого $X\in\mathbf{C}^{(m+n)d}$ решение в том и только том случае, когда объединение систем $\mathfrak{F}^{m+l}$ и $\mathfrak{G}^{m+l}$ является полным в $\mathbf{C}^{(m+n)d}$. Как отмечалось в § 3, последнее имеет место тогда и только тогда, когда матрица $R_{m+n}(A, B)$ обратима. Легко видеть, что в этом случае решение является единственным.

§ 5. Ядро безутианты

I. В качестве еще одного приложения теоремы 0.1 дадим описание ядра безутианты двух полиномов в случае, когда $d=1$.

Пусть $a(\lambda)=a_0+a_1\lambda+\cdots+a_n\lambda^n$ и $b(\lambda)=b_0+b_1\lambda+\cdots+b_m\lambda^m$ $(m\leqq n)$ — два полинома ($a_k, b_k\in\mathbf{C}^1$; $a_n\neq0$). Рассмотрим полином двух переменных

$$B(\lambda, \mu) = \frac{a(\lambda)b(\mu)-a(\mu)b(\lambda)}{\lambda-\mu} = \sum_{p,q=0}^{n-1} b_{pq}\lambda^p\mu^q.$$

Безутиантой полиномов $a(\lambda)$ и $b(\lambda)$ называется квадратная матрица $\mathscr{B}(a, b)= =\|b_{pq}\|_{p,q=0}^{n-1}$. Как известно (см., например, [2, 3]), дефект безутианты равен степени наибольшего общего делителя полиномов $a(\lambda)$ и $b(\lambda)$. Это утверждение допускает следующее уточнение.

Теорема 5.1. *Ядро безутианты $\mathscr{B}(a, b)$ полиномов $a(\lambda)$ и $b(\lambda)$ состоит из линейной оболочки векторов*

$$\varphi_{jk} = \left(\binom{p}{k}\lambda_j^p\right)_{p=0}^{n-1} \quad (k=0, 1, \ldots, \nu_j-1;\ j=1, 2, \ldots, l)$$

где λ_j $(j=1, 2, \dots, l)$ — *все общие нули полиномов* $a(\lambda)$ *и* $b(\lambda)$, *а* ν_j — *общая кратность нуля* λ_j.

Доказательство. Для безутианты $\mathcal{B}(a, b)$ имеет место равенство (см. [3]):

(5.1) $$\mathcal{B}(a,b) =$$
$$= \begin{bmatrix} a_1 & \dots & a_{n-1} & a_n \\ a_2 & \dots & a_n & \vdots \\ \vdots & \cdot^{\cdot^{\cdot}} & & \\ a_n & & \dots & 0 \end{bmatrix} \begin{bmatrix} b_0 & b_1 & \dots & b_{n-1} \\ \vdots & b_0 & \dots & b_{n-2} \\ & & \ddots & \vdots \\ 0 & & \dots & b_0 \end{bmatrix} - \begin{bmatrix} b_1 & \dots & b_{n-1} & b_n \\ b_2 & \dots & b_n & \vdots \\ \vdots & \cdot^{\cdot^{\cdot}} & & \\ b_n & & \dots & 0 \end{bmatrix} \begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ \vdots & a_0 & \dots & a_{n-2} \\ & & \ddots & \vdots \\ 0 & & \dots & a_0 \end{bmatrix}.$$

Образуем матрицы
$$\tilde{A}_n = \begin{bmatrix} a_n & \dots & 0 \\ a_{n-1} & a_n & \vdots \\ \vdots & \vdots & \ddots \\ a_1 & a_2 \dots & a_n \end{bmatrix} \quad A_n = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ \vdots & a_0 & \dots & a_{n-2} \\ & & \ddots & \vdots \\ 0 & & \dots & a_0 \end{bmatrix} \quad \Delta = [\delta_{j, n-k-1}]_{j,k=0}^{n-1}$$

и соответственно матрицы $\tilde{B}_n$ и B_n. Тогда равенство (5.1) примет вид

(5.2) $$\mathcal{B}(a, b) = \Delta(\tilde{A}_n B_n - \tilde{B}_n A_n).$$

Следовательно, уравнение $\mathcal{B}(a, b)\varphi=0$ эквивалентно уравнению

(5.3) $$(\tilde{A}_n B_n - \tilde{B}_n A_n)\varphi = 0.$$

В приведенных обозначениях, очевидно,
$$R(b, a) = \begin{bmatrix} B_n & \tilde{B}_n \\ A_n & \tilde{A}_n \end{bmatrix}.$$

Легко убедиться в справедливости равенства
$$\begin{bmatrix} B_n & \tilde{B}_n \\ A_n & \tilde{A}_n \end{bmatrix} = \begin{bmatrix} I & \tilde{B}_n \tilde{A}_n^{-1} \\ 0 & I \end{bmatrix} \begin{bmatrix} B_n - \tilde{B}_n \tilde{A}_n^{-1} A_n & 0 \\ 0 & \tilde{A}_n \end{bmatrix} \begin{bmatrix} I & 0 \\ \tilde{A}_n^{-1} A_n & I \end{bmatrix}.$$

Очевидно, матрицы $\tilde{B}_n$ и $\tilde{A}_n$ перестановочны, следовательно,

(5.4) $$B_n - \tilde{B}_n \tilde{A}_n^{-1} A_n = \tilde{A}_n^{-1}(\tilde{A}_n B_n - \tilde{B}_n A_n).$$

Пусть

(5.5) $$\begin{bmatrix} B_n & \tilde{B}_n \\ A_n & \tilde{A}_n \end{bmatrix} \begin{bmatrix} f \\ g \end{bmatrix} = 0.$$

Тогда из равенств (5.2)—(5.4) следует $\mathcal{B}(a, b)f=0$. Наоборот, если $\mathcal{B}(a, b)f=0$, то имеет место равенство (5.5) при $g=\tilde{A}_n^{-1} A_n f$. Осталось воспользоваться теоремой 0.1.

Теорема доказана.

2. Пусть заданы два полинома вида

(5.6) $$x(\lambda) = x_0 + x_1\lambda + \dots + x_n\lambda^n \quad \text{и} \quad y(\lambda) = y_0 + y_{-1}\lambda^{-1} + \dots + y_{-n}\lambda^{-n}$$

($x_n \neq 0$ или $y_{-n} \neq 0$). Безутиантой многочленов $x(\lambda)$ и $y(\lambda)$ называется квадратная матрица $\tilde{\mathscr{B}}(x, y) = \|b_{pq}\|_{p,q=0}^{n-1}$, где

$$\sum_{p,q=0}^{n-1} b_{pq}\lambda^p\mu^q = \frac{x(\lambda)y(\mu^{-1}) - (\lambda\mu)^n x(\mu^{-1})y(\lambda)}{1-\lambda\mu}.$$

Непосредственной проверкой убеждаемся в том, что

$$\tilde{\mathscr{B}}(x, y) \doteq$$

$$= \begin{bmatrix} x_0 & \dots & 0 \\ x_1 & x_0 & \vdots \\ \vdots & \vdots & \ddots \\ x_{n-1} & x_{n-2} \dots & x_0 \end{bmatrix} \begin{bmatrix} y_0 & y_{-1} \dots & y_{1-n} \\ \vdots & y_0 & \dots y_{2-n} \\ & & \ddots \vdots \\ 0 & \dots & y_0 \end{bmatrix} - \begin{bmatrix} y_{-n} & \dots & 0 \\ y_{1-n} & y_{-n} & \vdots \\ \vdots & \vdots & \ddots \\ y_{-1} & y_{-2} \dots & y_{-n} \end{bmatrix} \begin{bmatrix} x_n & x_{n-1} \dots & x_1 \\ \vdots & x_n & \dots x_2 \\ & & \ddots \vdots \\ 0 & \dots & x_n \end{bmatrix}.$$

Для безутианты $\tilde{\mathscr{B}}(x, y)$ имеет место теорема, аналогичная теореме 5.1. Для полноты приведем ее формулировку.

Теорема 5.2. *Ядро безутианты многочленов $x(\lambda)$ и $y(\lambda)$ вида* (5.6) *состоит из линейной оболочки векторов $\varphi_{jk} = \left(\lambda_j^p \binom{p}{k}\right)_{p=0}^{n-1}$ $(k=0, 1, \dots, k_j-1)$ где λ_j $(j=1, 2, \dots, l)$ — все общие нули функций $x(\lambda)$ и $y(\lambda)$, а k_j — общая кратность нуля λ_j.*

Литература

[1] А. Г. Курош, *Курс высшей алгебры*, Наука (Москва, 1968).

[2] М. Г. Крейн, М. А. Неймарк, *Метод эрмитовых и симметрических форм в теории отделения корней алгебраических уравнений* (Харьков, 1936).

[3] Ф. И. Ландер, Безутианта и обращение ганкелевых матриц, *Матем. исслед. Кишинев*, **9**: 2 (1974), 69—87.

[4] И. Ц. Гохберг, А. А. Семенцул, Об обращении конечных теплицевых матриц и их континуальных аналогов, *Матем. исслед. Кишинев*, **7**; 2 (1972), 201—223.

[5] И. Ц. Гохберг, Г. Хайниг, Обращение конечных теплицевых матриц, составленных из элементов некоммутативной алгебры, *Revue roumaine math. pures et appl.* **14**, 5 (1974), 623—663.

[6] И. Ц. Гохберг, Г. Хайниг, О матричных интегральных операторах на конечном интервале с ядрами, зависящими от разности аргументов, *Revue roumaine math. pures et appl.* (в печати).

[7] М. Г. Крейн, О расположении корней многочленов, ортогональных на единичной окружности по знакопеременному весу, *Теория функций, функциональный анализ и их приложения*, Харьков **2** (1966), 131—137.

[8] И. Ц. Гохберг, М. Г. Крейн, *Введение в теорию линейных несамосопряженных операторов в гильбертовом пространстве*, Наука (Москва, 1965).

[9] И. Ц. Гохберг, Е. И. Сигал, Операторное обобщение теоремы о логарифмическом вычете и теоремы Руше, *Матем. сборник*, **84**; 4 (1971), 607—630.

(Поступило 21/I/1974г.)

Wiener-Hopf operators induced by multipliers

By G. A. HIVELY in Lexington (Kentucky, USA)[1])

1. Introduction. Let R denote the real line $(-\infty, \infty)$ and let $M(R)$ denote the commutative Banach algebra of complex valued Borel measures on R equipped with total variation norm and with multiplication defined by convolution of measures. Let $R^+=[0, \infty)$ and $R^-=(-\infty, 0]$. For each $1 \leqq p \leqq \infty$, let $L^p(R)$ (resp. $L^p(R^+)$, $L^p(R^-)$) denote the usual Lebesgue space of complex valued Borel measurable functions on R (resp. R^+, R^-). *To avoid unnecessary repetition, it will be assumed henceforth that the index p of any L^p-space under consideration satisfies the constraint* $1 \leqq p \leqq \infty$. The subspace of $M(R)$ consisting of those measures whose support is contained in R^+ (resp. R^-) will be denoted by $M(R^+)$ (resp. $M(R^-)$). We shall frequently identify $L^p(R^+)$ and $L^p(R^-)$ as subspaces of $L^p(R)$. We write I (resp. I_+, I_-) for the identity operator on $L^p(R)$ (resp. $L^p(R^+)$, $L^p(R^-)$) and P (resp. Q) for the natural projection of $L^p(R)$ onto $L^p(R^+)$ (resp. $L^p(R^-)$). If $1 \leqq p < \infty$ (resp. $p=\infty$), we write $B(L^p(R))$ for the space of continuous (resp. weak*-continuous) linear operators on $L^p(R)$ equipped with the usual operator norm.

If $\mu \in M(R)$ and $f \in L^p(R)$, then the convolution

$$[\mu * f](x) = \int f(x-t)\, d\mu(t)$$

defines a.e. an element $\mu * f \in L^p(R)$ with $\|\mu * f\|_p \leqq \|\mu\| \, \|f\|_p$. For each $\mu \in M(R)$ the operator $S(\mu, p) \in B(L^p(R))$ is defined by

$$S(\mu, p)f = \mu * f, \quad f \in L^p(R),$$

and $\|S(\mu, p)\| \leqq \|\mu\|$. We say that $S(\mu, p)$ is the *convolution operator* on $L^p(R)$ induced by μ.

If T is any operator on $L^p(R)$, the operator $\mathrm{pr}\,(T)$ on $L^p(R^+)$ is defined by

$$\mathrm{pr}\,(T)f = PTf, \quad f \in L^p(R^+).$$

---

[1]) This paper is based on the author's doctoral dissertation at the University of California, written under the supervision of Professor Donald Sarason.

If $T\in B(L^p(R))$, then $\mathrm{pr}\,(T)\in B(L^p(R^+))$ and $\|\mathrm{pr}\,(T)\|\leqq\|T\|$. For each $\mu\in M(R)$, the *Wiener—Hopf operator* $W(\mu, p)$ on $L^p(R^+)$ induced by μ is defined by $W(\mu, p)=$ $=\mathrm{pr}\,(S(\mu, p))$.

Several authors have considered the Wiener—Hopf operators induced by various classes of measures (cf. [8], [12]), particularly with regard to their inversion. R. G. Douglas and J. L. Taylor [4] have recently provided inversion criteria of great generality. We summarize their results in the following

Theorem 1.1. *If $\mu\in M(R)$, $W(\mu, 1)$ is invertible if and only if $\mu\in\exp(M(R))$. If μ is invertible in $M(R)$, $W(\mu, p)$ is invertible if and only if $\mu\in\exp(M(R))$.*

An important consequence of this result is that the invertibility of $W(\mu, p)$ is independent of the index p provided that μ is invertible in $M(R)$. Douglas and Taylor also show that this need not be the case if μ is not invertible. Specifically, they exhibit a noninvertible measure $\nu\in M(R^+)$ for which $W(\nu, 2)$ is invertible. This example motivates our consideration of the more general class of Wiener—Hopf operators induced by multipliers. As we shall subsequently show, the invertibility of $W(\nu, 2)$ implies the invertibility of $S(\nu, 2)$. Since ν is not invertible in $M(R)$, $S(\nu, 2)^{-1}$ is a multiplier (cf. Section 2) which is not a convolution operator and, moreover, $W(\nu, 2)^{-1}$ is $\mathrm{pr}\,S(\nu, 2)^{-1}$.

In the next section we provide a summary of some important facts concerning Fourier transforms, multipliers and pseudomeasures which we will need later. In § 3 we define the class of Wiener—Hopf operators induced by multipliers and prove theorems analogous to results such as those of Hartman—Winter, Coburn and Brown—Halmos in the theory of Toeplitz operators. In § 4 we examine the Wiener—Hopf factorization technique for the inversion of a Wiener—Hopf operator. In contrast to the results of previous authors, we give an example of an invertible Wiener—Hopf operator on $L^2(R^+)$ whose inverse cannot be expressed in the form W_+W_- where W_+ and W_- are analytic and coanalytic (cf. Section 2) Wiener—Hopf operators respectively.

In § 5 we conclude by considering the problem of interpolating the inverse of a Wiener—Hopf operator suggested by the example of Douglas and Taylor. The Wiener—Pitt measure is used to provide an example of a Wiener—Hopf operator $W(\omega, p)$ which is invertible for $1<p<\infty$ yet not invertible for $p=1, \infty$. Although we are unable to show that interpolation of the inverse occurs in the general case, we show that interpolation does occur when the Wiener—Hopf operator is either analytic or coanalytic.

2. Fourier transforms, multipliers and pseudomeasures. If $f\in L^1(R)$, we define the Fourier transform of f by

$$\hat{f}(x) = \int e^{ixt} f(t)\,dt, \quad x\in R.$$

If p' denotes the conjugate exponent of p and $1 \leqq p \leqq 2$, then the Fourier transform defines a bounded linear mapping of $L^1(R) \cap L^p(R)$ (equipped with the norm from $L^p(R)$) into $L^{p'}(R)$. The unique continuous extension of this mapping from $L^p(R)$ into $L^{p'}(R)$ will also be called the Fourier transform and the result of applying this mapping to an element $f \in L^p(R)$ will be denoted by $\hat{f}$. In the case $p=2$ the Fourier transform is an invertible operator on $L^2(R)$ and we shall denote by U the *Fourier—Plancheral transform* on $L^2(R)$ defined by $Uf=(2\pi)^{-1/2}\hat{f}$. The operator U is a unitary operator on $L^2(R)$.

We shall eventually have need of relations between the Fourier transform and the Hardy spaces $H^p(R)$. The definitions and basic facts concerning these spaces may be found in [6] and [10]. The following result does not seem to be explicitly stated in the standard references. Since we will make crucial use of it, we sketch the proof.

Theorem 2.1. *If* $1 \leqq p \leqq 2$ *and* $f \in L^p(R^+)$, *then* $\hat{f} \in H^{p'}(R)$. *Moreover,* $U(L^2(R^+)) = H^2(R)$.

Proof. Let π^+ be the upper half-plane $\{z \mid \operatorname{Im} z > 0\}$ and define the Laplace transform of f by

$$Lf(z) = \int e^{izt} f(t)\, dt, \quad z \in \pi^+.$$

The function Lf is analytic in π^+. Consider the family of functions f_y, $y>0$, defined by $f_y(t)=e^{-yt}f(t)$ and note that $\sup_{y>0} \|f_y\|_p = \|f\|_p$ and that $\lim_{y\to 0} \|f_y - f\|_p = 0$. Since $Lf(x+iy)=\hat{f}_y(x)$, it follows that $Lf \in H^p(\pi^+)$ and that $\hat{f}$ is the boundary function for Lf. This proves the first assertion. The second assertion is then just a form of the Paley—Wiener theorem [15, Theorem 19.2, p. 368]. Q.E.D.

The space $M(R)$ and the spaces $L^p(R)$ admit natural involutions defined by setting $\mu^*(E) = \overline{\mu(-E)}$ for $\mu \in M(R)$ and E a Borel set in R and by setting $f^*(x) = \overline{f(-x)}$ a.e. for $f \in L^p(R)$. If the Fourier—Stieltjes transform of $\mu \in M(R)$ is defined by $\hat{\mu}(x) = \int e^{ixt} d\mu(t)$, then these involutions have the following properties:

$$\hat{\mu}^* = \bar{\hat{\mu}}, \quad \mu \in M(R),$$

and

$$\hat{f}^* = \bar{\hat{f}}, \quad f \in L^p(R),\ 1 \leqq p \leqq 2.$$

For each $a \in R$, let δ_a denote the measure with positive unit mass at the point a. Just as the ambiguity of space for the projections P and Q causes no problems, so we shall frequently write S_a in place of $S(\delta_a, p)$ and W_a in place of $W(\delta_a, p)$. We define a *multiplier* on $L^p(R)$ to be an operator $S \in B(L^p(R))$ such that S commutes with S_a for each $a \in R$. The set of multipliers on $L^p(R)$ will be denoted by $\mathcal{M}^p$.

It is clear that $\mathcal{M}^p$ is an inverse-closed algebra of operators on $L^p(R)$ and that $\mathcal{M}^p$ contains the convolution operators on $L^p(R)$. If $p=1$ or $p=\infty$, then $\mathcal{M}^p$ is precisely the set of convolution operators on $L^p(R)$ [13, Theorem 3.1.1 and Theorem 3.4.1]. If the adjoint operator on $L^{p'}(R)$ of an operator on $L^p(R)$, $1 \leqq p < \infty$, is defined by means of the pairing

$$(f, g) = \int f\bar{g}\, dx, \; f \in L^p(R), \; g \in L^{p'}(R),$$

then a simple application of Fubini's theorem shows that $S(\mu, p)^* = S(\mu^*, p')$ for $\mu \in M(R)$ and $1 \leqq p < \infty$. Setting $\mu = \delta_a$ we see that $S_a^* = S_{-a}$ and that $\mathscr{M}^{p^*} = \mathscr{M}^{p'}$ if $1 \leqq p < \infty$.

Let $A(R) = \{\hat{f} \mid f \in L^1(R)\}$ and let $A(R)$ be given the induced norm from $L^1(R)$. The algebra $A(R)$ is then a Banach algebra and is isometrically isomorphic to $L^1(R)$. The Banach space dual of $A(R)$ will be denoted by $P(R)$ and the elements of this dual space will be called *pseudomeasures.* The natural isomorphism mapping $\sigma \to \hat{\sigma}$ of $P(R)$ onto $L^\infty(R)$ will be called the Fourier transform on $P(R)$. If $\sigma \in P(R)$, the element $\hat{\sigma} \in L^\infty(R)$ is uniquely determined by the relation

$$\sigma(\hat{f}) = \int \hat{\sigma} f\, dx, \quad f \in L^1(R).$$

The space $P(R)$ is a commutative C^*-algebra via the induced operations from $L^\infty(R)$. If $M(R)$ is identified as a subalgebra of $P(R)$ by means of the relation

$$\mu(\hat{f}) = \int \hat{f}\, d\mu, \quad \mu \in M(R), f \in L^1(R),$$

then the multiplication, involution and Fourier transform defined on $P(R)$ are consistent with those previously defined on $M(R)$. In particular, we may denote by $*$ the multiplication on $P(R)$.

Theorem 2.2. [13, Theorem 4.3.1] *The relation*

$$(Sf)\hat{} = \hat{\sigma}\hat{f}, \quad f \in L^2(R),$$

between elements $S \in \mathscr{M}^2$ and $\sigma \in P(R)$ determines an isometric algebraic isomorphism between $\mathscr{M}^2$ and $P(R)$.

For $1 \leqq p \leqq \infty$, let $\lambda(p) = |(p-2)/p|$. The value of $\lambda(p)$ may be regarded as a measure of the distance of p from 2 and the function $\lambda(\cdot)$ is symmetric with respect to conjugate indices. The next result is essentially contained in [13, pp. 95—97].

Theorem 2.3. *If $S \in \mathscr{M}^p$ and $\lambda(r) \leqq \lambda(p)$, then S maps $L^1(R) \cap L^\infty(R)$ into $L^p(R) \cap L^{p'}(R)$ and hence into $L^r(R)$. Moreover, the restriction of S to $L^1(R) \cap L^\infty(R)$ has a unique extension to an element of $\mathscr{M}^r$. The resulting mapping of $\mathscr{M}^p$ into $\mathscr{M}^r$ is an injective norm-decreasing algebra homomorphism and is an isometric isomorphism if $\lambda(r) = \lambda(p)$.*

Combining theorems 2.2 and 2.3 we see that $\mathscr{M}^p$ may be identified with a subalgebra of $\mathscr{M}^2$ and hence with a subalgebra of $P(R)$ (containing $M(R)$). In particular, to each multiplier on $L^p(R)$ there is associated a unique pseudomeasure. The notation $S(\sigma, p)$ will be used to denote the multiplier on $L^p(R)$, *if it exists*, having σ as its associated pseudomeasure. With this notation, the natural mapping of $\mathcal{M}^p$ into $\mathcal{M}^r$ for $\lambda(r)\leqq\lambda(p)$ is given by $S(\sigma,p)\to S(\sigma,r)$.

As an easy consequence of theorems 2.2 and 2.3 we have

Theorem 2.4. *If* $1\leqq p\leqq 2$ *and* $S=S(\sigma,p)$, *then*

$$(Sf)\hat{} = \hat{\sigma}\hat{f}, \quad f\in L^p(R).$$

If $\sigma\in P(R)$, we say that σ is *analytic* if $\hat{\sigma}\in H^\infty(R)$ and that σ is *coanalytic* if $\hat{\sigma}\in\overline{H^\infty(R)}$. If the support of a pseudomeasure is defined as in [7], then a pseudomeasure is analytic (resp. coanalytic) if and only if its support is contained in R^+ (resp. R^-). If $S\in\mathcal{M}^p$, we say that S is *analytic* (resp. *coanalytic*) if S leaves $L^p(R^+)$ (resp. $L^p(R^-)$) invariant. Theorems 2.1, 2.2 and 2.3 imply the following

Theorem 2.5. *If* $S=S(\sigma,p)$, *then S is analytic (resp. coanalytic) if and only if σ is analytic (resp. coanalytic).*

3. The class $\mathcal{W}^p$. If $W\in B(L^p(R^+))$, we say that W is a *Wiener—Hopf operator* if $W=\mathrm{pr}\,(S)$ for some $S\in\mathcal{M}^p$. The class of Wiener—Hopf operators on $L^p(R^+)$ will be denoted by $\mathcal{W}^p$. If $S=S(\sigma,p)$, the Wiener—Hopf operator $\mathrm{pr}\,(S)$ induced by S may be denoted by $W(\sigma,p)$. Since the mapping $T\to\mathrm{pr}\,(T)$ of $B(L^p(R))$ into $B(L^p(R^+))$ is linear, $\mathrm{pr}\,(I)=I_+$ and $\mathrm{pr}\,(T)^*=\mathrm{pr}\,(T^*)$ if $1\leqq p<\infty$, it follows that $\mathcal{W}^p$ is a linear subspace of $B(L^p(R^+))$, $I_+\in\mathcal{W}^p$ and $\mathcal{W}^{p*}=\mathcal{W}^{p'}$ if $1\leqq p<\infty$.

In the case $p=1$ we know that $\mathcal{M}^1$ consists precisely of the convolution operators $S(\mu,1)$ for measures $\mu\in M(R)$. Thus $\mathcal{W}^1$ consists precisely of the Wiener—Hopf operators $W(\mu,1)$ induced by measures $\mu\in M(R)$. By duality, a similar statement holds for $\mathcal{W}^\infty$. If, for the moment, we assume that each $W\in\mathcal{W}^p$ is induced by a unique $S\in\mathcal{M}^p$ (a fact that will be established later), then it follows from Theorem 2.3 that we may identify $\mathcal{W}^p$ as a subspace of $\mathcal{W}^r$ whenever $\lambda(r)\leqq\lambda(p)$. In particular, we may think of $\mathcal{W}^p$ as being contained in $\mathcal{W}^2$, depending symmetrically on the index p and growing larger as p approaches 2.

If $\varphi\in L^\infty(R)$, define the operator $M_\varphi\in B(L^2(R))$ by setting $M_\varphi f=\varphi f$ for each $f\in L^2(R)$. Let P_+ be the orthogonal projection of $L^2(R)$ onto $H^2(R)$. The Toeplitz operator $T_\varphi\in B(H^2(R))$ induced by $\varphi\in L^\infty(R)$ is defined by setting $T_\varphi f=P_+M_\varphi f$ for each $f\in H^2(R)$. We now assert that *the class $\mathcal{W}^2$ is unitarily equivalent to the class of Toeplitz operators on* $H^2(R)$. For suppose that $\sigma\in P(R)$ and $f\in L^2(R^+)$ and let U_0 be the restriction of the Fourier—Plancherel transform to $L^2(R^+)$. Applying Theorems 2.1 and 2.2 we have

$$U_0W(\sigma,2)f = UPS(\sigma,2)f = P_+US(\sigma,2)f = P_+M_{\hat{\sigma}}U_0f = T_{\hat{\sigma}}U_0f.$$

Thus $U_0W(\sigma,2)U_0^{-1}=T_{\hat{\sigma}}$ and the assertion follows by observing that $\hat{\sigma}$ ranges over $L^\infty(R)$ as σ ranges over $P(R)$.

The following result gives a simple characterization of the Wiener—Hopf operators on $L^p(R^+)$ analogous to a well known characterization of Toeplitz operators [1, Theorem 6].

Theorem 3.1. *If* $W \in B(L^p(R^+))$, *then a necessary and sufficient condition in order that* $W \in \mathcal{W}^p$ *is that* $W_{-a}WW_a = W$ *for* $a \geqq 0$.

Proof. For each $a \in R$, let P_a denote the natural projection of $L^p(R)$ onto $L^p([a, \infty))$. If $W \in \mathcal{W}^p$, so that $W = \mathrm{pr}(S)$ for some $S \in \mathcal{M}^p$, then for each $a \geqq 0$ and $f \in L^p(R^+)$ we have

$$W_{-a}WW_af = P(S_{-a}P)S(PS_a)f = P(P_{-a}S_{-a})S(S_aP_{-a})f = PSf = Wf.$$

This establishes the necessity of the condition.

Since the assertion in the case $p = \infty$ follows by duality from the case $p = 1$, it follows that we need only prove the sufficiency of the condition in the case $1 \leqq p < \infty$. So suppose that $W \in B(L^p(R^+))$ where $1 \leqq p < \infty$ and that $W_{-a}WW_a = W$ for each $a \geqq 0$. Regard R as a directed set with its natural order and consider the net $\{S_{-a}WPS_a\}_{a \in R}$ in $B(L^p(R))$. If $a \leqq b$ and $f \in L^p([-a, \infty))$, then

$$P_{-a}S_{-b}WPS_bf = P_{-a}S_{-a}S_{(a-b)}WPS_{(b-a)}S_af =$$
$$= S_{-a}PS_{(a-b)}WPS_{(b-a)}S_af = S_{-a}W_{(a-b)}WW_{(b-a)}S_af = S_{-a}WPS_af.$$

Since the net $\{S_{-a}WPS_a\}_{a \in R}$ is bounded in norm and $1 \leqq p < \infty$, it follows that this net is strongly convergent on the set $\bigcup_{a \in R} L^p(-a, \infty))$. Since the latter set is dense in $L^p(R)$, it follows that the net is strongly convergent on $L^p(R)$ to some $S \in B(L^p(R))$. For each $b \in R$,

$$S_bS = s-\lim_a (S_bS_{-a}WPS_a) = s-\lim_a (S_{(b-a)}WPS_{(a-b)}S_b) = SS_b.$$

Thus $S \in \mathcal{M}^p$. If $f \in L^p(R^+)$, then

$$PSf = \lim_a (PS_{-a}WPS_af) = \lim_a (W_{-a}WW_af) = Wf.$$

Thus $W = \mathrm{pr}(S)$ and $W \in \mathcal{W}^p$.

Theorem 3.2. *If* $1 \leqq p < \infty$, $S \in \mathcal{M}^p$ *and* $W = \mathrm{pr}(S)$, *then* $S = s-\lim_a S_{-a}WPS_a$.

Proof. Since $1 \leqq p < \infty$, $s-\lim_a P_{-a} = I$. The desired conclusion follows from the fact that, for each $a \in R$,

$$S_{-a}WPS_a = S_{-a}PSPS_a = P_{-a}S_{-a}SS_aP_{-a} = P_{-a}SP_{-a}. \qquad \text{Q.E.D.}$$

An important consequence of this result is that each Wiener—Hopf operator on $L^p(R^+)$, $1 \leqq p < \infty$, is induced by a unique multiplier on $L^p(R)$ and that pr is isometric on $\mathcal{M}^p$. By duality, the same is true in the case $p = \infty$.

Corollary 3.3. *For each $W\in\mathcal{W}^p$ there is a unique $S\in\mathcal{M}^p$ such that* $W=\text{pr}\,(S)$ *and, moreover,* $\|W\|=\|S\|$.

Corollary 3.4. *If* $1\leqq p<\infty$, $S\in\mathcal{M}^p$ *and* $W=\text{pr}\,(S)$, *then*

$$\inf_{\substack{f\in L^p(R^+)\\ \|f\|_p=1}}\|Wf\|_p\leqq\inf_{\substack{g\in L^p(R)\\ \|g\|_p=1}}\|Sg\|_p.$$

Proof. Let $g\in L^p(R)$ and $\|g\|_p=1$. Since $1\leqq p<\infty$, $\lim_a\|PS_ag\|_p=1$ so that, by Theorem 3.2,

$$\|Sg\|_p=\lim_a\|S_{-a}WPS_ag\|_p=\lim_a\|WPS_ag\|_p\geqq\inf_{\substack{f\in L^p(R^+)\\ \|f\|_p=1}}\|Wf\|_p.$$

The assertion now follows immediately. Q.E.D.

The next result is an analogue for Wiener—Hopf operators of the spectral inclusion theorem of HARTMAN and WINTNER [9] for Toeplitz operators.

Theorem 3.5. *If* $S\in\mathcal{M}^p$, $S=S(\sigma,p)$ *and* $W=\text{pr}\,(S)$, *then*

$$\text{ess range}\,\hat{\sigma}\subseteqq\text{sp}\,(S)\subseteqq\text{sp}\,(W).$$

Proof. By Theorem 2.3, $\text{sp}\,(S(\sigma,2))\subseteqq\text{sp}\,(S(\sigma,p))$ and, by Theorem 2.2, $S(\sigma,2)=U^{-1}M_{\hat{\sigma}}U$ so that $\text{sp}\,(S(\sigma,2))=\text{ess range}\,\hat{\sigma}$. Thus ess range $\hat{\sigma}\subseteqq\text{sp}\,(S)$.

To prove the second inclusion, it will suffice to show that S is invertible whenever W is invertible. So suppose that W is invertible. If $p=1$, then $\sigma\in M(R)$ and, by Theorem 1.1, $\sigma\in\exp\,(M(R))$. This implies that σ is invertible in $M(R)$ and that S is invertible. If $p=\infty$, the same conclusion follows by duality. Finally, if $1<p<\infty$, then the invertibility of S follows from Corollary 3.4 and the fact [5, Lemma 3 on p. 488] that an operator on a Banach space is invertible if and only if both the operator and its adjoint are bounded from below. Q.E.D.

If $W\in\mathcal{W}^p$, we know from Corollary 3.3 that W is induced by a unique multiplier $S\in\mathcal{M}^p$. We may therefore make the following definition: if $W\in\mathcal{W}^p$, we say that W is *analytic* (resp. *coanalytic*) if its inducing multiplier is analytic (resp. coanalytic). If $W=W(\sigma,p)$, it follows from Theorem 2.5 that W is analytic or coanalytic according as σ is analytic or coanalytic. Theorem 2.5 also implies that a multiplier or Wiener—Hopf operator which is both analytic and coanalytic is a scalar multiple of I or I_+ respectively.

We now turn to a consideration of the multiplicative properties of the class $\mathcal{W}^p$. If W_1, $W_2\in\mathcal{W}^p$ and either W_2 is analytic or W_1 is coanalytic, then $W_1W_2\in\mathcal{W}^p$. For if S_i is the multiplier inducing W_i, $i=1,2$, it is easily seen that

$$\text{pr}\,(S_1)\,\text{pr}\,(S_2)=\text{pr}\,(S_1S_2),$$

so that under these conditions W_1W_2 is the Wiener—Hopf operator induced by S_1S_2. Conversely, the stated conditions are necessary in order that the product W_1W_2 be a Wiener—Hopf operator.

Theorem 3.6. *Let $S_i \in \mathcal{M}^p$ and $W_i = \mathrm{pr}\,(S_i)$, $i=1, 2, 3$. In order that $W_1 W_2 = W_3$ it is necessary and sufficient that $S_1 S_2 = S_3$ and that either W_2 be analytic or W_1 be coanalytic.*

This result is the analogue for Wiener—Hopf operators of a well known theorem of Brown and Halmos [1, Theorem 8] for Toeplitz operators. Although the proof of Theorem 3.6 can be achieved by first reducing to the class $\mathcal{W}^2$ and then applying the theorem of Brown and Halmos to the corresponding Toeplitz operators, we prefer to give an independent proof. (The proof in [1] uses the existence of an orthonormal basis in Hilbert space to reduce to a matrix computation.) We require the following

Lemma 3.7. *Let $1 \leqq p < \infty$, K_0 be a right translation invariant subspace of $L^p(R^-)$ and let K be the smallest closed left translation invariant subspace of $L^p(R^-)$ containing K_0. Then either $K_0 = \{0\}$ or $K = L^p(R^-)$.*

Proof. The hypothesis that K_0 is right translation invariant means that K_0 is invariant under the operators QS_a for $a \geqq 0$. It is clear, then, that $\chi_{[-a,0]} f \in K$ whenever $f \in K_0$ and $a > 0$. Also, if $f \in K_0$, then almost every $x \in R^-$ is a p-th order Lebesgue point for f so that the condition

$$\lim_{h \to 0} \left(\frac{1}{h} \int_0^h |f(x-t) - f(x)|^p \, dt \right)^{1/p} = 0 \tag{3.1}$$

holds for almost every $x \in R^-$.

Suppose, now, that $K_0 \neq \{0\}$. From the hypothesis on K_0 it follows that we can choose some $f \in K_0$ such that $f(0) = 1$ and (3.1) holds for $x = 0$. In order to show that $K = L^p(R^-)$ it suffices to show that K contains the function $\chi_{[-a,0]}$ for each $a > 0$. So let $a > 0$ and consider the sequence of functions $\{g_n\}_{n=1}^{\infty}$ in $L^p(R^-)$, where

$$g_n = \sum_{k=0}^{n-1} S_{-ka/n}(\chi_{[-a/n,0]} f).$$

It is easy to see that the sequence $\{g_n\}_{n=1}^{\infty}$ is in K and that $\lim_{n \to \infty} \|g_n - \chi_{[-a,0]}\|_p = 0$. Since K is closed, it follows that $\chi_{[-a,0]} \in K$. Q.E.D.

Proof of Theorem 3.6. The remarks preceding the statement of the theorem show the sufficiency of the conditions and it remains to show that they are necessary. Moreover, the necessity of the conditions in the case $p = \infty$ follows from their necessity when $p = 1$ so that we need only consider the case $1 \leqq p < \infty$.

Suppose that $1 \leqq p < \infty$ and that $W_1 W_2 = W_3$. Since

$$(S_{-a} W_1 P S_a)(S_{-a} W_2 P S_a) = S_{-a} W_1 W_2 P S_a, \quad a \in R,$$

it follows from Theorem 3.2 that $S_1 S_2 = S_3$. Let K_0 be the range of $QS_2 P$ and $K = \{f \in L^p(R^-) \mid PS_1 f = 0\}$. It is clear that K_0 is a right translation invariant subspace of $L^p(R^-)$ and that K is a closed left translation invariant subspace of $L^p(R^-)$. Since $S_1S_2=S_3$, the hypothesis that $W_1W_2=W_3$ implies that $PS_1PS_2P=PS_1S_2P$. It follows that $PS_1QS_2P=0$ so that K contains K_0. By Lemma 3.7, either $K_0=\{0\}$ or $K=L^p(R^-)$. Thus, either S_2 is analytic or S_1 is coanalytic. Q.E.D.

Corollary 3.8. *A necessary and sufficient condition in order that an operator $W\in B(L^p(R^+))$ be an analytic (resp. coanalytic) Wiener—Hopf operator is that W commute with W_a (resp. W_{-a}) for $a\geqq 0$.*

Proof. By symmetry it is enough to prove the assertion in the analytic case. The necessity of the condition is immediate. So suppose, conversely, that $W\in B(L^p(R^+))$ and that $W_aW=WW_a$ for each $a\geqq 0$. Then $W=W_{-a}W_aW=W_{-a}WW_a$ for $a\geqq 0$ so that, by Theorem 3.1, $W\in\mathscr{W}^p$. Since W_a is analytic but not coanalytic if $a>0$, Theorem 3.6 and the equality $W_aW=WW_a$ imply that W is analytic. Q.E.D.

Corollary 3.9. *Let $S\in\mathscr{M}^p$, $W=\text{pr}(S)$ and S be analytic (resp. coanalytic). Then a necessary and sufficient condition in order that W be invertible is that S have an analytic (resp. coanalytic) inverse. If the condition is satisfied, $W^{-1}=\text{pr}(S^{-1})$.*

Proof. It is enough to consider the analytic case. Moreover, the sufficiency of the condition and the last assertion follow immediately from Theorem 3.6. So suppose, conversely, that S is analytic and that W is invertible. By Theorem 3.5, S is invertible. Since $S(L^p(R^+))=W(L^p(R^+))=L^p(R^+)$, it follows that S^{-1} is analytic. Q.E.D.

If T_φ is a non-zero Toeplitz operator on $H^2(R)$, COBURN [2] has shown that T_φ either has trivial kernel or dense range. The existence of an analogous result for Wiener—Hopf operators (induced by measures) was conjectured by DOUGLAS and TAYLOR [4]. The following theorem establishes such an analogue for Wiener—Hopf operators.

Theorem 3.10. *If $W\in\mathscr{W}^p$ and $W\neq 0$, then W either has trivial kernel or dense range (w^*-dense range if $p=\infty$).*

Proof. By duality, it is enough to prove the assertion in the case $1\leqq p\leqq 2$. So suppose that $1\leqq p\leqq 2$, $W\in\mathscr{W}^p$ and that W has non-trivial kernel and non-dense range. We will show that $W=0$.

Let $W=\text{pr}(S)$ where $S=S(\sigma,p)$. Since W has non-trivial kernel, we may choose $f\in L^p(R^+)$ such that $f\neq 0$ and $Sf\in L^p(R^-)$. Since W has non-dense range, $W^*=\text{pr}(S^*)$ has non-trivial kernel. Thus we may choose $g\in L^{p'}(R^+)$ such that $g\neq 0$ and $S^*g\in L^{p'}(R^-)$. Since $Sf, f^*\in L^p(R)$ and $S^*g, g\in L^{p'}(R)$, the convolutions $Sf*g^*$ and f^**S^*g are well defined continuous functions on R. Moreover, a straightforward computation shows that $Sf*g^*=(f^**S^*g)^*$. Since both $Sf*g^*$ and f^**S^*g vanish on R^+, it follows that $Sf*g^*=0$. Since $g^*\neq 0$ in $L^{p'}(R^-)$, we may apply Titchmarsh's convolution theorem [16, Theorem 153] to conclude that $Sf=0$

in $L^p(R)$. (We are grateful to Professor Donald Sarason for suggesting this use of the Titchmarsh convolution theorem to us.) By Theorem 2.4, $\hat{\sigma}\hat{f}=0$ in $L^{p'}(R)$ and, by Theorem 2.1, $\hat{f}\in H^{p'}(R)$. Since $f\neq 0$ in $L^p(R^+)$, $\hat{f}\neq 0$ in $H^{p'}(R)$ [11, p.142] and therefore $\hat{f}$ is non-zero a.e. [10, p. 133]. It follows that $\hat{\sigma}=0$ in $L^\infty(R)$. Thus $\sigma=0$ in $P(R)$ and $W=0$. Q.E.D.

4. The failure of factorization. The problem of finding conditions under which a Wiener—Hopf operator W will be invertible and, when the inverse exists, of providing an analytical representation for W^{-1}, has been of central importance in the theory of Wiener—Hopf operators. The principal tool for inverting a Wiener—Hopf operator has been the so-called *Wiener—Hopf technique*, first developed by N. WIENER and E. HOPF [17] in a somewhat different setting and applied by several subsequent authors to the Wiener—Hopf operators induced by various classes of measures [4], [8], [12]. In this section we will first describe the Wiener—Hopf technique in its general form and then provide an example showing its inadequacy — at least in the case $p=2$.

Let $S\in\mathcal{M}^p$ and suppose that S can be factored in the form $S=S_-S_+$ where $S_+, S_-\in\mathcal{M}^p$, S_+ is analytic and S_- is coanalytic. Then by Theorem 3.6, $\operatorname{pr}(S)=\operatorname{pr}(S_-)\operatorname{pr}(S_+)$. If, moreover, S_+ has an analytic inverse and S_- has a coanalitic inverse, then Corollary 3.9 implies that $\operatorname{pr}(S_+)$ and $\operatorname{pr}(S_-)$ are invertible and that

$$\operatorname{pr}(S)^{-1} = \operatorname{pr}(S_+^{-1})\operatorname{pr}(S_-^{-1}). \tag{4.1}$$

Formula (4.1) is called the *Wiener—Hopf formula* and suggests the following definition: if $W\in\mathcal{W}^p$ and W is invertible, we say that W^{-1} is *factorable* if there exist $W_+, W_-\in\mathcal{W}^p$ with W_+ analytic and W_- coanalytic such that $W^{-1}=W_+W_-$.

The case of Wiener—Hopf operators induced by measures is of particular interest. If $\mu\in\exp(M(R))$, then $\mu=\exp(\nu)$ for some $\nu\in M(R)$ and we can write $\nu=\nu_-+\nu_+$ where $\nu_\pm\in M(R^\pm)$. (This decomposition need not be unique.) Thus $\mu=\exp(\nu_-)*\exp(\nu_+)$, $\exp(\nu_\pm)\in M(R^\pm)$ and $\exp(\nu_\pm)^{-1}=\exp(-\nu_\pm)\in M(R^\pm)$. We therefore have

$$W(\mu,p)^{-1} = W(\exp(-\nu_+),p)W(\exp(-\nu_-),p).$$

Thus an exponential measure induces an invertible Wiener—Hopf operator whose inverse is factorable. The following result is of interest in relation to Theorem 1.1.

Theorem 4.1. *If $\mu\in M(R)$ and $W(\mu,p)$ is invertible, then a necessary and sufficient condition in order that $W(\mu,p)^{-1}$ be factorable with factors induced by measures is that $\mu\in\exp(M(R))$.*

Proof. The sufficiency of the condition has already been shown (see also [4]). Conversely, suppose that $W(\mu,p)^{-1}=W(\nu_+,p)W(\nu_-,p)$ for some $\nu_\pm\in M(R^\pm)$. Then

$$W(\mu,p)W(\nu_+,p)W(\nu_-,p) = I_+ = W(\delta_0,p).$$

By Theorem 3.6, we conclude that

$$W(\mu * \nu_+, p)W(\nu_-, p) = W(\delta_0, p).$$

Applying Theorem 3.6 yet again, we conclude that $\mu * \nu_+ \in M(R^-)$, $\mu * \nu_+ * \nu_- = \delta_0$ and that μ is invertible in $M(R)$. Since μ is invertible in $M(R)$, Theorem 1.1 implies that $\mu \in \exp(M(R))$. Q.E.D.

In view of the above, it is somewhat surprising that factorization should fail in the case $p=2$. For if $S \in \mathcal{M}^2$ and $W = \mathrm{pr}\,(S)$ is invertible, then we know that S must be invertible. Since $\mathcal{M}^2$ is isometrically and algebraically isomorphic to $P(R)$ and hence to $L^\infty(R)$, it follows that *the invertible elements in $\mathcal{M}^2$ are the same as the exponentials in $\mathcal{M}^2$*. Thus S has a logarithm $S(\sigma, 2)$ in $\mathcal{M}^2$. What goes wrong is that, in contrast to the case of measures, it may not be possible to write σ as the sum of an analytic and a coanalytic pseudomeasure [10, p. 151]. We shall not, however, base our example upon this fact, since logarithms in $\mathcal{M}^2$ are highly non-unique.

One further remark is in order. Factorization can be restored in the case $p=2$ provided that we do not require that the factors be induced by multipliers. If $S \in \mathcal{M}^2$ and $W = \mathrm{pr}\,(S)$ is invertible, then S is invertible and a theorem of Devinatz and Shinbrot [3, Theorem 5] implies that there exist invertible *operators* A_+ and A_- on $L^2(R)$ such that $S = A_- A_+$, $A_+(L^2(R^+)) = L^2(R^+)$, $A_-(L^2(R^-)) = L^2(R^-)$ and $W^{-1} = \mathrm{pr}\,(A_+^{-1})\,\mathrm{pr}\,(A_-^{-1})$.

If $f \in L^p(R)$, then in order that f have the same modulus as some nonzero element of $H^p(R)$ it is necessary and sufficient [10, p. 133] that

$$\int \frac{\log |f|}{1+t^2}\,dt > -\infty.$$

In constructing our example showing the failure of factorization in the case $p=2$ we shall make use of the fact that the argument of a nonzero element of $H^p(R)$ is, likewise, not arbitrary. To simplify matters, we introduce an auxiliary mapping. Let $Z(R)$ denote the multiplicative group of measurable functions on R which are nonzero a.e. and define the mapping u of $Z(R)$ into itself by setting $u(f) = f/|f|$ for each $f \in Z(R)$. For each, $f, g \in Z(R)$ we have

(i) $$u(fg) = u(f)u(g),$$

(ii) $$u(f^{-1}) = u(f)^{-1} = u(\bar{f}) = \overline{u(f)}.$$

(iii) $$u(u(f)) = u(f).$$

Note that $Z(R)$ contains $H^p(R) - \{0\}$.

Lemma 4.2. *If $f \in H^\infty(R) - \{0\}$, then $u(f^{-1}) = u(g)$ for some $g \in H^p(R) - \{0\}$ if and only if $f^{-1} \in H^p(R)$.*

Proof. Suppose that $f \in H^\infty(R) - \{0\}$ and that $u(f^{-1}) = u(g)$ for some $g \in H^p(R) - \{0\}$. Then $u(fg) = u(f)u(g) = u(f)u(f)^{-1} = 1$. Since $fg \in H^p(R)$, it follows that $fg = c$ for some positive constant c. Thus $f^{-1} = c^{-1} g \in H^p(R)$. Q.E.D.

Our example may now be constructed as follows: Let f be the continuous branch of $(x+i)^{1/3}$ on R with $0 < \arg(f) < \pi/3$. Then $f \notin H^\infty(R)$ and $f^{-1} \in H^\infty(R)$ so that, by Lemma 4.2,

$$u(f) \neq u(g) \quad \text{for each} \quad g \in H^\infty(R) - \{0\}. \tag{4.2}$$

Since $0 < \arg u(f) < \pi/3$, the closed convex hull of the essential range of $u(f)$ does not contain 0. From this it follows [1, p. 99] that the Toeplitz operator $T_{u(f)}$ is invertible on $H^2(R)$. Let σ be the pseudomeasure with $\hat{\sigma} = u(f)$ and let $W = W(\sigma, 2)$. Since W is unitarily equivalent to $T_{u(f)}$, W is invertible on $L^2(R^+)$.

Suppose, now, that W^{-1} is factorable. Then $W^{-1} = W(\sigma_+, 2)\,W(\sigma_-, 2)$ for some $\sigma_+, \sigma_- \in P(R)$ with σ_+ analytic and σ_- coanalytic. The equations

$$WW(\sigma_+, 2)W(\sigma_-, 2) = I_+ = W(\delta_0, 2), \quad W(\sigma_+, 2)W(\sigma, 2)W = I_+ = W(\delta_0, 2)$$

imply, as in the proof of Theorem 4.1, that $\sigma * \sigma_+ * \sigma_- = \delta_0$, that $\sigma_- * \sigma$ is an analytic inverse for σ_+ and that $\sigma * \sigma_+$ is a coanalytic inverse for σ_-. From this it follows that $u(f) = f_1 \bar{f}_2$ for some $f_1, f_2 \in H^\infty(R)$ with $f_1^{-1}, f_2^{-1} \in H^\infty(R)$. Then $u(f) = u(u(f)) = u(f_1)u(\bar{f}_2) = u(f_1)u(f_2^{-1}) = u(f_1 f_2^{-1})$. Since $f_1 f_2^{-1} \in H^\infty(R) - \{0\}$, this contradicts (4.2) and we conclude that W^{-1} is not factorable.

Before turning to the next section we comment on the example of Douglas and Taylor [4] mentioned in § 1. In this example, a noninvertible measure ν is constructed with the property that $\hat{\nu}$ and $\hat{\nu}^{-1}$ are in $H^\infty(R)$. It follows that ν has an analytic inverse $\sigma \in P(R)$ and that $S(\nu, 2)^{-1} = S(\sigma, 2)$. Thus, by Corollary 3.9, $W(\nu, 2)^{-1} = W(\sigma, 2)$ so that $W(\nu, 2)^{-1}$ is (trivially) factorable.

5. Interpolation of the inverse. We begin this section by exhibiting a measure ω such that $W(\omega, p)$ is invertible for $1 < p < \infty$ yet not invertible for $p = 1, \infty$. It is a consequence of the work of Krein [12] and of Gohberg and Feldman [8] that such a measure must necessarily have a nonzero singular continuous part. Our example is based on the fact [14, p. 107] that there exists a continuous positive measure $\nu \in M(R)$ such that $\|\nu\| = 1$, $\nu^* = \nu$ and $\pm i \in \operatorname{sp}(\nu)$. Let ν be such a measure and let $\omega = \delta_0 + \nu^2$. The measure ω has the remarkable property that $\hat{\omega} = 1 + |\hat{\nu}|^2 \geqq 1$ yet ω is not invertible in $M(R)$. Wiener and Pitt [18, Theorem 3] were the first to show the existence of measures exhibiting such spectral misbehavior and we shall therefore call ω the *Wiener—Pitt measure.*

Since ω is not invertible in $M(R)$, Theorem 1.1 implies that $W(\omega, 1)$ is not invertible. Since $\omega^* = \omega$, it follows that $W(\omega, \infty)$ is not invertible.

To show that $W(\omega, p)$ is invertible for $1<p<\infty$, it suffices to show that $W(\omega, p)$ is invertible for $1<p\leqq 2$. So let $1<p\leqq 2$ and set $\lambda=\lambda(p)$ so that $\frac{1}{p}=\lambda\frac{1}{1}+(1-\lambda)\frac{1}{2}$. Since $\hat{\omega}\geqq 1$ we may choose $0<\varepsilon<1$ so that $\|1-\varepsilon\hat{\omega}\|_\infty<1$. By the Riesz interpolation theorem [5, p. 525] and the Hölder inequality we have

$$\|I_+-\varepsilon W(\omega, p)\| = \|W(\delta_0-\varepsilon\omega, p)\| \leqq \|W(\delta_0-\varepsilon\omega, 1\|^\lambda \|W(\delta_0-\varepsilon\omega, 2)\|^{1-\lambda} \leqq$$
$$\leqq \lambda\|W(\delta_0-\varepsilon\omega, 1)\|+(1-\lambda)\|W(\delta_0-\varepsilon\omega, 2)\|.$$

By Corollary 3.3 and [13, Cor. 0.1.1] we have

$$\|W(\delta_0-\varepsilon\omega, 1)\| = \|S(\delta_0-\varepsilon\omega, 1)\| = \|\delta_0-\varepsilon\omega\|$$

and, by Corollary 3.3 and Theorem 2.2, we have

$$\|W(\delta_0-\varepsilon\omega, 2)\| = \|S(\delta_0-\varepsilon\omega, 2)\| = \|1-\varepsilon\hat{\omega}\|_\infty.$$

It follows that

$$\|I_+-\varepsilon W(\omega, p)\| < \lambda\|\delta_0-\varepsilon\omega\|+(1-\lambda) = \lambda\|(1-\varepsilon)\delta_0-\varepsilon\nu^2\|+(1-\lambda) \leqq$$
$$\leqq \lambda\big((1-\varepsilon)+\varepsilon\big)+(1-\lambda) = 1,$$

so that $W(\omega, p)$ is invertible.

By a considerable refinement of the argument just given we can prove the following.

Theorem 5.1. *If $\mu\in M(R)$ and K is the closed convex hull of the range of $\hat{\mu}$, then*

$$\operatorname{sp}\big(W(\mu, p)\big) \subseteqq \{z \mid \operatorname{dist}(z, K) \leqq \lambda(p)\|\mu'\|\},$$

where μ' denotes the measure $\mu-\mu(\{0\})\delta_0$.

Proof. Since $(\mu-z\delta_0)\hat{} = \hat{\mu}-z$ and $(\mu-z\delta_0)'=\mu'$, it is enough to prove that $W(\mu, p)$ is invertible for those p such that $\lambda(p)\|\mu'\|<\operatorname{dist}(0, K)$. If $0\in K$ there is nothing to prove, so suppose that $\operatorname{dist}(0, K)>0$ and that $\lambda(p)\|\mu'\|<\operatorname{dist}(0, K)$. By Parseval's formula we see that

$$\mu(\{0\}) = \lim_{a\to\infty}\int\frac{\operatorname{Sin}(ax)}{ax}\,d\mu(x) = \lim_{a\to\infty}\frac{1}{2a}\int_{-a}^{a}\hat{\mu}(x)\,dx,$$

so that $\mu(\{0\})\in K$ and hence $\mu(\{0\})\neq 0$. Without loss of generality we may assume that $\mu(\{0\})=1\in K$. Since K is a compact convex set, it follows that (for a suitable branch of $\arg(z)$) $\arg(K)=[\theta_1, \theta_2]$ where $\theta_1\leqq 0\leqq\theta_2$ and $\theta_2-\theta_1<\pi$ and that there exists a complex number z_0 with $|z_0|=1$ such that

$$\inf_{k\in K}\operatorname{Re}(\bar{z}_0 k) = \operatorname{dist}(0, K).$$

Since $\arg(K)=[\theta_1, \theta_2]$, it is evident that $z_0=\exp(i\theta_0)$ for some $\theta_0\in[\theta_1, \theta_2]$ satisfying

$$-\pi/2 < \theta_1-\theta_0 \leqq \theta_2-\theta_0 < \pi/2.$$

Since $\mu(\{0\})=1$, $\mu=\delta_0+\mu'$ and for each $\varepsilon>0$ we have

$$\|z_0\delta_0-\varepsilon\mu\| = \|(z_0-\varepsilon)\delta_0-\varepsilon\mu'\| = |z_0-\varepsilon|+\varepsilon\|\mu'\|.$$

It follows from elementary calculus that

$$\|z_0\delta_0-\varepsilon\mu\| = 1+\varepsilon\|\mu'\|-\varepsilon\,\mathrm{Cos}\,\theta_0+o(\varepsilon). \tag{5.1}$$

Now let $r_1=\inf_{k\in K}\mathrm{Re}\,(\bar{z}_0k)$ and $r_2=\sup_{k\in K}\mathrm{Re}\,(\bar{z}_0k)$. Since $\arg\,(K)=[\theta_1,\theta_2]$, it follows from the usual equation for a line in polar coordinates that

$$\sup_{k\in K}|z_0-\varepsilon k| = \sup_{k\in K}|1-\varepsilon\bar{z}_0k|$$

$$\leqq \sup_{r_1\leqq r\leqq r_2}\ \sup_{\theta_1\leqq\theta\leqq\theta_2}|1-\varepsilon e^{-i\theta_0}r\,\mathrm{Sec}\,(\theta-\theta_0)e^{i\theta}| \leqq \sup_{r_1\leqq r\leqq r_2}|1-\varepsilon r+i\varepsilon rm|,$$

where $m=\max\,\{\mathrm{Tan}\,(\theta_0-\theta_1),\ \mathrm{Tan}\,(\theta_2-\theta_0)\}$. By elementary calculus it follows that for $\varepsilon>0$ sufficiently small

$$\sup_{k\in K}|z_0-\varepsilon k| \leqq |1-\varepsilon r_1+i\varepsilon r_1m|,$$

from which it follows that

$$\|z_0-\varepsilon\hat{\mu}\|_\infty \leqq 1-\varepsilon r_1+o(\varepsilon). \tag{5.2}$$

By the same reasoning as in our example using the Wiener—Pitt measure we conclude from (5.1) and (5.2) that

$$\|z_0I_+-\varepsilon W(\mu,p)\| \leqq \lambda(p)\{1+\varepsilon\|\mu'\|-\varepsilon\,\mathrm{Cos}\,\theta_0\}+\big(1-\lambda(p)\big)\{1-\varepsilon r_1\}+o(\varepsilon).$$

Since $1\in K$ it follows that $r_1\leqq\mathrm{Cos}\,\theta_0$ and that

$$\|z_0I_+-\varepsilon W(\mu,p)\| \leqq 1+\varepsilon\big(\lambda(p)\,\|\mu'\|-r_1\big)+o(\varepsilon).$$

Since $\lambda(p)\|\mu'\|<\mathrm{dist}\,(0,K)=r_1$, it follows that $\|z_0I_+-\varepsilon W(\mu,p)\|<1$ for some $\varepsilon>0$ and hence that $W(\mu,p)$ is invertible. Q.E.D.

In view of Theorem 2.3, it seems natural to conjecture that if a Wiener—Hopf operator $W(\sigma,p)$ is invertible on $L^p(R^+)$, then the Wiener—Hopf operators $W(\sigma,r)$ for $\lambda(r)\leqq\lambda(p)$ are also invertible. If $\sigma\in M(R)$ and σ has no singular continuous part then the conjecture is true even without the restriction on r (cf. [8]). If $p=1$ or $p=\infty$, then the conjecture is also true and is a consequence of Theorem 1.1. Our example employing the Wiener—Pitt measure gives further support for this conjecture. We have been unable to prove this conjecture — even in the case of measures. However, it is quite easy to prove in the case of an analytic or coanalytic Wiener—Hopf operator. In a sense, therefore, the behavior exhibited in the example of Douglas and Taylor is typical of at least these two classes of Wiener—Hopf operators.

Theorem 5.2. *If $W(\sigma,p)$ is an analytic or coanalytic Wiener—Hopf operator and $W(\sigma,p)$ is invertible, then $W(\sigma,r)$ is invertible for $\lambda(r)\leqq\lambda(p)$.*

Proof. It suffices to give the proof in the analytic case. If $W(\sigma, p)$ is an invertible analytic Wiener—Hopf operator, then Corollary 3.9 implies that $S(\sigma, p)$ has an analytic inverse and we see that $S(\sigma, p)^{-1}=S(\sigma^{-1}, p)$ where σ^{-1} is the analytic inverse of σ in $P(R)$. If $\lambda(r)\leqq\lambda(p)$, then, by Theorem 2.3, $S(\sigma, r)$ is invertible and $S(\sigma, r)^{-1}=S(\sigma^{-1}, r)$. Since $S(\sigma^{-1}, r)$ is analytic, Corollary 3.9 implies that $W(\sigma, r)$ is invertible. Q.E.D.

References

[1] A. BROWN and P. R. HALMOS, Algebraic properties of Toeplitz operators, *J. reine angew. Math.*, **213** (1963), 89—102.

[2] L. A. COBURN, Weyl's theorem for nonnormal operators, *Michigan Math. J.*, **13** (1966), 285—288.

[3] A. DEVINATZ and M. SHINBROT, General Wiener-Hopf operators *Trans. Amer. Math. Soc.*, **145** (1969), 467—494.

[4] R. G. DOUGLAS and J. L. TAYLOR, Wiener-Hopf operators with measure kernels, *Proc. of Intern. Conf. on Operator Theory, Tihany, Hungary, 1970.*

[5] N. DUNFORD and J. T. SCHWARTZ, *Linear Operators*, Part I, Pure and Applied Mathematics, vol. **7**, Interscience (New York, 1958).

[6] P. DUREN, *Theory of H^p Spaces*, Pure and Applied Mathematics, vol. **38**, Academic Press (New York, 1970).

[7] R. E. EDWARDS, Supports and singular supports of pseudomeasures, *J. Austral. Math. Soc.*, **6** (1966), 65—75.

[8] I. C. GOHBERG and I. A. FELDMAN, Wiener-Hopf integral-difference equations (Russian), *Acta Sci. Math.*, **30** (1969), 199—224.

[9] P. HARTMAN and A. WINTNER, On the spectra of Toeplitz's matrices, *Amer. J. Math.*, **72** (1950), 359—366.

[10] K. HOFFMAN, *Banach Spaces of Analytic Functions*, Prentice-Hall (Englewood Cliffs N. J., 1962).

[11] Y. KATZNELSON, *Introduction to Harmonic Analysis*, John Wiley and Sons (New York, 1968).

[12] M. G. KREIN, Integral equations on a half-line with kernel depending upon the difference of the arguments, *Uspekhi Mat. Nauk*, **13**, n. 5 (1958), 3—120. (Russian)

[13] R. LARSEN, *Introduction to the Theory of Multipliers*, Springer-Verlag (Berlin, 1971).

[14] W. RUDIN, *Fourier Analysis on Groups*, Interscience (New York, 1962).

[15] W. RUDIN, *Real and Complex Analysis*, McGreaw-Hill (New York, 1966).

[16] E. C. TITCHMARSH, *Introduction to the Theory of Fourier Integrals*, Oxford Univ. Press (London, 1937).

[17] N. WIENER and E. HOPF, Über eine Klasse singulärer Integralgleichungen, *S.-B. Preuss. Akad. Wiss. Berlin, Math.-Phys. Klasse* (1931), 696—706. See also R. E. A. C. PALEY and N. WIENER, *Fourier Transforms in the Complex Domain*, Amer. Math. Soc. (New York, 1934).

[18] N. WIENER and R. H. PITT, On absolutely convergent Fourier-Stieltjes transforms, *Duke Math. J.*, **4** (1938), 420—436.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF KENTUCKY
LEXINGTON, KENTUCKY 40506

(Received December 12, 1973)

Modular lattices of locally finite length

By J. JAKUBÍK in Košice (ČSSR)

A lattice L is said to be of locally finite length if each bounded chain in L is finite. A sublattice S of L will be called a c-sublattice if, whenever $s_1, s_2 \in S$ and s_1 covers s_2 in S, then s_1 covers s_2 in L.

It is well-known that a lattice is modular if and only if it does not contain a sublattice isomorphic to the lattice A on Fig. 1 (this result goes back to DEDEKIND [3]; cf. also [1], [4], [6]). A relatively complemented lattice with the greatest element 1 and the least element 0 is modular if and only if it does not contain a sublattice S isomorphic to the lattice on Fig. 1 such that $0 \in S$ and $1 \in S$ (SZÁSZ [7]). A finite lattice is nonmodular if and only if it contains a lattice on Fig. 1 as a sublattice such that a covers b (cf. GRÄTZER [4], p. 151). Other conditions for a lattice to be modular were established by CROISOT [2].

The following result on finite modular lattices is known (cf. GRÄTZER [4], p. 151):

(*) Let L be a finite modular lattice. Then L is nondistributive if and only if it contains the lattice on Fig. 4 as a sublattice such that a, b, and c cover u and v covers a, b, and c.

Thus distributive lattices in the class of finite modular lattices can be characterized by means of c-sublattices.

The purpose of this note is to characterize modular lattices in the class of lattices of locally finite length by means of their c-sublattices. A nonmodular lattice of locally finite length need not contain a c-sublattice isomorphic to the lattice A on Fig. 1. Let B be the lattice on Fig. 2 and let B' be the lattice dual to B. We denote by $L(m, n)$ the lattice on Fig. 3 ($m \geqq 3, n \geqq 4$). Further let C be the lattice on Fig. 4. The following theorems will be proved:

Theorem 1. *Let L be a lattice of locally finite length. Then L is modular if and only if L does not contain a sublattice isomorphic to some of the following lattices:* $B, B', L(m, n)$ ($m \geqq 3$, $n \geqq 4$).

Corollary. (ŠIK [5].) *A lattice of locally finite length fulfilling the upper covering condition is modular if and only if it does not contain a sublattice isomorphic to B.*

Theorem 2. *Let L be a lattice of locally finite length. Then L is distributive if and only if it does not contain a c-sublattice isomorphic with some of the following lattices:* B, B', $L(m, n)(m \geqq 3,\ n \geqq 4)$, C.

The standard terminology of the lattice theory will be used (cf. [1], [4], [6]). The lattice operations will be denoted by $\wedge$, $\vee$. Let L be a lattice, $a, b \in L$, $a \leqq b$. The interval $[a, b]$ is the set $\{x \in L: a \leqq x \leqq b\}$. If $a < b$ and $[a, b] = \{a, b\}$, then $[a, b]$ is called a prime interval; in this case b covers a (and a is covered by b).

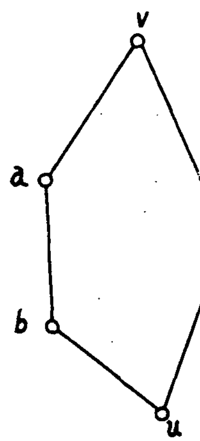


Fig. 1

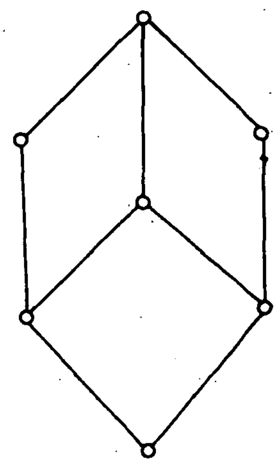


Fig. 2

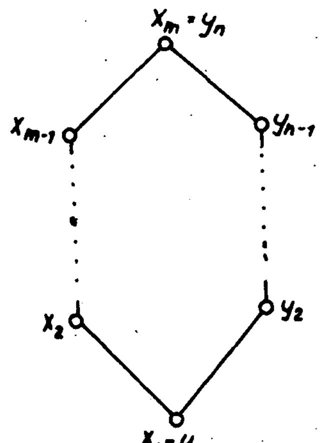


Fig. 3

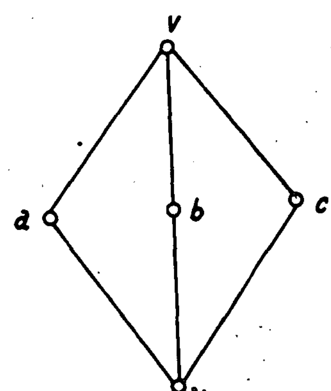


Fig. 4

If two elements x, y of a lattice are uncomparable, we write $x|y$. Let m, n be positive integers, $m\geqq 3$, $n\geqq 4$. We denote by $L(m, n)$ a lattice with elements $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n$ such that $x_1=y_1$, $x_m=y_n$, $x_i<x_{i+1}$ $(i=1, \ldots, m-1)$, $y_j<y_{j+1}$ $(j=1, \ldots, n-1)$, $x_i|y_j$ $(i=2, 3, \ldots, m-1;\ j=2, 3, \ldots, n-1)$ (cf. Fig. 3).

Let L be a lattice of locally finite length. We denote by M_1 the set of all intervals $[u, v]$ of L such that there are elements $a, b\in[u, v]$, $a|b$ fulfilling the conditions:

(i) both a and b are covered by v;

(ii) $u=a\wedge b$ and either a or b does not cover u.

Let M_2 be defined dually and put $M=M_1\cup M_2$. The set M is partially ordered by the inclusion. Since L is of locally finite length, M satisfies the descending chain condition. If L is nonmodular, then we have $M\neq\emptyset$ and hence the set M_0 of all minimal elements of M is nonempty.

Let us recall that if K is a bounded lattice of locally finite length and if L is modular, then any two maximal chains in K have the same number of elements (cf. [1]).

Proof of Theorem 1.

The lattices B, B', $L(m, n)$ $(m\geqq 3, n\geqq 4)$ being nonmodular, it suffices to verify the assertion "only if".

Assume that L is nonmodular. Then $M_0\neq\emptyset$. Let $[u, v]$ be a fixed element of M_0. We may suppose that $[u, v]\in M_1$ (in the case $[u, v]\in M_2$ we would apply a dual method). Let a, b be as in (i) and (ii).

Let $u=x_1<\ldots<x_{m-1}=a$, $u=y_1<\ldots<y_{n-1}=b$ be two maximal chains in $[u, a]$, $[u, b]$, respectively. In case $x_2\vee y_2=v$ the set $N_1=\{u, v, x_2, \ldots, x_{m-1}, y_2, \ldots, y_{n-1}\}$ is a c-sublattice isomorphic to $L(m, n)$, $m\geqq 3$, $n\geqq 3$ and by (ii), either m or n is $\geqq 4$. Therefore N_1 is isomorphic to one of the lattices listed in the Theorem.

Suppose that $x_2\vee y_2=v_1<v$. Then $[u, v_1]$ is a proper subset of $[u, v]$, both x_2 and y_2 cover u, thus with respect to the minimality of $[u, v]$ in M it follows, that v_1 covers both x_2 and y_2, as well. Obviously $x_2|b$ and $y_2|a$. Therefore

(1) $v_1\vee a = v_1\vee b = v$, (2) $v_1\wedge a = x_2$, $v_1\wedge b = y_2$, (3) $x_2\vee b = y_2\vee a = v$.

From (1)—(3) it follows that the set $N_2=\{a, b, u, v, x_2, y_2, v_1\}$ is a sublattice of L isomorphic to B.

From the minimality of $[u, v]$ it follows that the lattices $[x_2, v]$ and $[y_2, v]$ are modular. Let $\bar{v}\in[v_1, v]$ such that $\bar{v}$ covers v_1. Let $\bar{a}=\bar{v}\wedge a$, $\bar{b}=\bar{v}\wedge b$.

Because of the modularity of $[x_2, v]$ and $[y_2, v]$ both $\bar{a}$ and $\bar{b}$ are covered by $\bar{v}$, furthermore $\bar{a}|\bar{b}$, $\bar{a}\wedge\bar{b}=u$ and neither $\bar{a}$ nor $\bar{b}$ covers u. Hence $[u, \bar{v}]\in M$ and $[u, \bar{v}]\subseteq[u, v]$, i.e., $[u, \bar{v}]=[u, v]$; $\bar{v}=v$.

Thus we proved that v covers v_1; therefore a covers x_2 and b covers y_2 which proves that N_2 is a c-sublattice. Q.e.d.

Lemma. *Let L be a non-distributive modular lattice fulfilling the descending chain condition. Then L contains a c-sublattice isomorphic to C.*

Remark. Since a distributive lattice can not contain any sublattice isomorphic to C, this Lemma generalizes the statement $(*)$ to modular lattices fulfilling the descending chain condition.

Proof of the Lemma. In fact, $C=\{u, a, b, c, v\}$ $(u \leqq a, b, c \leqq v)$ is a sublattice of L. Let $\bar{a} \in [u, a]$ such that $\bar{a}$ covers u. Set

$$\bar{v} = (\bar{a} \vee b) \wedge (\bar{a} \vee c), \quad \bar{b} = b \wedge (\bar{a} \vee c), \quad \bar{c} = c \wedge (\bar{a} \vee b).$$

Clearly $\bar{b} = \bar{v} \wedge b$ and $\bar{c} = \bar{v} \wedge c$. Using the projectivity it follows easily that all intervals $[\bar{a}, \bar{v}]$, $[\bar{b}, \bar{v}]$, $[\bar{c}, \bar{v}]$, $[u, \bar{b}]$, $[u, \bar{c}]$ are prime. From this we obtain that the set $C = \{u, \bar{a}, \bar{b}, \bar{c}, \bar{v}\}$ is a c-sublattice of L isomorphic to C. The proof of Theorem 2 follows immediately from Lemma and Theorem 1.

Added in proof. Theorem 1 can be deduced also from Thm. 2.2 of V. Vilhelm, Двойственное себе ядро условий Биркгофа в структурах с конечными цепями, *Czech. Math. J.*, **5** (1955), 439—450.

References

[1] G. Birkhoff, *Lattice theory*, second edition (Providence, 1948).
[2] R. Croisot, Axiomatique des treillis modulaires, *C. R. Acad. Sci. Paris*, **231** (1950), 12—14.
[3] R. Dedekind, Über die von drei Moduln erzeugte Dualgruppe, *Math. Annalen*, **53** (1900), 371—403.
[4] G. Grätzer, *Lattice theory* (San Francisco, 1971).
[5] F. Šik, A note on the modular lattices of locally finite length (preprint).
[6] G. Szász, *Einführung in die Verbandstheorie* (Budapest—Leipzig, 1962).
[7] G. Szász, On complemented lattices, *Acta Sci. Math.*, **19** (1958), 77—81.

(Received December 27, 1973, revised March 18, 1974)

Equational classes of rings generated by zero rings and Galois fields

By LEE SIN-MIN in Winnipeg (Canada)

H. WERNER and R. WILLE [6] gave some characterization of those equational classes of rings in which the lattice of congruences of every ring is distributive. They showed that these are precisely the equational classes of rings generated by a finite set of Galois fields, and they also gave a set of identities characterizing these equational classes.

We give in this note a characterization of the equational class of rings generated by all zero rings and a finite number of Galois fields. A ring in such an equational class is a directed sum of its Jacobson radical $J(R)$, which is a zero ring, and its semisimple part, $R/J(R)$. We also consider the lattice of equational subclasses of this equational class and show that it is distributive.

1. Characterization of $\mathcal{R}_g(P, N)\vee\mathcal{C}_0$.

Let π be the set of all primes, $\mathcal{N}^+$ the set of positive integers, and $\mathcal{P}(\mathcal{N}^+)$ the set of all non-empty finite subsets of $\mathcal{N}^+$.

Let P be a fixed, non-empty, finite subset of π and consider a mapping $N: P\to\mathcal{P}(\mathcal{N}^+)$, i.e., N associates with every $p\in P$ an $N(p)\in\mathcal{P}(\mathcal{N}^+)$. Denote by $\mathcal{R}_g(P, N)$ the equational class of rings generated by the set $\{GF(p^k)\,|\,p\in P,\ k\in N(p)\}$ of Galois fields.

For $S\in\mathcal{P}(\mathcal{N}^+)$ write $\Pi S=n_1\dots n_k$ if $S=\{n_1, \dots, n_k\}$, and define $\Pi\emptyset=1$ for the empty set $\emptyset$.

With every element x of a ring we associate the element

$$x^*=\sum_{p\in P}\Big(\prod_{q\in P-\{p\}} q\Big)^{p^{n(p)}-1} x^{p^{n(p)}},$$

where $n(p)=\Pi N(p)$.

Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be two equational classes of algebras of the same type, $\mathcal{K}_1$ and $\mathcal{K}_2$ are independent if there exists a binary polynomial symbol $\mathbf{p}(x, y)=x$ is an identity in $\mathcal{K}_1$ and $\mathbf{p}(x, y)=y$ is an identity in $\mathcal{K}_2$.

G. GRÄTZER, H. LAKSER and J. PLONKA [1] showed that if $\mathscr{K}_1$ and $\mathscr{K}_2$ are independent, then every algebra in $\mathscr{K}_1 \vee \mathscr{K}_2$ (the smallest equational class of algebras containing $\mathscr{K}_1$ and $\mathscr{K}_2$) is the direct product of an algebra in $\mathscr{K}_1$ and another in $\mathscr{K}_2$. If, in addition, each algebra $\mathscr{A}$ of $\mathscr{K}_1 \vee \mathscr{K}_2$ has a modular congruence lattice then each $\mathscr{A} \in \mathscr{K}_1 \vee \mathscr{K}_2$ has, up to isomorphism, a unique representation $\mathscr{A} = \mathscr{A}_1 \times \mathscr{A}_2$ where $\mathscr{A}_1 \in \mathscr{K}_1$ and $\mathscr{A}_2 \in \mathscr{K}_2$.

Let $\mathscr{C}_0$ denote the class of all zero rings, i.e. $\mathscr{C}_0$ consists of all rings satisfying $xy=0$.

Theorem 1. *$\mathscr{R}_g(P, N)$ and $\mathscr{C}_0$ are independent equational classes of rings.*

Proof. $\mathscr{R}_g(P, N)$ is defined by the identities $x^*=x$ and $x \prod_{p\in P} \prod_{n\in N(p)} (x^{p^n}-x)=0$ (see [6]). In $\mathscr{R}_g(P, N)$, $(\Pi P)x=0$ for all $x \in R \in \mathscr{R}_g(P, N)$. Then consider the binary polynomial $\mathbf{p}(x, y)=x^*+y+(\Pi P-1)y^*$.

The object of this note is to prove the following result:

Theorem 2. *The following statements are equivalent:*

(1) $R \in \mathscr{R}_g(P, N) \vee \mathscr{C}_0$,

(2) $R \cong B \times C$, $B \in \mathscr{R}_g(P, N)$, $C \in \mathscr{C}_0$ *and this representation is unique,*

(3) *R satisfies the identities:*

(a) $xy = yx$, (b) $(\Pi P)(xy) = 0$, (c) $(xy)^* = xy$, (d) $(x-x^*)^2 = 0$,

(e) $x \prod_{p\in P} \prod_{n\in N(p)} (x^{p^n}-x) = 0$, (f) $2\big(\prod_{p\in P-\{2\}} q\big)^{2^{n(2)}-1} x^{2^{n(2)}} = 0$ (if $2\in P$).

Proof. The equivalence of (1) and (2) follows immediately from Theorem 1 and the result of GRÄTZER, LAKSER and PLONKA [1] mentioned above, and also the fact that the congruence lattices of rings are modular.

(2)⇒(3) is a routine calculation.

(3)⇒(2). Let $B=\{x\in R \mid x^*=x\}$, $C=\{x\in R \mid x^2=0\}$. Claim: B and C are ideals of R.

Let $x, y \in B$, then

$$(x+y)^* = \sum_{p\in P} \Big(\prod_{q\in P-\{p\}} q\Big)^{p^{n(p)}-1} \left(x^{p^{n(p)}} + \sum_{i=1}^{p^{n(p)}-1} \binom{p^{n(p)}}{i} x^{p^{n(p)}-i} y^i + y^{p^{n(p)}}\right) =$$

$$= x^* + \sum_{p\in P} \sum_{i=1}^{p^{n(p)}-1} \Big(\prod_{q\in P-\{p\}} q\Big)^{p^{n(p)}-1} \binom{p^{n(p)}}{i} x^{p^{n(p)}-i} y^i + y^*.$$

Since ΠP divides $\big(\prod_{q\in P-\{p\}} q\big)^{p^{n(p)}-1} \binom{p^{n(p)}}{i}$, using (b) we have immediately $(x+y^*)= =x^*+y^*=x+y$ and hence $x+y\in B$. If $2\in P$, then $(-x)^*=-x$ follows from (f). If $2 \notin P$, then $(-x)^{p^{n(p)}}=(-1)x^{p^{n(p)}}$ and so $(-x)^*=-x$. Therefore $-x\in B$ for any

$x\in B$. Now by condition (c) it is obvious that $rx\in B$ for any $x\in B$ and $r\in R$. Thus B is an ideal of R.

C is an ideal. For, if $x, y\in C$ and $r\in R$ then

$$(x+y)^2 = x^2+2xy+y^2 = 2(xy)^* = 2\cdot 0 = 0,$$
$$rx = (rx)^* = \sum_{p\in P}\Big(\prod_{q\in P-\{p\}} q\Big)^{p^{n(p)}-1} r^{p^{n(p)}} x^{p^{n(p)}} = 0,$$

thus C is an ideal of R and it is also a zero ring.

Now for each $x\in R$ we have

$$\begin{aligned}(x^*)^* &= \Big(\sum_{p\in P}\Big(\sum_{q\in P-\{p\}} q\Big)^{p^{n(p)}-1} x^{p^{n(p)}}\Big)^* \\ &= \Big(x\sum_{p\in P}\Big(\sum_{q\in P-\{p\}} q\Big)^{p^{n(p)}-1} x^{p^{n(p)}-1}\Big)^* \\ &= x\sum_{p\in P}\Big(\prod_{q\in P-\{p\}} q\Big)^{p^{n(p)}-1} x^{p^{n(p)}-1} \quad \text{by (c)} \\ &= x^*.\end{aligned}$$

Therefore $x^*\in B$ and by condition (d) $x-x^*\in C$. Since $B\cap C=\{0\}$ and $x=x^*+x-x^*$ we have $R=B\oplus C$.

Remark. Let $n\geqq 2$. Let $P=\{p\in\pi \mid p^r-1\mid n-1$ for some $r\geqq 1\}$ and $N(p)= =\{r\in\mathcal{N}^+ \mid p^r-1\mid n-1\}$ for each $p\in P$. The equational class of rings $\mathcal{R}_g(P, N)$ is defined by the identity $x^n=x$. (See L. LESIEUR [5] Théorème 6.)

We have shown in [4], the equational class $\mathcal{R}_g(P, N)\vee\mathcal{C}_0$ is defined by the identities $(x+y)^n=x^n+y^n$, $(xy)^n=xy=x^n y^n$.

2. Lattice of equational subclasses of $\mathcal{R}_g(P, N)\vee\mathcal{C}_0$.

It is an easy consequence of a result in [1] that if $\mathcal{K}_1$ and $\mathcal{K}_2$ are two independent equational classes of algebras of the same type, then the lattice $\mathcal{L}(\mathcal{K}_1\vee\mathcal{K}_2)$ of equational subclasses of $\mathcal{K}_2\vee\mathcal{K}_1$ is isomorphic to the direct product of $\mathcal{L}(\mathcal{K}_1)$ and $\mathcal{L}(\mathcal{K}_2)$.

Thus $\mathcal{L}(\mathcal{R}_g(P, N)\vee\mathcal{C}_0)\cong\mathcal{L}(\mathcal{R}_g(P, N))\times\mathcal{L}(\mathcal{C}_0)$.

Now all rings in $\mathcal{R}_g(P, N)$ have distributive congruence lattices (see [4]). A well-known result of B. JONSSON [2], Corollary 4.2, states that if $\mathcal{K}$ is an equational class of algebras such that each algebra in it has distributive congruence lattice, then $\mathcal{L}(\mathcal{K})$ is distributive. We conclude that $\mathcal{L}(\mathcal{R}_g(P, N))$ is distributive.

$\mathcal{L}(\mathcal{C}_0)$ is obviously distributive. The above results are summarized in

Theorem 3. *$\mathcal{L}(\mathcal{R}_g(P, N)\vee\mathcal{C}_0)$ is distributive and isomorphic to the direct product of $\mathcal{L}(\mathcal{R}_g(P, N))$ and $\mathcal{L}(\mathcal{C}_0)$.*

Finally the author wishes to thank Professor G. Grätzer for his encouragement during the preparation of this note.

Bibliography

[1] G. GRÄTZER, H. LAKSER and J. PLONKA, Direct product and joins of algebras, *Bull. Canad. Math. Soc.*, **12** (1969), 741—744.

[2] B. JONSSON, Algebras whose congruence lattices are distributive, *Math. Scand.*, **21** (1967), 110—121.

[3] LEE SIN-MIN, Equational classes of rings generated by all zero rings and finite number of Galois fields. *Notices of Amer. Math. Soc.*, **18** (1971), 71T—A63.

[4] LEE SIN-MIN, Semigroups and rings satisfying $(xy)^n = xy = x^n y^n$, *Nanta Mathematica*, VI: 1 (January—June 1973), 21—28.

[5] L. LESIEUR, Sur les anneaux tels que $x^n = x$, *Séminaire Dubreil-Pisot: Algèbre et Théorie des nombres, 19 années* (1965/66).

[6] H. WERNER and R. WILLE, Charactcrisierungen der primitiven Klassen arithmetischer Ringe, *Math. Z.*, **115** (1970), 197—200.

THE UNIVERSITY OF MANITOBA
WINNIPEG 19, MANITOBA, CANADA

Present address:
UNIVERSITÉ DE PARIS-SUD, BÂTIMENT 425
91405 ORSAY, FRANCE.

(Received February 7, 1972)

On the strong approximation of orthogonal series

By L. LEINDLER in Szeged

Dedicated to Professor Károly Tandori on his 50th birthday

Introduction

Let $\{\varphi_n(x)\}$ be an orthogonal system on the interval (a, b). We consider the orthogonal series

$$\sum_{n=0}^{\infty} c_n \varphi_n(x) \quad \text{with} \quad \sum_{n=0}^{\infty} c_n^2 < \infty. \tag{1}$$

It is well known that the series (1) converges in L^2 to a square-integrable function $f(x)$. Let us denote the partial sums and the (C, α)-means of the series (1) by $s_n(x)$ and $\sigma_n^\alpha(x)$, respectively.

In [2] we proved that *if*

$$\sum_{n=1}^{\infty} c_n^2 n^{2\gamma} < \infty \quad \text{and} \quad 0 < \gamma < 1, \tag{2}$$

then

$$f(x) - \sigma_n^1(x) = o_x(n^{-\gamma})$$

almost everywhere in (a, b).

G. SUNOUCHI [4] generalized this result proving that *if* (2) *is satisfied, then*

$$\left\{\frac{1}{A_n^\alpha} \sum_{\nu=0}^{n} A_{n-\nu}^{\alpha-1} |f(x) - s_\nu(x)|^k\right\}^{1/k} = o_x(n^{-\gamma}) \tag{3}$$

holds almost everywhere in (a, b) *for any* $\alpha > 0$ *and* $0 < k < \gamma^{-1}$, *where* $A_n^\alpha = \binom{n+\alpha}{n}$.

This result was generalized in [3] in such a way that *we replaced the partial sums in* (3) *by* (C, δ)*-means, where* δ *can also be negative.* (See Theorem 1 of [3].)

In [3] (Theorem 2) we also proved that *if* $\sum_{n=1}^{\infty} c_n^2 n^{2\alpha} < \infty$ *with any positive* γ, *then*

$$\left\{\frac{1}{n} \sum_{\nu=n}^{2n} |s_\nu(x) - f(x)|^k\right\}^{1/k} = o_x(n^{-\gamma}) \tag{4}$$

holds almost everywhere in (a, b) *for any* $0 < k \leq 2$.

The aim of the present paper is to generalize further these results.

We consider a regular summation method T_n determined by a triangular matrix $\|\alpha_{nk}/A_n\|$ $\left(\alpha_{nk}\geqq 0 \text{ and } A_n=\sum_{k=0}^{n}\alpha_{nk}\right)$, i.e. if s_k tends to s, then

$$T_n=\frac{1}{A_n}\sum_{k=0}^{n}\alpha_{nk}s_k \to s.$$

Theorem I. *Suppose that* $0<\gamma<1$ *and* $0<k<\gamma^{-1}$,

$$\sum_{n=1}^{\infty}c_n^2 n^{2\gamma}<\infty, \tag{5}$$

furthermore that there exists a number $p>1$ *such that*

$$\frac{p}{p-1}k\geqq 2 \tag{6}$$

and with this p for any $0<\delta<1$ *and* $2^m<n\leqq 2^{m+1}$

$$\sum_{l=0}^{m}\left\{\sum_{\nu=2^l-1}^{\min(2^{l+1},n)}\alpha_{n\nu}^p(\nu+1)^{p(1-\delta)-1}\right\}^{1/p}\leqq K\left(\sum_{\nu=0}^{n}\alpha_{n\nu}\right)n^{-\delta}.\text{[1)]} \tag{7}$$

Then for arbitrary

$$\beta>1-\frac{p-1}{pk} \tag{8}$$

we have

$$\left\{\frac{1}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|f(x)-\sigma_\nu^{\beta-1}(x)|^k\right\}^{1/k}=o_x(n^{-\gamma}) \tag{9}$$

almost everywhere in (a, b).

It is easy to verify that in the special case $\alpha_{n\nu}=A_{n-\nu}^{\alpha-1}$ $(\alpha>0)$ condition (7) is satisfied, thus with $\beta=1$ Theorem I contains the result of SUNOUCHI. It can be shown that Theorem I includes our result in connection with (C, δ)-means of negative order, too. Furthermore we have some corollaries:

Corollary 1. *Suppose that* $0<\gamma<1$, $0<k<\gamma^{-1}$, *and that* (5) *is satisfied. Then we have*

$$\left\{\frac{1}{n}\sum_{\nu=n}^{2n}|f(x)-\sigma_\nu^{\beta-1}(x)|^k\right\}^{1/k}=o_x(n^{-\gamma})$$

for any $\beta>1-\min(1/2, 1/k)$ *almost everywhere in* (a, b).

Corollary 2. *Under the hypothesis of Theorem 1 we have*

$$\left\{\frac{1}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|f(x)-\sigma_\nu^{\beta-1}(\{\mu_i\}; x)|^k\right\}^{1/k}=o_x(n^{-\gamma})$$

[1)] $K, K_1, K_2, \ldots$ will denote positive constants not necessarily the same at each occurrence.

almost everywhere in (a, b) *for any* $\beta > 1-(p-1)/pk$ *and for any increasing sequence* $\{\mu_i\}$; *where*

$$\sigma_n^\alpha(\{\mu_i\}; x) = \frac{1}{A_n^\alpha} \sum_{\nu=0}^{n} A_{n-\nu}^{\alpha-1} s_{\mu_i}(x).$$

From Corollary 2 in the special case $\beta=1$ we obtain immediately

Corollary 3. *Under the conditions of Theorem 1 we have*

$$\left\{\frac{1}{A_n} \sum_{\nu=0}^{n} \alpha_{n\nu} |f(x)-s_{\mu_\nu}(x)|^k\right\}^{1/k} = o_x(n^{-\gamma}) \tag{10}$$

almost everywhere in (a, b) *for any increasing sequence* $\{\mu_\nu\}$.

In the special case $\alpha_{n\nu}=A_{n-\nu}^{\alpha-1}$ $(\alpha>0)$ Corollary 3 reduces to Theorem 3 of [3].

Under the restrictions $0<k\leqq 2$ and $\beta=1$, but for arbitrary positive γ, Corollary 1 can be generalized to very strong approximation. In fact we have

Theorem II. *Suppose that* $0<k\leqq 2$ *and* $\gamma>0$; *and that* (5) *holds. Then*

$$\left\{\frac{1}{n} \sum_{\nu=n}^{2n} |s_{\mu_\nu}(x)-f(x)|^k\right\}^{1/k} = o_x(n^{-\gamma}) \tag{11}$$

almost everywhere in (a, b) *for any increasing sequence* $\{\mu_\nu\}$.

It is clear that (11) is a generalized form of (4).

Finally we show that under certain restrictions on γ, and $\{c_n\}$ an estimate similar to (10) can be given with any not necessarily monotonic sequence $\{l_\nu\}$ of distinct non-negative integers. Namely we have

Theorem III. *Suppose that* $0<\gamma<1/2$, $0<k\leqq 2$ *and*

$$\sum_{n=4}^{\infty} c_n^2 n^{2\gamma} (\log\log n)^2 < \infty, \tag{12}$$

furthermore that

$$\left\{\sum_{\nu=0}^{n} (\alpha_{n\nu})^{2/(2-k)}\right\}^{(2-k)/2} \leqq K\left(\sum_{\nu=0}^{n} \alpha_{n\nu}\right) n^{-k/2}. \tag{13}$$ [2]

Then we have

$$\left\{\frac{1}{A_n} \sum_{\nu=0}^{n} \alpha_{n\nu} |s_{l_\nu}(x)-f(x)|^k\right\}^{1/k} = o_x(n^{-\gamma}) \tag{14}$$

almost everywhere in (a, b) *for any (not necessarily monotonic) sequence* $\{l_\nu\}$ *of distinct non-negative integers.*

Theorem III gives immediately

---

[2]) If $k=2$ then (13) means that $\max\limits_{0\leqq\nu\leqq n} \alpha_{n\nu} \leqq K\left(\sum_{\nu=0}^{n} \alpha_{n\nu}\right) n^{-1}$.

Corollary 4. *If* $0<\gamma<1/2$, $0<k\leqq 2$ *and* $\alpha>k/2$, *furthermore* (12) *is satisfied, then*

$$\left\{\frac{1}{A_n^\alpha}\sum_{\nu=0}^{n} A_{n-\nu}^{\alpha-1}|s_{l_\nu}(x)-f(x)|^k\right\}^{1/k} = o_x(n^{-\gamma})$$

almost everywhere in (a, b) *for any (not necessarily monotonic) sequence* $\{l_\nu\}$ *of distinct non-negative integers.*

§ 1. Lemmas

We require the following lemmas.

Lemma 1 ([1], p. 359). *Let* $r\geqq l>1$, $\bar{\gamma}>0$, $\bar{\alpha}>\bar{\gamma}-1$ *and* $\bar{\beta}\geqq\bar{\alpha}+l^{-1}-r^{-1}$. *Then*

$$\left\{\sum_{n=0}^{\infty}(n+1)^{r\bar{\gamma}-1}|\tau_n^{\bar{\beta}}(x)|^r\right\}^{1/r}\leqq K\left\{\sum_{n=0}^{\infty}(n+1)^{l\bar{\gamma}-1}|\tau_n^{\bar{\alpha}}(x)|^l\right\}^{1/l},$$

where $\tau_n^\alpha(x)=\alpha\big(\sigma_n^{\alpha-1}(x)-\sigma_n^\alpha(x)\big)$.

Lemma 2 ([4], Lemma 1). *If*

$$\sum_{n=1}^{\infty} c_n^2 n^{2\gamma}<\infty \quad \textit{with} \quad 0<\gamma<1,$$

then

$$\int_a^b\left\{\sum_{n=0}^{\infty}(n+1)^{2\gamma-1}|\sigma_n^{\alpha-1}(x)-\sigma_n^\alpha(x)|^2\right\}dx\leqq K\sum_{n=1}^{\infty}c_n^2 n^{2\gamma}$$

for any $\alpha>1/2$.

Lemma 3 ([3], Theorem 4). *If* $0<\gamma\leqq 1/2$, $0<k\leqq 2$, $k\gamma<1$ *and*

$$\sum_{n=4}^{\infty}c_n^2 n^{2\gamma}(\log\log n)^2<\infty,$$

then

$$\left\{\frac{1}{n}\sum_{\nu=0}^{n}|s_{l_\nu}(x)-f(x)|^k\right\}^{1/k}=o_x(n^{-\gamma}) \tag{1.1}$$

almost everywhere in (a, b) *for any (not necessarily monotonic) sequence* $\{l_\nu\}$ *of distinct non-negative integers.*

Lemma 4. *Under the conditions of Theorem I we have the inequality*

$$\int_a^b\left\{\sup_{0\leqq n<\infty}\left(\frac{n^{k\gamma}}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\sigma_\nu^{\beta-1}(x)-\sigma_\nu^\beta(x)|^k\right)^{1/k}\right\}^2dx\leqq K\sum_{n=1}^{\infty}c_n^2n^{2\gamma}. \tag{1.2}$$

Proof of Lemma 4. Set $q=p/(p-1)$, then

$$qk\geqq 2 \quad\text{and}\quad \beta>1-\frac{1}{qk}. \tag{1.3}$$

Applying Hölder's inequality, by (7) and $0<\gamma k<1$ we obtain that

$$\sum_{\nu=0}^{n}\alpha_{n\nu}|\tau_\nu^\beta(x)|^k \leqq \left\{\sum_{\nu=0}^{n}\alpha_{n\nu}^p(\nu+1)^{(p/q)-\gamma kp}\right\}^{1/p}\times$$

$$(1.4)\qquad \times\left\{\sum_{\nu=0}^{n}(\nu+1)^{\gamma kq-1}|\tau_\nu^\beta(x)|^{qk}\right\}^{1/q}\leqq$$

$$\leqq K\left(\sum_{\nu=0}^{n}\alpha_{n\nu}\right)n^{-\gamma k}\left\{\sum_{\nu=0}^{n}(\nu+1)^{\gamma kq-1}|\tau_\nu^\beta(x)|^{qk}\right\}^{1/q}$$

By (1.3) we can choose α^* such that

$$(1.5)\qquad \beta-\frac{1}{2}+\frac{1}{qk}>\alpha^*>\frac{1}{2}.$$

By (1.5), $0<\gamma<1$ and $qk\geqq 2$ the conditions of Lemma 1 are fulfilled with $r=qk$, $l=2$, $\bar\gamma=\gamma$, $\alpha=\alpha^*$ and $\bar\beta=\beta$. Using Lemma 1 we get

$$(1.6)\qquad \left\{\sum_{\nu=0}^{\infty}(\nu+1)^{\gamma kq-1}|\tau_\nu^\beta(x)|^{qk}\right\}^{1/q}\leqq K_1\left\{\sum_{\nu=0}^{\infty}(\nu+1)^{2\gamma-1}|\tau_\nu^{\alpha^*}(x)|^2\right\}^{1/2}.$$

Thus by (1.4), (1.5), (1.6) and Lemma 2 we have

$$\int_a^b\left\{\sup_{1\leqq n<\infty}\left(\frac{n^{\gamma k}}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\tau_\nu^\beta(x)|^k\right)^{1/k}\right\}^2dx\leqq K_2\int_a^b\left\{\sum_{\nu=0}^{\infty}(\nu+1)^{2\gamma-1}|\tau_\nu^{\alpha^*}(x)|^2\right\}dx\leqq$$

$$\leqq K_3\sum_{n=1}^{\infty}c_n^2n^{2\gamma}<\infty,$$

which gives statement (1.2).

§ 2. Proof of the theorems and corollaries

Proof of Theorem I. First we show that (7) implies

$$(2.1)\qquad \sum_{\nu=0}^{n}\alpha_{n\nu}(\nu+1)^{-\delta}\leqq KA_nn^{-\delta}$$

for any $0<\delta<1$. Indeed,

$$\sum_{\nu=0}^{n}\alpha_{n\nu}(\nu+1)^{-\delta}\leqq\sum_{l=0}^{m}\sum_{\nu=2^l-1}^{\min(2^{l+1},n)}\alpha_{n\nu}(\nu+1)^{-\delta}\leqq$$

$$\leqq\sum_{l=0}^{m}\left\{\sum_{\nu=2^l-1}^{\min(2^{l+1},n)}\alpha_{n\nu}^p(\nu+1)^{-\delta p}\right\}^{1/p}\cdot 2^{l/q}\leqq KA_nn^{-\delta}.$$

By conditions (6) and (8) $\beta>1/2$, so we have (see e.g. inequality (3) with $k=1$)

$$\sigma_n^\beta(x)-f(x)=o_x(n^{-\gamma}).$$

Hence and from (2.1) it follows

$$\frac{1}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\sigma_\nu^\beta(x)-f(x)|^k = o_x(n^{-\gamma k}), \tag{2.2}$$

which implies

$$\frac{1}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\sigma_\nu^{\beta-1}(x)-f(x)|^k \leqq \frac{K}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\sigma_\nu^{\beta-1}(x)-\sigma_\nu^\beta(x)|^k+o_x(n^{-\gamma k}). \tag{2.3}$$

Now for any fixed positive ε we choose N such that

$$\sum_{n=N}^{\infty} c_n^2 n^{2\gamma} < \varepsilon^3. \tag{2.4}$$

Let us define two new series

$$\sum_{n=1}^{\infty} a_n\varphi_n(x) \quad \text{with} \quad a_n = \begin{cases} c_n & \text{for} \quad n \leqq N, \\ 0 & \text{for} \quad n > N, \end{cases} \tag{2.5}$$

and

$$\sum_{n=1}^{\infty} b_n\varphi_n(x) \quad \text{with} \quad b_n = \begin{cases} 0 & \text{for} \quad n \leqq N, \\ c_n & \text{for} \quad n > N. \end{cases} \tag{2.6}$$

Denote $\sigma_n^\beta(a; x)$ and $\sigma_n^\beta(b; x)$, respectively, the n-th Cesàro-means of order β of the series (2.5) and (2.6).

It is clear that

$$\sigma_n^\beta(x) = \sigma_n^\beta(a; x)+\sigma_n^\beta(b; x).$$

Applying Lemma 4 with the series (2.5) and γ' satisfying the conditions $\gamma<\gamma'<1$ and $k\gamma'<1$, we obtain that

$$\frac{n^{\gamma k}}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\sigma_\nu^{\beta-1}(a; x)-\sigma_\nu^\beta(a; x)|^k \to 0 \tag{2.7}$$

almost everywhere in (a, b).

On the other hand using Lemma 4 and (2.4) we obtain

$$\int_a^b \left\{\sup_{0\leqq n<\infty}\left(\frac{n^{k\gamma}}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\sigma_\nu^{\beta-1}(b; x)-\sigma_\nu^\beta(b; x)|^k\right)^{1/k}\right\}^2 dx \leqq K\varepsilon^3.$$

Hence

$$\operatorname{meas}\left\{x \,|\, \limsup\left(\frac{n^{k\gamma}}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\sigma_\nu^{\beta-1}(b; x)-\sigma_\nu^\beta(b; x)|^k\right)^{1/k} > \varepsilon\right\} \leqq K\varepsilon.$$

This and (2.7) imply

$$\frac{n^{\gamma k}}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|\sigma_\nu^{\beta-1}(x)-\sigma_\nu^\beta(x)|^k \to 0$$

almost everywhere in (a, b).

Collecting our results we obtain statement (9).

Proof of Corollary 1. It is easy to verify that if

$$\alpha_{n\nu} = \begin{cases} 0 & \text{for} \quad \nu \leqq n/2, \\ 1 & \text{for} \quad \nu > n/2, \end{cases}$$

then (7) holds for arbitrary $p>1$. Thus, if $\beta>1-\min(1/2, 1/k)$, (6) and (8) can be satisfied with a suitably chosen p, and the statement of Corollary 1 follows from (9) immediately.

Proof of Corollary 2. We define

$$C_n = \left(\sum_{i=\mu_{n-1}+1}^{\mu_n} c_i^2 \right)^{1/2}$$

and

$$\Phi_n(x) = \begin{cases} C_n^{-1} \sum\limits_{i=\mu_{n-1}+1}^{\mu_n} c_i \varphi_i(x) & \text{for} \quad C_n \neq 0, \\ (\mu_n - \mu_{n-1})^{-1/2} \sum\limits_{i=\mu_{n-1}+1}^{\mu_n} \varphi_i(x) & \text{for} \quad C_n = 0. \end{cases}$$

It is clear that the system $\{\Phi_n(x)\}$ is also an orthonormal one and

$$\sum_{n=1}^{\infty} C_n^2 n^{2\gamma} < \infty$$

obviously. Since

$$S_n(x) = \sum_{k=1}^{n} C_k \Phi_k(x) = s_{\mu_n}(x),$$

applying Theorem I to the series $\sum\limits_{n=1}^{\infty} C_n \Phi_n(x)$, we obtain the statement of Corollary 2.

Proof of Theorem II. Applying inequality (4) to the series $\sum\limits_{n=1}^{\infty} C_n \Phi_n(x)$ defined above, we get (11).

Proof of Theorem III. If $k=2$, then for any ν ($\leqq n$)

$$\frac{\alpha_{n\nu}}{A_n} \leqq \frac{K}{n}$$

whence, by (1.1), the estimate (13) follows obviously.

If $k<2$, then we can choose $p=2/k$. Using Hölder's inequality with this p and $q=2/(2-k)$ we obtain that

$$\sum_{\nu=0}^{n} \alpha_{n\nu} |s_{l_\nu}(x) - f(x)|^k \leqq \left\{ \sum_{\nu=0}^{n} \alpha_{n\nu}^q \right\}^{1/q} \left\{ \sum_{\nu=0}^{n} |s_{l_\nu}(x) - f(x)|^{kp} \right\}^{1/p}.$$

Hence, by (13) and (1.1),

$$\left\{\frac{1}{A_n}\sum_{\nu=0}^{n}\alpha_{n\nu}|s_{l_\nu}(x)-f(x)|^k\right\}^{1/k} \leqq K\left\{\frac{1}{n}\sum_{\nu=0}^{n}|s_{l_\nu}(x)-f(x)|^2\right\}^{1/2} = o_x(n^{-\gamma})$$

which is the required estimate.

References

[1] T. M. FLETT, Some more theorems concerning the absolute summability of Fourier series and power series, *Proc. London Math. Soc.*, **8** (1958), 357—387.

[2] L. LEINDLER, Über die Rieszschen Mittel allgemeiner Orthogonalreihen, *Acta Sci. Math.*, **24** (1963), 129—138.

[3] L. LEINDLER, On the strong approximation of orthogonal series, *Acta Sci. Math.*, **32** (1971), 41—50.

[4] G. SUNOUCHI, Strong approximation by Fourier series and orthogonal series, *Indian J. Math.*, **9** (1967), 237—246.

(Received April 20, 1974)

On locally regular Rees matrix semigroups

By LÁSZLÓ MÁRKI in Budapest

The aim of this paper is to investigate the behaviour of locally regular Rees matrix semigroups over a semigroup with zero and identity with respect to certain properties. This class of semigroups was defined by STEINFELD [3] in the following way.

Let H be a semigroup with zero 0 and identity e. Let $M^\circ = M^\circ(H; I, \Lambda; P)$ denote the Rees matrix semigroup over H with sandwich matrix $P = (p_{\lambda i})$ $(\lambda \in \Lambda; i \in I; p_{\lambda i} \in H)$. Denote the elements of M° by $(a)_{i\lambda}$ with a in H, i in I, and λ in Λ. The product of the matrices $(a)_{i\lambda}$, $(b)_{j\mu}$ is defined by

$$(a)_{i\lambda} \circ (b)_{j\mu} = (ap_{\lambda j}b)_{i\mu} \quad (a, b \in H;\ i, j \in I;\ \lambda, \mu \in \Lambda).$$

We say that $M^\circ(H; I, \Lambda; P)$ is *locally regular* if $P = (p_{\lambda i})$ has the following properties:

1) in every row λ of P there exists an element $p_{\lambda j(\lambda)}$ $(j(\lambda) \in I)$ which has a right inverse $p'_{\lambda j(\lambda)}$ in H, that is,

$$p_{\lambda j(\lambda)} p'_{\lambda j(\lambda)} = e;$$

2) in every column i of P there exists an element $p_{\mu(i) i}$ $(\mu(i) \in \Lambda)$ which has a eft inverse $p''_{\mu(i) i}$ in H, that is,

$$p''_{\mu(i) i} p_{\mu(i) i} = e;$$

3) there exists at least one element $p_{\lambda i}$ in P which has a right and left inverse in H.

One can see immediately that a Rees matrix semigroup over a group with zero is locally regular if and only if it is regular, hence, by the Rees representation theorem, if and only if it is completely 0-simple, which means that an abstract characterization of the class of locally regular Rees matrix semigroups yields a generalization of the Rees theorem. This characterization was given by STEINFELD [3] by means of the notion of similarity of one-sided ideals of a semigroup, introduced in the same paper of his.

The left ideals L_1 and L_2 of a semigroup S are said to be *left similar* if there exists a one-to-one mapping φ of L_1 onto L_2 such that $(sx)\varphi = s(x\varphi)$ for all $s \in S$ and $x \in L_1$. If, in addition, we have $x\varphi \in xS$ and $y\varphi^{-1} \in yS$ for all $x \in L_1$ and $y \in L_2$, then we say that L_1 and L_2 are *strongly left similar* (this notion proved to be useful in [1], where it was also shown that left similarity and strong left similarity of the left ideals L_1 and L_2 are equivalent in the case when L_1 and L_2 both can be generated by regular elements). Dually one defines right similarity and strong right similarity of right ideals of a semigroup S. Let S be a semigroup with 0 such that

$$S = \bigcup_{\lambda\in\Lambda} Se_\lambda = \bigcup_{i\in I} e_i S \quad (e_\lambda^2 = e_\lambda;\ e_i^2 = e_i;\ I\cap\Lambda \neq \emptyset)$$

where Se_λ $(\lambda\in\Lambda)$ $[e_i S\ (i\in I)]$ are (strongly) left [right] similar left [right] ideals of S with $Se_\mu\cap Se_\nu=0$ $(\mu,\nu\in\Lambda;\ \mu\neq\nu)$ and $e_j S\cap e_k S=0$ $(j,k\in I;\ j\neq k)$. We call a semigroup with these properties *similarly decomposable.*

Now Theorem 4.1 of STEINFELD [3] asserts that a semigroup issimilarly decomposable if and only if it is isomorphic to a locally regular Rees matrix semigroup over a semigroup with zero and identity.

As far as we know, regularity and simplicity properties of similarly decomposable semigroups have not been studied yet. We are going to show that a similarly decomposable semigroup can have, but need not have such properties. To be more precise, we shall see that several properties (regularity, 0-simplicity, 0-bisimplicity, complete 0-simplicity) of a locally regular Rees matrix semigroup $M^\circ = M^\circ(H; I, \Lambda; P)$ depend solely upon the underlying semigroup H, while other properties (like inversity, semi-simplicity, left- or right- or intra-regularity) depend also upon the sandwich matrix P of M°. However, of the latter properties we shall investigate inversity only, for the other ones we but mentioned that the fact that M° has any of them depends on H and P (and I and Λ) either.

In the sequel, H will always denote a semigroup with zero 0 and identity e and $M^\circ=M^\circ(H; I, \Lambda; P)$ a locally regular Rees matrix semigroup over H.

From the multiplication law $\circ$ of M° it follows immediately that for any $i\in I$ and $\lambda\in\Lambda$, the set $\{(a)_{i\lambda}\,|\,a\in H\}$ endowed with the multiplication $\circ$ forms a subsemigroup $M_{i\lambda}^\circ$ of M°. It is well-known from the theory of completely 0-simple semigroups, that if H is a group with zero, then each $M_{i\lambda}^\circ$ is either a zero-semigroup or is isomorphic to H. The following two lemmas (the first of which includes the above mentioned result) will show that this is far from being true in general.

Lemma 1. *$M_{i\lambda}^\circ$ is isomorphic to H if and only if the entry $p_{\lambda i}$ of the sandwich matrix P has a (two-sided) inverse (in H).*

Proof. Suppose that $\varphi\colon H\to M_{i\lambda}^\circ\colon a\to(\varphi'(a))_{i\lambda}$ is an isomorphism, then we have $\varphi(a)=\varphi(ea)=\varphi(e)\circ\varphi(a)$; putting $a=\varphi^{-1}((e)_{i\lambda})$, herefrom we obtain that $\varphi'(e)p_{\lambda i}=e$. Similarly, $\varphi(a)=\varphi(a)\circ\varphi(e)$ implies $p_{\lambda i}\varphi'(e)=e$, thus $\varphi'(e)$ is an inverse of $p_{\lambda i}$.

Suppose now that $p_{\lambda i}$ has an inverse $p'_{\lambda i}$. We shall show that

$$\varphi\colon H\to M_{i\lambda}^\circ\colon a\to(ap'_{\lambda i})_{i\lambda}$$

is an isomorphism.

In fact,

1) φ is a homomorphism since for any $a, b \in H$ we have

$$\varphi(ab) = (abp'_{\lambda i})_{i\lambda} = (ap'_{\lambda i}p_{\lambda i}bp'_{\lambda i})_{i\lambda} = (ap'_{\lambda i})_{i\lambda} \circ (bp'_{\lambda i})_{i\lambda} = \varphi(a) \circ \varphi(b),$$

2) φ is one-to-one as $ap'_{\lambda i} = bp'_{\lambda i}$ implies $a = ap'_{\lambda i}p_{\lambda i} = bp'_{\lambda i}p_{\lambda i} = b$,

3) φ is onto since for any $a \in H$ we have $(a)_{i\lambda} = (ap_{\lambda i}p'_{\lambda i})_{i\lambda} = \varphi(ap_{\lambda i})$, q.e.d.

Corollary. *If the entry $p_{\lambda i}$ of the sandwich matrix P has a one-sided inverse which is not a two-sided inverse then $M^\circ_{i\lambda}$ is neither isomorphic to H nor is it a zero semigroup.*

Note that for 1) and 2) we used only that $p'_{\lambda i}$ is a left inverse of $p_{\lambda i}$, thus φ is a monomorphism in this case already. Similarly, if $p'_{\lambda i}$ is a right inverse of $p_{\lambda i}$, then

$$\tilde{\varphi} : a \to (p'_{\lambda i}a)_{i\lambda}$$

is a monomorphism of H into $M^\circ_{i\lambda}$. This remark constitutes our

Lemma 2. *If $p_{\lambda i}$ has a one-sided inverse, $M^\circ_{i\lambda}$ contains a subsemigroup which is isomorphic to H.*

Theorem 1. *$M^\circ = M^\circ(H; I, \Lambda; P)$ is 0-simple if and only if H is 0-simple.*

Proof. Suppose that M° is 0-simple and let a and b be arbitrary non-zero elements of H, we have to show the existence of elements $x, y \in H$ with $xay = b$. Now choose arbitrarily $i, j \in I$ and $\lambda, \mu \in \Lambda$, then, by the 0-simplicity of M°, there exist indices $k \in I$, $\nu \in \Lambda$ and elements $x', y' \in H$ such that

$$(x')_{j\nu} \circ (a)_{i\lambda} \circ (y')_{k\mu} = (b)_{j\mu},$$

that is,

$$x'p_{\nu i}ap_{\lambda k}y' = b.$$

Thus we have $xay = b$ with $x = x'p_{\nu i}$ and $y = p_{\lambda k}y'$.

Suppose now that H is 0-simple and let $(a)_{i\lambda}$ and $(b)_{j\mu}$ be arbitrary non-zero elements of M°. Since H is 0-simple, there exist elements $x', y' \in H$ with $x'ay' = b$. Now let $\nu(i) \in \Lambda$ and $k(\lambda) \in I$ be indices for which $p_{\nu(i)i}$ has a left inverse $p''_{\nu(i)i}$ and $p_{\lambda k(\lambda)}$ has a right inverse $p'_{\lambda k(\lambda)}$, and put $x = x'p''_{\nu(i)i}$, $y = p'_{\lambda k(\lambda)}y'$. Then we have

$$(x)_{j\nu(i)} \circ (a)_{i\lambda} \circ (y)_{k(\lambda)\mu} = (xp_{\nu(i)i}ap_{\lambda k(\lambda)}y)_{j\mu} = (x'ay')_{j\mu} = (b)_{j\mu},$$

q.e.d.

Theorem 2. *$M^\circ = M^\circ(H; I, \Lambda; P)$ is completely 0-simple if and only if H is completely 0-simple.*

Proof. If H is completely 0-simple, it is a group with zero (since by Rees [2], a completely 0-simple semigroup with identity is a group with zero). Then local regularity of M° is equivalent to regularity by one of our first remarks, thus M° is completely 0-simple by the Rees representation theorem (s. [2]).

Suppose now that M° is completely 0-simple, then H is 0-simple by Theorem 1. On the other hand, by the Corollary of Lemma 1, H is isomorphic to a subsemigroup of M°, thus all idempotents of H are primitive. Hence H is completely 0-simple.

Theorem 3. *$M^\circ = M^\circ(H; I, \Lambda; P)$ is 0-bisimple if and only if H is 0-bisimple.*

Proof. We shall see that the $\mathcal{R}$-classes of M° are of the form

$$\{(a)_{i\lambda} | a \in R, \lambda \in \Lambda\}$$

where i is an element of I and R is an $\mathcal{R}$-class of H. Since the same proof gives a similar form for the $\mathcal{L}$-classes of M°, this implies that the $\mathcal{D}$-classes of M° are exactly the sets of the form

$$\{(a)_{i\lambda} | a \in D, i \in I, \lambda \in \Lambda\}$$

where D is a $\mathcal{D}$-class of H, which proves our assertion.

Let $a, b \in H$ with $a\mathcal{R}b$, $i \in I$ and $\lambda, \mu \in \Lambda$, we are going to show that $(a)_{i\lambda}\mathcal{R}(b)_{i\mu}$ in M°. From $a\mathcal{R}b$ it follows that there exist elements $x', y' \in H$ with $a = bx'$ and $b = ay'$. Now let $j(\lambda) \in I$ and $k(\mu) \in I$ be indices for which $p_{\lambda j(\lambda)}$ and $p_{\lambda k(\mu)}$ have right inverses $p'_{\lambda j(\lambda)}$ and $p'_{\mu k(\mu)}$, respectively, and put $x = p'_{\mu k(\mu)} x'$, $y = p'_{\lambda j(\lambda)} y'$, then we have

$$(b)_{i\mu} \circ (x)_{k(\mu)\lambda} = (bp_{\mu k(\mu)} x)_{i\lambda} = (bx')_{i\lambda} = (a)_{i\lambda}$$

and similarly $(a)_{i\lambda} \circ (y)_{j(\lambda)\mu} = (b)_{i\mu}$. Thus $(a)_{i\lambda}\mathcal{R}(b)_{i\mu}$.

We still have to show that $(a)_{i\lambda}\mathcal{R}(b)_{j\mu}$ in M° implies $i=j$ and $a\mathcal{R}b$ in H. In fact, if $(a)_{i\lambda}\mathcal{R}(b)_{j\mu}$, then there exist elements $(x)_{k\nu}$ and $(y)_{l\pi}$ with

$$(a)_{i\lambda} \circ (x)_{k\nu} = (b)_{j\mu} \quad \text{and} \quad (b)_{j\mu} \circ (y)_{l\pi} = (a)_{i\lambda},$$

that is,

$$(ap_{\lambda k} x)_{i\nu} = (b)_{j\mu} \quad \text{and} \quad (bp_{\mu l} y)_{j\pi} = (a)_{i\lambda}$$

which imply, among others, $i=j$, $a(p_{\lambda k} x) = b$ and $b(p_{\mu l} y) = a$. The last two equations give $a\mathcal{R}b$ in H, which completes the proof of our theorem.

Theorem 4. *$M^\circ = M^\circ(H; I, \Lambda; P)$ is regular if and only if H is regular.*

Proof. Let H be regular, $(a)_{i\lambda}$ be an arbitrary element of M° and $j(\lambda) \in I$, $\mu(i) \in \Lambda$ be indices for which $p_{\lambda j(\lambda)}$ has a right inverse $p'_{\lambda j(\lambda)}$ and $p_{\mu(i)i}$ has a left inverse $p''_{\mu(i)i}$. By the regularity of H we have $a = aya$ with some $y \in H$, thus we also have

$$(a)_{i\lambda} = (ap_{\lambda j(\lambda)} p'_{\lambda j(\lambda)} y p''_{\mu(i)i} p_{\mu(i)i} a)_{i\lambda} = (a)_{i\lambda} \circ (p'_{\lambda j(\lambda)} y p''_{\mu(i)i})_{j(\lambda)\mu(i)} \circ (a)_{i\lambda}$$

which proves the regularity of M°.

On the other hand, suppose that M° is regular, let a be an arbitrary element of H and choose any indices $i \in I$ and $\lambda \in \Lambda$. Then we have

$$(a)_{i\lambda} \circ (x)_{j\mu} \circ (a)_{i\lambda} = (a)_{i\lambda}$$

for some $x \in H$, $j \in I$ and $\mu \in \Lambda$, hence

$$a = a(p_{\lambda j} x p_{\mu i}) a.$$

Thus H is also regular.

Remark. Combining the first part of this proof with the fact that if $a = axa$ then xax is a generalized inverse of a, we obtain that each element of $M^\circ_{i\lambda}$ in a regular M° has a generalized inverse in $M^\circ_{j(\lambda)\mu(i)}$.

The only if parts of Theorems 1 and 4, in the proofs of which not even local regularity of M° was made use of, were already given in the most general case by VENKATESAN [4]. Corollary 1 to Proposition 1 and Corollary 1 to Theorem 1 of VENKATESAN [4], together with our Theorem 4, give the following result for locally regular Rees matrix semigroups:

Theorem 5. *$M^\circ = M^\circ(H; I, \Lambda; P)$ is a union of its completely 0-simple ideals if and only if the same is true for H.*

In connection with the Corollary to Lemma 2, we should like to mention that the behaviour of the subsemigroups $M^\circ_{i\lambda}$ of M° is, in general, far from being so nice as that of H with respect to the above treated properties. As an illustration, let us see the following example:

Let H be the bicyclic semigroup $\mathscr{C}(q, r)$ with zero adjoined, $I = \Lambda = \{0, 1, 2, \dots\}$ and the sandwich matrix P be

$$P = \begin{pmatrix} \underset{\smile}{0} & \underset{\smile}{1} & \underset{\smile}{2} & \underset{\smile}{3} \dots \underset{\smile}{m} & \dots \\ e & 0 & 0 & 0 \dots 0 & \dots \\ 0 & r & q & r^3 \dots r^m & \dots \\ 0 & q^2 & r^2 & 0 \dots 0 & \dots \\ 0 & q^3 & 0 & 0 \dots 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & q^n & 0 & 0 \quad 0 & \\ \vdots & \vdots & \vdots & \vdots & \end{pmatrix},$$

and consider the Rees matrix semigroup $M^\circ(H; I, \Lambda; P)$. Since for all $n \geqq 0$, r^n has a left inverse and q^n has a right inverse, M° is a locally regular Rees matrix semigroup. It is well-known that this H is 0-bisimple, thus the same is true for M°. If $n \geqq 3$, by Lemma 2, M°_{n1} contains a subsemigroup which is isomorphic to H, however, M°_{n1} is not even regular. In fact, let $k < n$ and consider the element $(r^k q^l)_{n1}$ with some $l \geqq 0$, then for any element $(r^s q^t)_{n1}$ of M°_{n1} we have

$$(r^k q^l)_{n1} \circ (r^s q^t)_{n1} \circ (r^k q^l)_{n1} = (r^k q^l q^n r^s q^t q^n r^k q^l)_{n1} = (r^k q^{l+n} r^s q^{t+n-k+l})_{n1} \neq (r^k q^l)_{n1}$$

since multiplication by $r^k q^{l+n} r^s$ from the left cannot reduce the exponent $t+n-$ $-k+l>l$ of q.

At last we give a necessary and sufficient condition that $M^\circ(H; I, \Lambda; P)$ be an inverse semigroup.

Theorem 6. *The locally regular Rees matrix semigroup $M^\circ = M^\circ(H; I, \Lambda; P)$ is an inverse semigroup if and only if the following conditions are satisfied: H is an inverse semigroup, in each row and each column of the sandwich matrix P there exists exactly one element which has a two-sided inverse (clearly, this implies $|I|=|\Lambda|$), and all the other entries of P are zero.*

Proof. Suppose first that $M^\circ(H; I, \Lambda; P)$ satisfies all these conditions, and, for any $\lambda\in\Lambda$ and $i\in I$, let $j(\lambda)\in I$ and $\mu(i)\in\Lambda$ denote the indices for which $p_{\lambda j(\lambda)}$ and $p_{\mu(i)i}$ have two-sided inverses.

Let $(a)_{i\lambda}$ and $(b)_{j\mu}$ be generalized inverses of each other, $a\neq 0$, then we have

$$a = ap_{\lambda j}bp_{\mu i}a \neq 0,$$

whence $j=j(\lambda)$ and $\mu=\mu(i)$. Suppose further that $(c)_{j(\lambda)\mu(i)}$ is also a generalized inverse of $(a)_{i\lambda}$. Then we have

$$(*) \qquad a = ap_{\lambda j(\lambda)}bp_{\mu(i)i}a = ap_{\lambda j(\lambda)}cp_{\mu(i)i}a,$$

$$(**) \qquad b = bp_{\mu(i)i}ap_{\lambda j(\lambda)}b, \quad c = cp_{\mu(i)i}ap_{\lambda j(\lambda)}c.$$

Multiplying the equations $(*)$ and $(**)$ from the right by $p_{\lambda j(\lambda)}$ and $p_{\mu(i)i}$, respectively, we obtain that $bp_{\mu(i)i}$ and $cp_{\mu(i)i}$ are both generalized inverses of $ap_{\lambda j(\lambda)}$ in H. In view of the inversity of H, this implies

$$bp_{\mu(i)i} = cp_{\mu(i)i},$$

and multiplication from the right by the inverse of $p_{\mu(i)i}$ gives now $b=c$. Hence each element of M° may have at most one generalized inverse, but it does have one, since by Theorem 4 the regularity of H implies that M° is also a regular semigroup. Thus M° is an inverse semigroup.

Conversely, suppose that M° is an inverse semigroup. By Theorem 4, H is regular, and as H is isomorphic to a subsemigroup of M° by the Corollary of Lemma 1, no element of H can have more than one generalized inverse element. Thus H is an inverse semigroup.

Let $(a)_{i\lambda}$ be an arbitrary non-zero element of M°, and suppose that $(b)_{j\mu}$ is the generalized inverse of $(a)_{i\lambda}$.

We have seen in the Remark after Theorem 4 that each $(a)_{i\lambda}$ has a generalized inverse in $M^\circ_{j(\lambda)\mu(i)}$, hence we must have, by the unicity of the generalized inverse element, $j=j(\lambda)$ and $\mu=\mu(i)$. On the other hand, $(b)_{j\mu}=(b)_{j(\lambda)\mu(i)}$ has $(a)_{i\mu}$ as its generalized inverse, but it also has a generalized inverse in $M^\circ_{j(\mu(i))\mu(j(\lambda))}$, whence

$ij = (\mu(i))$ and $\lambda = \mu(j(\lambda))$. Herefrom we can conclude that the elements $p_{\lambda j(\lambda)}$ and $p_{i\mu(i)}$ have (two-sided) inverses in H. Suppose now that the element $p_{\lambda m}$ has a right inverse $p'_{\lambda m}$ in H for some $m \in I$. Then we have

$$(a)_{i\lambda} = (a)_{i\lambda} \circ (b)_{j\mu} \circ (a)_{i\lambda} = (ap_{\lambda m} p'_{\lambda m} p_{\lambda j} bp_{\mu i} a)_{i\lambda} = (a)_{i\lambda} \circ (p'_{\lambda m} p_{\lambda j} b)_{m\mu} \circ (a)_{i\lambda}$$

and

$$b = bp_{\mu i} ap_{\lambda j} b = bp_{\mu i} ap_{\lambda m} p'_{\lambda m} p_{\lambda j} b,$$

multiplying here by $p'_{\lambda m} p_{\lambda j}$ from the left we obtain that

$$(p'_{\lambda m} p_{\lambda j} b)_{m\mu} = (p'_{\lambda m} p_{\lambda j} b)_{m\mu} \circ (a)_{i\lambda} \circ (p'_{\lambda m} p_{\lambda j} b)_{m\mu},$$

that is, $(p'_{\lambda m} p_{\lambda j} b)_{m\mu}$ is also a generalized inverse of $(a)_{i\lambda}$. Since $(a)_{i\lambda}$ may have but one generalized inverse, this implies $m = j = j(\lambda)$. In other words, in each row of P there exists exactly one element which has a right inverse in H, and we have seen that this element must have a two-sided inverse. Dually we obtain the analogous result for columns.

We still have to show that all the other entries of P are zero. Suppose that, on the contrary, there exists an entry $p_{\lambda i} \neq 0$ in P, which does not have an inverse of either sides in H. As H is an inverse semigroup, $p_{\lambda i}$ has a generalized inverse a in H:

$$ap_{\lambda i} a = a \quad \text{and} \quad p_{\lambda i} ap_{\lambda i} = p_{\lambda i}.$$

Then we also have

$$a = ap_{\lambda i} a = ap_{\lambda i} ap_{\lambda i} a$$

and

$$(a)_{i\lambda} = (ap_{\lambda i} ap_{\lambda i} a)_{i\lambda} = (a)_{i\lambda} \circ (a)_{i\lambda} \circ (a)_{i\lambda},$$

thus $(a)_{i\lambda}$ is a generalized inverse of itself, which contradicts the fact that M° is an inverse semigroup, since we have seen that in such a semigroup each element $(a)_{i\lambda}$ has its generalized inverse in $M^\circ_{j(\lambda)\mu(i)}$, and now $i \neq j(\lambda)$ for $p_{\lambda i}$ does not have a right inverse. This completes the proof of Theorem 6.

Remark. For the notions occurring in the following Corollary we refer to [3]. As it is easy to show that a 0-cancellative regular semigroup with identity is a group with zero adjoined, our Theorem 6 and Theorem 5.1 in [3] imply the following result:

Corollary. *For a special similarly decomposable semigroup S the following conditions are equivalent:*

(i) *S is regular,*
(ii) *S is an inverse semigroup,*
(iii) *S is completely 0-simple,*
(iv) *S is a Brandt semigroup.*

Thanks are due to Prof. O. Steinfeld for his attention during the preparation of the present work.

References

[1] L. MÁRKI—O. STEINFELD, A generalization of Green's relations in semigroups, *Semigroup Forum*, 7 (1974), 74—85.
[2] D. REES, On semi-groups, *Proc. Cambridge Phil. Soc.*, 36 (1940), 387—400.
[3] O. STEINFELD, On a generalization of completely 0-simple semigroups, *Acta Sci. Math.*, **28** (1967), 135—145.
[4] P. S. VENKATESAN, Matrix semigroups over a semigroup with zero, *Math. Ann.*, **181** (1969), 60—64.

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
REÁLTANODA U. 13—15
H—1053 BUDAPEST

(Received January 16, 1974)

On a paper of Blum, Eisenberg, and Hahn concerning ergodic theory and the distribution of sequences in the Bohr group

By H. NIEDERREITER in Princeton (New Jersey, USA)

Let $\mathbf{Z}$ be the additive group of integers in the discrete topology, and let $\overline{\mathbf{Z}}$ be its Bohr compactification. In a recent paper, BLUM, EISENBERG, and HAHN [1] have pointed out a remarkable connection between the validity of the mean ergodic theorem for sums of the type $\frac{1}{N}\sum_{n=1}^{N} T^{a_n}f$, where (a_n), $n=1, 2, \dots$, is a given sequence of integers, and the distribution of the sequence (a_n) in $\overline{\mathbf{Z}}$. In fact, it is noted in that paper that the mean ergodic theorem holds for the above sums if and only if the sequence (a_n) is uniformly distributed in $\overline{\mathbf{Z}}$ in the sense of Definition 1 below. Therefore, it becomes an interesting problem to exhibit classes of sequences (a_n) that satisfy the required type of uniform distribution property. BLUM, EISENBERG, and HAHN have already made a contribution to this problem by providing a sufficient condition that can be checked fairly easily (see condition (i) in [1, p. 23] or condition (1) below). The authors state that they do not know of any sequence in $\mathbf{Z}$ that is uniformly distributed in $\overline{\mathbf{Z}}$ but does not satisfy the condition (1). It is the main purpose of this note to show that the condition (1) of BLUM, EISENBERG, and HAHN is certainly not necessary for uniform distribution in $\overline{\mathbf{Z}}$, and that one may in fact construct sequences in $\mathbf{Z}$ that are uniformly distributed in $\overline{\mathbf{Z}}$ but for which (1) fails drastically. At the same time, we exhibit large classes of sequences (a_n) in $\mathbf{Z}$ that are uniformly distributed in $\overline{\mathbf{Z}}$ and that can therefore be used to obtain generalized mean ergodic theorems.

We recall some well-known notions of uniform distribution in topological groups. For a detailed discussion of this topic, see KUIPERS and NIEDERREITER [2, Ch. 4]. Since all the groups we shall consider in the sequel will be abelian, we restrict our attention to this case.

This research was carried out while the author was supported by NSF grant GP 36418X1.

Definition 1. The sequence (x_n), $n=1, 2, \dots$, in the locally compact abelian group G is called Hartman-uniformly distributed in G if

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi(x_n) = 0$$

holds for all nontrivial characters χ of G.

Definition 2. The sequence (x_n), $n=1, 2, \dots$, in the locally compact abelian group G is called uniformly distributed in G if for any subgroup H of G of compact index (i.e., for any closed subgroup H of G for which G/H is compact), the sequence (x_n+H), $n=1, 2, \dots$, is Hartman-uniformly distributed in G/H.

A Hartman-uniformly distributed sequence in G is also uniformly distributed in G, but the converse is not true in general. For compact groups the two kinds of uniform distribution are the same. Moreover, the sequence (x_n) is Hartman-uniformly distributed in G if and only if (x_n) is uniformly distributed in the Bohr compactification $\bar{G}$ of G. For these results and for an exposition of the theory of uniform distribution in locally compact groups, see KUIPERS and NIEDERREITER [2, Ch. 4, Sect. 5].

For the special cases $G=\mathbf{Z}$ and $G=\mathbf{R}$, the additive group of real numbers in the usual topology, one arrives at the following equivalent characterizations by using the WEYL criterion for uniform distribution mod 1 (for details, see [2, Ch. 4, Sect. 5]).

Lemma 1. *The sequence* (x_n), $n=1, 2, \dots$, *in* $\mathbf{R}$ *is uniformly distributed in* $\mathbf{R}$ *if and only if the sequence* $(x_n\alpha)$, $n=1, 2, \dots$, *is uniformly distributed* mod 1 *for all nonzero real numbers* α.

Lemma 2. *The sequence* (a_n), $n=1, 2, \dots$, *in* $\mathbf{Z}$ *is Hartman-uniformly distributed in* $\mathbf{Z}$ *if and only if* (a_n) *is uniformly distributed in* $\mathbf{Z}$ *and* $(a_n\alpha)$, $n=1, 2, \dots$, *is uniformly distributed* mod 1 *for all irrational numbers* α.

We remark that the notion of uniform distribution in $\mathbf{Z}$ according to Definition 2 is identical with the notion introduced by NIVEN [3].

In the language of the present paper, the basic result mentioned in [1] concerning the mean ergodic theorem reads as follows: The mean ergodic theorem holds for sums of the type $\frac{1}{N}\sum_{n=1}^{N} T^{a_n}f$ if and only if the sequence (a_n), $n=1, 2, \dots$, is Hartman-uniformly distributed in $\mathbf{Z}$. The sufficient condition for Hartman-uniform distribution in $\mathbf{Z}$ given by BLUM, EISENBERG, and HAHN is as follows. Let (a_n), $n=1, 2, \dots$, be a sequence in $\mathbf{Z}$, let E_N be the set consisting of the first N terms of (a_n), and let E_N+k be the set E_N shifted by the integer k. Then, if

$$(1) \qquad \lim_{N\to\infty} \frac{1}{N} \operatorname{card}\left(E_N \cap (E_N+k)\right) = 1 \quad \text{for all} \quad k \in \mathbf{Z},$$

the sequence (a_n) is Hartman-uniformly distributed in $\mathbf{Z}$ (see [1, Theorem 1]). Obviously, it suffices to consider only positive integers k in (1).

The following theorem provides many examples of Hartman-uniformly distributed sequences in $\mathbf{Z}$, most of which do not satisfy condition (1).

Theorem 1. *If (x_n), $n=1, 2, \dots$, is uniformly distributed in $\mathbf{R}$, then the sequence $([x_n])$, $n=1, 2, \dots$, of integral parts is Hartman-uniformly distributed in $\mathbf{Z}$.*

Proof. We proceed by Lemma 2. In order to prove that $([x_n])$ is uniformly distributed in $\mathbf{Z}$, we note that by Lemma 1 the sequence (x_n/m), $n=1, 2, \dots$, is uniformly distributed mod 1 for any integer $m \geqq 2$. Therefore, $([x_n])$ is uniformly distributed in $\mathbf{Z}$ by a well-known theorem (see Niven [4] and Kuipers and Niederreiter [2, Ch. 5, Theorem 1.4]).

Now let α be an irrational number. For any $(h_1, h_2) \in \mathbf{Z}^2$ with $(h_1, h_2) \neq (0, 0)$, the number $h_1\alpha + h_2$ is nonzero; therefore, the sequence $\big((h_1\alpha+h_2)x_n\big)$, $n=1, 2, \dots$, is uniformly distributed mod 1 by Lemma 1. Hence, by [2, Ch. 1, Theorem 6.3], the sequence $\big((x_n\alpha, x_n)\big)$, $n=1, 2, \dots$, in $\mathbf{R}^2$ is uniformly distributed mod 1 in $\mathbf{R}^2$. Now, for any sequence $\big((y_n, z_n)\big)$, $n=1, 2, \dots$, in $\mathbf{R}^2$ which is uniformly distributed mod 1 in $\mathbf{R}^2$, we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{y_n\}, \{z_n\}) = \int_0^1 \int_0^1 f(y, z)\, dy\, dz \tag{2}$$

for any complex-valued continuous function f on $[0, 1]^2$ (see [2, Ch. 1, Theorem 6.1]), where $\{t\}$ denotes the fractional part of $t \in \mathbf{R}$.

For typographic convenience, we write $\exp(t) = e^{2\pi i t}$ for $t \in \mathbf{R}$. We choose a nonzero integer h. Then

$$\exp(h[x_n]\alpha) = \exp(hx_n\alpha - h\alpha\{x_n\}) = \exp(h\{x_n\alpha\} - h\alpha\{x_n\})$$

for all $n \geqq 1$. Hence, if we apply (2) to the sequence $\big((x_n\alpha, x_n)\big)$ and to the function $f(y, z) = \exp(hy - h\alpha z)$, we obtain

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp(h[x_n]\alpha) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp(h\{x_n\alpha\} - h\alpha\{x_n\})$$
$$= \int_0^1 \int_0^1 \exp(hy - h\alpha z)\, dy\, dz = 0.$$

This means that the sequence $([x_n]\alpha)$ $(n=1, 2, \dots)$ is uniformly distributed mod 1. Since α was an arbitrary irrational number, the proof of the theorem is complete by Lemma 2.

Theorem 1 contains a variety of interesting special cases. We list a few of them.

Corollary 1. *Let $P(x)=\alpha_s x^s+\cdots+\alpha_0$ be a polynomial over* **R** *of degree at least 2. If the system $\{\alpha_s, \alpha_{s-1}, \ldots, \alpha_1\}$ has rank at least 2 over the rationals, then the sequence $([P(n)])$ $(n=1, 2, \ldots)$ is Hartman-uniformly distributed in* **Z**.

Proof. This follows from [2, Ch. 4, Example 5.4] and Theorem 1.

We remark that VEECH [5] has even shown a somewhat stronger property of the sequence $([P(n)])$. Obviously, the sequence $(a_n)=([P(n)])$ is eventually increasing or eventually decreasing with $\lim_{n\to\infty} |a_{n+1}-a_n|=\infty$, and therefore

$$\lim_{N\to\infty} \frac{1}{N} \operatorname{card}\big(E_N \cap (E_N+k)\big) = 0 \quad \text{for all} \quad k \geqq 1,$$

so that (1) fails drastically.

For positive integers r, we define the action of the difference operator Δ^r on sequences (x_n) in **R** recursively: we set $\Delta^1 x_n = x_{n+1}-x_n$ for $n\geqq 1$ and $\Delta^r x_n = \Delta^{r-1}(\Delta^1 x_n)$ for $r\geqq 2$ and $n\geqq 1$.

Corollary 2. *Let (x_n) be a sequence in* **R** *such that for some positive integer r the following properties are satisfied: $\Delta^r x_n$ tends monotonically to 0 as $n\to\infty$ and $\lim_{n\to\infty} n|\Delta^r x_n|=\infty$. Then the sequence $([x_n])$ is Hartman-uniformly distributed in* **Z**.

Proof. We note that for any nonzero $\alpha\in\mathbf{R}$ the sequence $(x_n\alpha)$ satisfies the same properties as (x_n). Therefore, by [2, Ch.1, Theorem 3.4], the sequence $(x_n\alpha)$ is uniformly distributed mod 1. The desired result follows from Lemma 1 and Theorem 1.

The following condition is usually easier to check.

Corollary 3. *Suppose the function $f(t)$ is defined for $t\geqq 1$ and r times differentiable for sufficiently large t and for some positive integer r. Furthermore, assume that $f^{(r)}(t)$ tends monotonically to 0 as $t\to\infty$ and that $\lim_{t\to\infty} t|f^{(r)}(t)|=\infty$. Then the sequence $([f(n)])$, $n=1, 2, \ldots,$ is Hartman-uniformly distributed in* **Z**.

Proof. One uses [2, Ch. 1, Theorem 3.5] and proceeds as in the proof of Corollary 2.

If we choose $\sigma>1$, $\sigma\notin\mathbf{Z}$, then the sequence $(a_n)=([n^\sigma])$, $n=1, 2, \ldots$, is Hartman-uniformly distributed in **Z** by Corollary 3. On the other hand, the sequence (a_n) is increasing with $\lim_{n\to\infty}(a_{n+1}-a_n)=\infty$, so that we have again

$$\lim_{N\to\infty} \frac{1}{N} \operatorname{card}\big(E_N \cap (E_N+k)\big) = 0 \quad \text{for all} \quad k \geqq 1.$$

In the following theorem, we go beyond the examples constructed above and show that for a Hartman-uniformly distributed sequence in $\mathbf{Z}$ the limits in (1) may have any prescribed value.

Theorem 2. *For a given positive integer k and a real number α with $0 \leqq \alpha \leqq 1$, there exists a Hartman-uniformly distributed sequence in* $\mathbf{Z}$ *with*

$$\lim_{N\to\infty} \frac{1}{N} \operatorname{card}\left(E_N \cap (E_N + k)\right) = \alpha. \tag{3}$$

Proof. We have already constructed examples for $\alpha=0$. If $\alpha=1$, we may take the sequence of positive integers as an example. Now suppose $0<\alpha<1$, and let $m \geqq 1$ be an integer with $\alpha \leqq \frac{m}{m+1}$. By choosing a sequence $(a_n)=([n^\sigma])$ $(n=1, 2, \dots)$ with a sufficiently large $\sigma \notin \mathbf{Z}$, we get a Hartman-uniformly distributed sequence in $\mathbf{Z}$ with $a_{n+1}-a_n>k(m+1)$ for all $n \geqq 1$. We set $\beta=\frac{m}{\alpha}-m$, so that $\beta \geqq 1$. Furthermore, we put $s(j)=[\beta j]$ for $j=0, 1, \dots$. Consider the following sequence:

$$a_1, a_2, \dots, a_{s(1)}, a_1+k, a_1+2k, \dots, a_1+mk, a_{s(1)+1}, a_{s(1)+2}, \dots,$$
$$a_{s(2)}, a_2+k, a_2+2k, \dots, a_2+mk, \dots, a_{s(j-1)+1}, a_{s(j-1)+2}, \dots,$$
$$a_{s(j)}, a_j+k, a_j+2k, \dots, a_j+mk, \dots.$$

Let us denote this sequence by (b_n). We show first that (b_n) is Hartman-uniformly distributed in $\mathbf{Z}$. Let χ be a nontrivial character of $\mathbf{Z}$. For $N>s(1)+m$, there exists a unique $j \geqq 1$ such that $s(j)+jm<N \leqq s(j+1)+(j+1)m$. Then

$$\left|\sum_{n=1}^{N} \chi(b_n)\right| \leqq \left|\sum_{n=1}^{s(j)+jm} \chi(b_n)\right| + s(j+1)-s(j)+m,$$

so that

$$\left|\frac{1}{N} \sum_{n=1}^{N} \chi(b_n)\right| \leqq \left|\frac{1}{s(j)+jm} \sum_{n=1}^{s(j)+jm} \chi(b_n)\right| + \frac{s(j+1)-s(j)+m}{s(j)+jm}.$$

Therefore, it suffices to show that

$$\lim_{j\to\infty} \frac{1}{s(j)+jm} \sum_{n=1}^{s(j)+jm} \chi(b_n) = 0. \tag{4}$$

For $j \geqq 1$ we have

$$\sum_{n=1}^{s(j)+jm} \chi(b_n) = \sum_{n=1}^{s(j)} \chi(a_n) + \sum_{p=1}^{m} \sum_{q=1}^{j} \chi(a_q+pk),$$

and therefore

$$\left|\frac{1}{s(j)+jm} \sum_{n=1}^{s(j)+jm} \chi(b_n)\right| \leqq \left|\frac{1}{s(j)} \sum_{n=1}^{s(j)} \chi(a_n)\right| + \left|\frac{1}{j} \sum_{q=1}^{j} \chi(a_q)\right|. \tag{5}$$

But since (a_n) is Hartman-uniformly distributed in $\mathbf{Z}$, the right-hand side of (5) tends to 0 as $j\to\infty$, and so (4) is established.

It remains to prove that (b_n) satisfies (3). For $N>s(1)+m$, there is a unique $j\geqq 1$ with $s(j)+jm<N\leqq s(j+1)+(j+1)m$. Then

$$\frac{s(j)+jm}{s(j+1)+(j+1)m}\cdot\frac{\operatorname{card}\left(E_{s(j)+jm}\cap(E_{s(j)+jm}+k)\right)}{s(j)+jm}\leqq\frac{\operatorname{card}\left(E_N\cap(E_N+k)\right)}{N}\leqq$$

$$\leqq\frac{\operatorname{card}\left(E_{s(j+1)+(j+1)m}\cap(E_{s(j+1)+(j+1)m}+k)\right)}{s(j+1)+(j+1)m}\cdot\frac{s(j+1)+(j+1)m}{s(j)+jm},$$

nd since

$$\lim_{j\to\infty}\frac{s(j+1)+(j+1)m}{s(j)+jm}=1,$$

it suffices to show that

$$\lim_{j\to\infty}\frac{\operatorname{card}\left(E_{s(j)+jm}\cap(E_{s(j)+jm}+k)\right)}{s(j)+jm}=\alpha. \tag{6}$$

Using $a_{n+1}-a_n>k(m+1)$ for all $n\geqq 1$, it follows easily that for every $j\geqq 1$ we have

$$E_{s(j)+jm}\cap(E_{s(j)+jm}+k)=\bigcup_{q=1}^{j}\{a_q+k,\,a_q+2k,\,\dots,\,a_q+mk\}.$$

We conclude that

$$\lim_{j\to\infty}\frac{\operatorname{card}\left(E_{s(j)+jm}\cap(E_{s(j)+jm}+k)\right)}{s(j)+jm}=\lim_{j\to\infty}\frac{jm}{s(j)+jm}=\frac{m}{\beta+m}=\alpha,$$

and so (6) is shown. This completes the proof of Theorem 2.

References

[1] J. R. Blum, B. Eisenberg and L.-S. Hahn, Ergodic theory and the measure of sets in the Bohr group, *Acta Sci. Math.*, **34** (1973), 17—24.

[2] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences,* Interscience Tracts, John Wiley and Sons (New York, 1974).

[3] I. Niven, Uniform distribution of sequences of integers, *Trans. Amer. Math. Soc.*, **98** (1961), 52—61.

[4] I. Niven, Uniform distribution of sequences of integers, *Compositio Math.*, **16** (1964), 158—160.

[5] W. A. Veech, Well distributed sequences of integers, *Trans. Amer. Math. Soc.*, **161** (1971), 63—70.

SCHOOL OF MATHEMATICS
THE INSTITUTE FOR ADVANCED STUDY
PRINCETON, NEW JERSEY, U.S.A.

(Received January 11, 1974)

Dissipative J-self-adjoint operators and associated J-isometries

By C. R. PUTNAM in West Lafayette (Indiana, USA)

1. Introduction. Only bounded operators on a Hilbert space $\mathfrak{H}$ will be considered in this paper. Let J be self-adjoint. If A is any operator satisfying

$$JA = A^*J, \tag{1.1}$$

then A will be called J-self-adjoint; similarly, if V satisfies

$$V^*JV = J, \tag{1.2}$$

V will be called J-isometric or a J-isometry. This terminology corresponds to that in the literature dealing with geometry of spaces having indefinite metrics. Thus, if (x, y) is the usual inner product on $\mathfrak{H}$ and if one introduces the modified inner product $(x, y)_J = (Jx, y)$ then A is J-self-adjoint if $(Ax, y)_J = (x, Ay)_J$ for all x, y in $\mathfrak{H}$. This is the same as $(JAx, y) = (Jx, Ay)$, that is, (1.1). Similarly, V is J-isometric if $(Vx, Vy)_J = (x, y)_J$ for all x, y in $\mathfrak{H}$, which is equivalent to (1.2). See, in particular, the surveys by KREIN [5] and NAIMARK and ISMAGILOV [6] where, for the most part, it is assumed that $J^2 = I$. Another kind of indefinite scalar product is considered by BEREZIN [1]. In the present paper, the aforementioned restriction $J^2 = I$ will be considerably relaxed (see (1.5) below) but additional conditions ((1.3), (1.4)) will be imposed on the operators A and V of (1.1) and (1.2).

Throughout it will be supposed that if A satisfies (1.1) then $\mathrm{Im}\,(A) = (A - A^*)/2i$ satisfies

$$\text{either} \quad \mathrm{Im}\,(A) \geqq 0 \quad \text{or} \quad \mathrm{Im}\,(A) \leqq 0. \tag{1.3}$$

An operator A will be called dissipative if the first part of (1.3) holds; thus, condition (1.3) is that either A or $-A$ be dissipative. (This definition coincides with that of SZ.-NAGY and FOIAŞ [9], p. 167. It should be noted, however, that sometimes A

This work was supported by a National Science Foundation research grant.

is said to be dissipative if $\operatorname{Re}(A) \leqq 0$; see, e.g., KATO [4], p. 279). Further, it will be supposed that if V satisfies (1.2) then

$$(1.4) \qquad 1 \notin \operatorname{sp}(V) \quad \text{and either} \quad VV^* \leqq I \quad \text{or} \quad VV^* \geqq I.$$

The first inequality of (1.4) is of course equivalent to $\|V\| \leqq 1$, that is, that V is a contraction. Incidentally, if (1.2) holds then $\|J\| \leqq \|J\| \, \|V\|^2$ so that, unless $J=0$, necessarily $\|V\| \geqq 1$.

It will be convenient to recall the notion of the absolutely continuous part of a self-adjoint operator J. If J has the spectral resolution $J=\int t dE_t$, then the set, $\mathfrak{H}_a(J)$, of vectors x in $\mathfrak{H}$ for which $\|E_t x\|^2$ is an absolutely continuous function of t is a subspace of $\mathfrak{H}$ invariant under J. If $\mathfrak{H}_a(J) \neq 0$, the restriction $J_a = J|\mathfrak{H}_a(J)$ is called the absolutely continuous part of J; in particular, J is said to be absolutely continuous if $J=J_a$. (See, e.g., HALMOS [3], p. 104, KATO [5], p. 516.) For later use, let $P_0(J)=\{x: Jx=0\}$; clearly, $\mathfrak{H}_a(J) \perp P_0(J)$.

Theorem 1. *Let J be self-adjoint and suppose that J and A are bounded operators on a Hilbert space $\mathfrak{H}$ satisfying* (1.1), (1.3) *and*

$$(1.5) \qquad J \neq J_a \oplus 0, \quad \text{that is,} \quad \mathfrak{H}_a(J) \oplus P_0(J) \quad \text{is a proper subspace of } \mathfrak{H}.$$

Then there exists a subspace $\mathfrak{M}$ satisfying

$$(1.6) \qquad \mathfrak{M} \supset (\mathfrak{H}_a(J) \oplus P_0(J))^{\perp} \neq 0,$$

reducing both A and J and for which

$$(1.7) \qquad A|\mathfrak{M} \quad \text{is self-adjoint.}$$

It is understood that either term in the direct sum on the right side of the inequality (1.5) may be absent, that is, that either $\mathfrak{H}_a(J)$ or $P_0(J)$ may be the 0 space. In particular, if J has no absolutely continuous part and if 0 is not in the point spectrum of J then $\mathfrak{M}$ of (1.6) is $\mathfrak{H}$ and so, by (1.7), A is self-adjoint.

Theorem 2. *Let J be self-adjoint and suppose that J and V are bounded operators on a Hilbert space $\mathfrak{H}$ satisfying* (1.2), (1.4) *and* (1.5). *Then there exists a subspace $\mathfrak{M}$ satisfying* (1.6), *reducing both V and J and for which*

$$(1.8) \qquad V|\mathfrak{M} \quad \text{is unitary.}$$

The proof of Theorem 1 will be given in section 2 and will depend on a general result on commutators in PUTNAM [7], p. 20. The proof of Theorem 2 will be derived in section 3 as a corollary of Theorem 1 via the Cayley transform. Some remarks on the Theorems as well as some applications will be given in section 4.

2. Proof of Theorem 1. In view of (1.1),

$$AJ-JA = (A-A^*)J, \tag{2.1}$$

therefore,

$$(JA)J-J(JA) = iC, \quad \text{where} \quad C = 2J(\mathrm{Im}\,(A))J. \tag{2.2}$$

Let $\mathfrak{N}$ denote the least subspace of $\mathfrak{H}$ reducing both self-adjoint operators JA and J and containing the range of the self-adjoint operator C. By (1.3), either $C\geqq 0$ or $C\leqq 0$, and so, by the Theorem of [7], p. 20, $\mathfrak{N}\subset(\mathfrak{H}_a(J)\cap\mathfrak{H}_a(JA))\subset\mathfrak{H}_a(J)$, hence $\mathfrak{N}^\perp\supset(\mathfrak{H}_a(J))^\perp$. In addition, it is clear that $\mathfrak{N}^\perp$ reduces both J and JA (and C) and that $C|\mathfrak{N}^\perp=0$. Thus, if $x\in\mathfrak{N}$, $0=(Cx, x)=2(\mathrm{Im}\,(A)Jx, Jx)$, hence, since $\mathrm{Im}\,(A)$ is semi-definite,

$$\mathrm{Im}\,(A)Jx = 0 \quad \text{for} \quad x\in\mathfrak{N}^\perp. \tag{2.3}$$

Next, note that $P_0(J)\subset(\mathfrak{H}_a(J))^\perp\subset\mathfrak{N}^\perp$ and that $\mathfrak{N}^\perp\ominus P_0(J)\supset(\mathfrak{H}_a(J)\oplus P_0(J))^\perp\neq 0$, the last inequality by (1.5). Let

$$\mathfrak{M} = \mathfrak{N}^\perp\ominus P_0(J) \quad (\neq 0). \tag{2.4}$$

It is clear that $\mathfrak{M}$ reduces J. Also, if $x\in\mathfrak{M}$ and $y\in P_0(J)$ then $(JAx, y)=(Ax, Jy)=0$, so that, since $\mathfrak{N}$ reduces JA, so also does $\mathfrak{M}$. Thus,

$$\mathfrak{M} \text{ reduces } J \text{ and } JA. \tag{2.5}$$

Further,

$$J(\mathfrak{M}) \text{ is dense in } \mathfrak{M}. \tag{2.6}$$

In fact, otherwise, there would exist a vector $y\in\mathfrak{M}$, $y\neq 0$, such that $0=(Jx, y)=$ $=(x, Jy)$ for all $x\in\mathfrak{M}$. Hence $y\in P_0(J)$ and hence $y\in M\cap P_0(J)$, so $y=0$, a contradiction.

It now follows from (2.1), (2.3) and (2.6) that

$$AJx = JAx \quad \text{for} \quad x\in\mathfrak{M}. \tag{2.7}$$

In view of (2.5) and (2.6), this implies that $\mathfrak{M}$ is invariant under A. Finally, relations (1.1), (2.5) and (2.6) imply that $\mathfrak{M}$ is also invariant under A^*. Thus, $\mathfrak{M}$ reduces A and relations (2.1), (2.6) and (2.7) imply (1.7).

3. Proof of Theorem 2. Since $1\notin\mathrm{sp}\,(V)$, the operator $A=i(I+V)(I-V)^{-1}$ is bounded. Further it is easily verified that $-i\notin\mathrm{sp}\,(A)$ and that V is the Cayley transform of A, that is

$$V = (A-iI)(A+iI)^{-1} \quad \text{and} \quad A = i(I+V)(I-V)^{-1}. \tag{3.1}$$

A straightforward calculation shows that A satisfies (1.1) if and only if V satisfies (1.2). Furthermore, $(I-V)(\mathrm{Im}\,(A))(I-V^*)=I-VV^*$, so that $\mathrm{Im}\,(A)\geqq 0$ or $\leqq 0$ according as $I-VV^*\geqq 0$ or $\leqq 0$; in this connection, see [9], p. 357.

In order to prove Theorem 2 one need only define A as in (3.1) and then apply Theorem 1 to A. Then the space $\mathfrak{M}$ of Theorem 1 clearly reduces V while (1.7) implies (1.8) by the well-known properties of the Cayley transform.

4. Remarks. It may be noted that the first part of (1.4), namely, that 1 not be in the spectrum of V, is essential in Theorem 2 for the validity of assertion (1.8). In fact, if $J=I$ and if V denotes the unilateral shift, then, although $1\in \mathrm{sp}\,(V)$ (in fact, $\mathrm{sp}\,(V)$ is the unit disk $\{z\colon |z|\leqq 1\}$), nevertheless, V is a contraction, V and J satisfy (1.2) and (1.5), and V is irreducible, so that, in particular, V has no unitary part; cf. [3], p. 73.

It is clear that if (1.1) holds and if J is non-singular, then A^* is similar to A and hence A and A^* have identical spectra. Further, condition (1.3) implies that the spectrum of A lies either in the upper half-plane or in the lower half-plane. Thus, if J is non-singular then (1.1) and (1.3) imply that the spectrum of A is real. Hence, for instance, if A is also normal it is necessarily self-adjoint. On the other hand, there exist non-singular self-adjoint operators J and dissipative operators A for which (1.1) holds and for which A is completely non-self-adjoint, that is, A has no reducing space on which it is self-adjoint. It follows from Theorem 1 that such an operator J is necessarily absolutely continuous.

To obtain such a pair J and A, let A be the operator on $\mathfrak{H}=L^2(0, 1)$ defined by

$$(Ax)(t) = t\,x(t)+i\int_0^t x(s)\,ds.$$

Then A is dissipative (see [9], p. 365). In addition, A is completely non-self-adjoint and is similar to the self-adjoint multiplication operator $A_0=t$ on $L^2(0, 1)$. (This result is due to SAHNOVIČ; see [9], pp. 368, 372.) Let T denote any non-singular operator T for which $A=TA_0T^{-1}$. If T has the polar factorization $T=PU$ where P is positive and U is unitary, then $A=PUA_0U^*P^{-1}$ and $A^*=P^{-1}UA_0U^*P=$ $=P^{-2}AP^2$, so that (1.1) holds with $J=P^{-2}$. It follows from Theorem 1 that P^{-2}, hence also P, must be absolutely continuous.

It is clear from the above argument that if T is non-singular with the polar factorization $T=PU$ and if B is any self-adjoint operator then (1.1) holds with $A=TBT^{-1}$ and $J=P^{-2}$.

Concerning not necessarily bounded dissipative operators and, in particular, ones similar to self-adjoint operators, see SZ.-NAGY and FOIAŞ [9], Chapt. IX, §§ 4, 5, as well as their paper [8].

Reference

[1] F. A. BEREZIN, On the Lee model, *Amer. Math. Soc. Translations* (2), **56** (1966) 249—272.

[2] P. R. HALMOS, *Introduction to Hilbert space and the theory of spectral multiplicity,* 2nd edition, Chelsea (1951).

[3] P. R. HALMOS, *A Hilbert space problem book,* van Nostrand (1967).

[4] T. KATO. *Perturbation theory for linear operators,* Springer-Verlag (New York, 1966).

[5] M. G. KREIN, Introduction to the geometry of indefinite J-spaces and to the theory of operators in those spaces, *Amer. Math. Soc. Translations* (2), **93** (1970), 103—176.

[6] M. A. NAIMARK and R. S. ISMAGILOV, Representations of groups and algebras in spaces with indefinite metric, *Progress in Mathematics,* **10** (Mathematical Analysis), edited by R. V. Gamkrelidze; Plenum Press (New York—London, 1971).

[7] C. R. PUTNAM, *Commutation properties of Hilbert space operators and related topics* (Ergebnisse der Math., 36), Springer-Verlag (1967).

[8] B. SZ.-NAGY and C. FOIAŞ, Sur les contractions de l'espace de Hilbert. X. Contractions similaires à des transformations unitaires, *Acta Sci. Math.* **26** (1965), 79—91.

[9] B. SZ.-NAGY and C. FOIAŞ, *Harmonic analysis of operators on Hilbert space,* Akadémiai Kiadó and American Elsevier Pub. Co., Inc. (Budapest and New York, 1970).

PURDUE UNIVERSITY
WEST LAFAYETTE, INDIANA

(Received January 31, 1974)

An identity for Laguerre polynomials

By L. B. RÉDEI in Umeå (Sweden)

Dedicated to my loved father, Professor László Rédei, on the occasion of his seventy-fifth birthday.

We shall prove the following representation for Laguerre polynomials:

$$L_n(x) = (-1)^n \frac{e^x}{n!}\left(x\frac{d^2}{dx^2}+\frac{d}{dx}\right)^n e^{-x}. \tag{1}$$

(We use the same convention for $L_n(x)$ as in reference [1].) This representation for $L_n(x)$ is an analogue of the well known representation for Hermite polynomials:

$$H_n(x) = (-1)^n e^{x^2}\left(\frac{d}{dx}\right)^n e^{-x^2}.$$

In spite of its simple and potentially useful form, we have not been able to find formula (1) in any of the standard texts.

Proof. Using the standard representation

$$L_n(x) = \frac{1}{n!}e^x\left(\frac{d}{dx}\right)^n (x^n e^{-x}) \tag{2}$$

we can put equation (1) into the equivalent form

$$A_n(x) = (-1)^n \left(\frac{d}{dx}\right)^n (x^n e^{-x}), \tag{3}$$

$A_n(x)$ being defined by

$$A_n(x) = \left(x\frac{d^2}{dx^2}+\frac{d}{dx}\right)^n e^{-x}.$$

We proceed by induction. Equation (3) is obviously true for $n=0$ and for $n=1$. We assume it to be true for n. It then follows that

$$A_{n+1}(x) = \left(x\frac{d^2}{dx^2}+\frac{d}{dx}\right)\left[(-1)^n\left(\frac{d}{dx}\right)^n(x^n e^{-x})\right] =$$
$$= (-1)^n\left(x\frac{d^{n+2}}{dx^{n+2}}(x^n e^{-x})+\frac{d^{n+1}}{dx^{n+1}}(x^n e^{-x})\right).$$

We use, for the first term in the right hand side of this equation, the identity

$$\left(\frac{d}{dx}\right)^n(xf(x)) = n\frac{d^{n-1}}{dx^{n-1}}f(x)+x\frac{d^n}{dx^n}f(x)$$

valid for any smooth function $f(x)$, to obtain that

$$A_{n+1}(x) = (-1)^n\left[\frac{d^{n+2}}{dx^{n+2}}(x^{n+1}e^{-x})-(n+1)\frac{d^{n+1}}{dx^{n+1}}(x^n e^{-x})\right].$$

Since

$$\frac{d}{dx}(x^{n+1}e^{-x}) = (n+1)x^n e^{-x}-x^{n+1}e^{-x}$$

it follows that

$$A_{n+1}(x) = (-1)^{n+1}\left(\frac{d}{dx}\right)^{n+1}(x^{n+1}e^{-x}).$$ Q.E.D.

Reference

[1] Bateman Manuscript Project, *Higher Transcendental Functions*, vol. II (New York, 1953).

DEPT. OF THEORETICAL PHYSICS
UNIVERSITY OF UMEÅ

(Received September 5, 1974)

Subnormal limits of nilpotent operators

By NORBERTO SALINAS in Ann Arbor (Michigan, USA)

1. Introduction. Let $\mathfrak{H}$ be a fixed separable, infinite dimensional complex Hilbert space and let $\mathcal{L}(\mathfrak{H})$ denote the algebra of all (bounded, linear) operators on $\mathfrak{H}$. In [3, Problem 7] HALMOS has asked for a characterization of the set of all operators in $\mathcal{L}(\mathfrak{H})$ which are uniform limits of nilpotent operators. In what follows we shall denote by $N(\mathfrak{H})$ the set of all nilpotent operators on $\mathfrak{H}$. In the recent paper [5] HERRERO made a remarkable contribution to Halmos' problem by showing that a normal operator is in the uniform closure $\overline{N(\mathfrak{H})}$ of $N(\mathfrak{H})$ if and only if its spectrum is connected and contains the origin [5, Theorem 7]. In his paper Herrero asked whether the direct sum of a unilateral shift in $\mathcal{L}(\mathfrak{H})$ and a normal operator on $\mathfrak{H}$ whose spectrum coincides with the closed unit disk is in $\overline{N(\mathfrak{H}\oplus\mathfrak{H})}$. In the present note we answer this question in the affirmative. Actually, we prove a more general result making a further progress in the solution of Halmos' question.

Our main theorem can be stated as follows:

Theorem 1.1. *If T is a subnormal operator on $\mathcal{L}(\mathfrak{H})$ whose approximate point spectrum is simply connected and contains the origin, then T is the uniform limit of nilpotent operators.*

The proof of the above theorem requires some auxiliary results and will be given in Section 2. In the final section of this paper we introduce a subclass of $\overline{N(\mathfrak{H})}$ which we call the class of pseudonilpotent operators and we study some of its properties. The main characteristic of these operators is that its nilpotent approximants are easy to determine. From this point of view, pseudonilpotent operators are perhaps more tractable than an arbitrary operator in $\overline{N(\mathfrak{H})}$.

2. Proof of Theorem 1.1. Throughout, for a given operator T in $\mathcal{L}(\mathfrak{H})$ we shall denote by $\sigma(T)$ the spectrum of T and by $\sigma_l(T)$ the left spectrum of T (or approximate point spectrum of T). Furthermore, we denote by $E(T)$ the essential spectrum of T and by $E_l(T)$ the left essential spectrum of T. (We recall that $E(T)$ and $E_l(T)$ are the spectrum and the left spectrum, respectively of the image of T in the Calkin algebra.) Also, in what follows D will denote the closed unit disk of the complex plane.

Theorem 2.1. *Let T be a subnormal operator in $\mathcal{L}(\mathfrak{H})$ such that $\sigma(T)\subset D$ and let M be a normal operator in $\mathcal{L}(\mathfrak{H})$ such that $\sigma(M)=D$. Then $T\oplus M\in\overline{N(\mathfrak{H}\oplus\mathfrak{H})}$.*

Proof. If T is a normal operator, then $T\oplus M$ is a normal operator whose spectrum is connected and contains the origin and hence the theorem follows from [5, Theorem 7]. Therefore, we may assume that T is not normal. Let $\mathfrak{K}$ be a complex Hilbert space and let N be a normal operator in $\mathcal{L}(\mathfrak{K})$ such that N is a minimal normal extension of the subnormal operator T, i.e. $\mathfrak{H}$ is an invariant subspace of N such that $N|\mathfrak{H}=T$ and the smaller reducing subspace of N containing $\mathfrak{H}$ coincides with $\mathfrak{K}$ [2]. Since T is not normal it is easy to see that $\mathfrak{K}\ominus\mathfrak{H}$ is infinite dimensional. Thus, after an identification via a suitable unitary transformation, we can assume that $\mathfrak{K}=\mathfrak{H}\oplus\mathfrak{H}$ and that N can be represented by the 2×2 operator matrix

$$N=\begin{bmatrix} S & O_{\mathfrak{H}} \\ R & T \end{bmatrix},$$

where R and S are in $\mathcal{L}(\mathfrak{H})$ and $0_{\mathfrak{H}}$ is the zero operator on $\mathfrak{H}$. It also follows that $\sigma(N)\subset\sigma(T)$ and hence $\sigma(N)\subset\sigma(M)$. Now we observe that for every $n=1, 2, \ldots$

$$D=\sigma(M)=\sigma\left\{\left[\sum_{j=1}^{n}\oplus\frac{n-j}{n}(M\oplus N)\right]\oplus M\right\}.$$

An easy exercise in spectral theory shows that for every $\varepsilon>0$ and every $n=1, 2, \ldots$ there exists a unitary transformation $U_{\varepsilon,n}\colon\mathfrak{H}\to\sum_{1}^{3n+1}\oplus\mathfrak{H}$ such that

$$\left\|U_{\varepsilon,n}MU_{\varepsilon,n}^{-1}-\left\{\left[\sum_{j=1}^{n}\oplus\frac{n-j}{n}(M\oplus N)\right]\oplus M\right\}\right\|<\varepsilon.$$

Therefore, since $M\in\overline{N(\mathfrak{H})}$ (cf. [5, Theorem 7]), it follows that in order to prove that $T\oplus M\in\overline{N(\mathfrak{H}\oplus\mathfrak{H})}$ it suffices to establish the following assertion: For every $n=2, 3, \ldots$ there exists and operator in $N\left(\sum_{1}^{3n+1}\oplus\mathfrak{H}\right)$ whose distance to the operator

$$A_n=T\oplus\left[\sum_{j=1}^{n}\oplus\frac{n-j}{n}(M\oplus N)\right]$$

is less that $\frac{1}{n}$. To prove this fact, for $n=2, 3, \ldots$, let

$$B_n=\frac{n-1}{n}T\oplus\left\{\sum_{j=1}^{n-1}\oplus\left[\frac{n-j}{n}(M\oplus N)-\frac{1}{n}(0_{\mathfrak{H}}\oplus 0_{\mathfrak{H}}\oplus T)\right]\right\}\oplus 0_{\mathfrak{H}}\oplus 0_{\mathfrak{H}}\oplus 0_{\mathfrak{H}}.$$

Since $A_n-B_n=\left[\sum_{j=1}^{n}\oplus\frac{1}{n}(T\oplus 0_{\mathfrak{H}}\oplus 0_{\mathfrak{H}})\right]\oplus 0_{\mathfrak{H}}$ we deduce that $\|A_n-B_n\|\leqq\frac{1}{n}$, $n=$ $=2, 3, \ldots$. Now we show that the operator B_n is the uniform limit of nilpotent operators. In fact, the operator B_n can be represented as the direct sum of a lower triangular $n\times n$ matrix whose j-th diagonal term is $\frac{n-j}{n}(T\oplus M\oplus S)$ and the operator

$0_{\mathfrak{H}}$. Thus, in order to complete the proof of theorem (cf. [5, Theorem 5]) it remains to show that $T\oplus M\oplus S\in\overline{N(\mathfrak{H}\oplus\mathfrak{H}\oplus\mathfrak{H})}$. To see this let's observe first that

$$S\oplus T=\lim_{\varepsilon\to 0}\begin{bmatrix} S & 0_{\mathfrak{H}} \\ \varepsilon R & T\end{bmatrix}=\lim_{\varepsilon\to 0}\begin{bmatrix} 1_{\mathfrak{H}} & 0_{\mathfrak{H}} \\ 0_{\mathfrak{H}} & \varepsilon 1_{\mathfrak{H}}\end{bmatrix}\begin{bmatrix} S & 0_{\mathfrak{H}} \\ R & T\end{bmatrix}\begin{bmatrix} 1_{\mathfrak{H}} & 0_{\mathfrak{H}} \\ 0_{\mathfrak{H}} & \dfrac{1}{\varepsilon}1_{\mathfrak{H}}\end{bmatrix}.$$

In view of the last remark, the fact that $\overline{N(\mathfrak{H}\oplus\mathfrak{H}\oplus\mathfrak{H})}$ is invariant under similarities and since

$$N\oplus M=\begin{bmatrix} S & 0_{\mathfrak{H}} \\ R & T\end{bmatrix}\oplus M$$

is in $\overline{N(\mathfrak{H}\oplus\mathfrak{H}\oplus\mathfrak{H})}$ we conclude that $S\oplus T\oplus M$ and hence $T\oplus M\oplus S$ is in $\overline{N(\mathfrak{H}\oplus\mathfrak{H}\oplus\mathfrak{H})}$, as desired.

Corollary 2.2. *Let U be a unilateral shift in $\mathscr{L}(\mathfrak{H})$ and let M be a normal operator in $\mathscr{L}(\mathfrak{H})$ such that $\sigma(M)=D$. Then $U\oplus M\in\overline{N(\mathfrak{H}\oplus\mathfrak{H})}$.*

The following lemma generalizes a result in [5].

Lemma 2.3. *Let $T\in\overline{N(\mathfrak{H})}$ and let S be an operator in the uniformly closed, inverse closed algebra generated by T. Then $TS\in\overline{N(\mathfrak{H})}$.*

Proof. By hypothesis there exists a sequence $\{f_n\}$ of rational functions with poles off $\sigma(T)$ such that $\lim\limits_{n\to\infty}\|S-f_n(T)\|=0$. Also, there exists a sequence $\{Q_k\}$ in $N(\mathfrak{H})$ such that $\lim\limits_{k\to\infty}\|T-Q_k\|=0$. Now let k_1 be the first positive integer such that $\|f_1(T)-f_1(Q_{k_1})\|<1$; having defined k_n, $n\geqq 1$ let k_{n+1} be the first positive integer greater than k_n such that $\|f_{n+1}(T)-f_{n+1}(Q_{k_{n+1}})\|<\dfrac{1}{n+1}$. Letting $R_n=Q_{k_n}$ $(n=1, 2, \ldots)$ it readily follows that $\lim\limits_{n\to\infty}\|TS-R_nf_n(R_n)\|=0$. Since $R_nf_n(R_n)\in N(\mathfrak{H})$ $(n=1, 2, \ldots)$ we conclude that $TS\in\overline{N(\mathfrak{H})}$.

Proof of theorem 1.1. Let T be a subnormal operator in $\mathscr{L}(\mathfrak{H})$ such that $\sigma_l(T)$ is simply connected and contains the origin. It follows that $\sigma(T)=\sigma_l(T)-E(T)=E_l(T)$. From [6] we deduce that, up to a small norm perturbation, T is unitarily equivalent to an operator of the form $T\oplus T'$ where T' is any normal operator in $\mathscr{L}(\mathfrak{H})$ such that $\sigma(T')=E(T')=\sigma(T)$. Since, up to a small norm perturbation and a unitary equivalence, T' can be replaced in the above direct sum by a normal operator N in $\mathscr{L}(\mathfrak{H})$ whose spectrum $\sigma(N)$ is "closed" to $\sigma(T)$ in the Hausdorff metric topology, and such that $\sigma(N)$ is simply connected, has smooth boundary and contains $\sigma(T)$ in its interior, in order to complete the proof of the theorem it suffices to prove that $T\oplus N\in\overline{N(\mathfrak{H}\oplus\mathfrak{H})}$, for any normal operator N in $\mathfrak{H}$ satisfying the properties described previously. Let φ be a homeomorphism from $\sigma(N)$ onto D such that $\varphi(0)=0$, φ is analytic in the interior of $\sigma(N)$ and φ maps the boundary of $\sigma(N)$ onto the boundary of D. (The existence of this function φ can be deduced from standard facts in the theory of conformal mappings.) Since $\sigma(N)$ is simply connected and φ is analytic on $\sigma(T)$ it follows that $\varphi(T)$ is subnormal and $\sigma[\varphi(T)]=\varphi[\sigma(T)]$ is contained in the interior of D. Employing the fact that $\varphi(N)$ is normal and $\sigma[\varphi(N)]=D$, from Theorem 2.1 we deduce that $\varphi(T)\oplus\varphi(N)\in\overline{N(\mathfrak{H}\oplus\mathfrak{H})}$. Let $\psi\colon D\to\sigma(N)$ be the inverse function of φ. Since $\psi(0)=0$, there exists a continuous complex valued function η on D which is analytic on the interior of D and satisfies $\psi(\lambda)=\lambda\eta(\lambda)$, for every $\lambda\in D$. Observing that $\eta[\varphi(T)]\oplus\eta[\varphi(N)]$ is in the uniformly closed, inverse closed algebra generated by $\varphi(T)\oplus\varphi(N)$ and using Lemma 2.3 we conclude that

$$T\oplus N\big(=\psi[\varphi(T)]\oplus\psi[\varphi(N)]=\varphi(T)\eta[\varphi(T)]\oplus\varphi(N)\eta[\varphi(N)]=$$
$$=[\varphi(T)\oplus\varphi(N)]\{\eta[\varphi(T)]\oplus\eta[\varphi(N)]\}\big)$$

is in $\overline{N(\mathfrak{H}\oplus\mathfrak{H})}$, as asserted.

Remark 2.4. Since the subset of elements with connected spectrum in any complex Banach algebras with identity is closed in the norm topology (cf. [8, Theorem 3]) and the spectrum is an uppersemicontinuous function, it follows that every operator T in $\overline{N(\mathfrak{H})}$ must satisfy

(*) $\qquad \sigma(T)$ and $E(T)$ are connected and $E(T)$ contains the origin.

Let $\Omega(T)=\{\lambda\in\sigma(T)\colon T-\lambda$ is not a Fredholm operator of index zero$\}$. From the continuity properties of the index function on the set of semi-Fredholm operators in $\mathscr{L}(\mathfrak{H})$ we see that every operator T in $\overline{N(\mathfrak{H})}$ must also satisfy

(**) $$\Omega(T)=E_l(T)\cap E_r(T).$$

(Recall that $E_r(T)$ is the conjugate set of $E_l(T^*)$). Conversely, we conjecture that if an operator T in $\mathscr{L}(\mathfrak{H})$ satisfies conditions (*) and (**), then $T\in\overline{N(\mathfrak{H})}$. The validity of this conjecture would imply of course that every quasinilpotent operator on $\mathfrak{H}$ is in $\overline{N(\mathfrak{H})}$, answering in the affirmative Problem 7 of [3].

Let $QT(\mathfrak{H})$ be the set of all quasitriangular operators on $\mathfrak{H}$, i.e. $T\in QT(\mathfrak{H})$ if and only if there exists an increasing sequence $\{P_n\}$ in $\mathscr{L}(\mathfrak{H})$ of finite rank projections tending strongly to the identity such that $\lim_{n\to\infty}\|TP_n-P_nTP_n\|=0$ (cf. [3, Problem 4]). From the spectral characterization of quasitriangular operators given in [1] it readily follows that $QT(\mathfrak{H})\cap QT(\mathfrak{H})^*=\{T\in\mathscr{L}(\mathfrak{H})\colon\Omega(T)=E_l(T)\cap E_r(T)\}$. Following the same circle of ideas of the above comments, we conjecture that $QT(\mathfrak{H})\cap QT(\mathfrak{H})^*$ is the uniform closure of the set of all algebraic operators on $\mathfrak{H}$. (We recall that an operator T in $\mathscr{L}(\mathfrak{H})$ is called an algebraic operator if there exists a polynomial p such that $p(T)=0$.) The results of [4], [5] and those of the present paper give partial affirmative answers to the above conjectures.

It may also be worth noting that if the first conjecture were true, it would follow from the above mentioned theorem of [1] that every operator in $\mathscr{L}(\mathfrak{H})$ which is not in $\overline{N(\mathfrak{H})}$ has a non-trivial invariant subspace, thereby reducing the invariant subspace problem to operators in $\overline{N(\mathfrak{H})}$.

3. Pseudonilpotent operators. In the rest of the paper it will be convenient to adopt the following terminology. Let $\mathfrak{H}_1, \ldots, \mathfrak{H}_n$ be an orthogonal family of n subspaces of $\mathfrak{H}$ such that $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$. Then every T in $\mathscr{L}(\mathfrak{H})$ can be represented, on the decomposition $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$, by an $n\times n$ matrix of the form

$$T=\begin{bmatrix} T_{11} & T_{12} & \cdots & T_{1n} \\ T_{21} & T_{22} & \cdots & T_{2n} \\ \vdots & \vdots & & \vdots \\ T_{n1} & T_{n2} & \cdots & T_{nn} \end{bmatrix}$$

where T_{ij} is a bounded, linear transformation from $\mathfrak{H}_j$ into $\mathfrak{H}_i$, $1\leq i, j\leq n$. The operator in $\mathscr{L}(\mathfrak{H})$ represented by the lower triangular matrix

$$\begin{bmatrix} T_{11} & 0 & & \ldots & 0 \\ T_{21} & T_{22} & 0 & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ & & & & 0 \\ T_{n1} & T_{n2} & & \cdots & T_{nn} \end{bmatrix}$$

will be called the lower triangular part of T with respect to the decomposition $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$. Similarly, the upper triangular part of T with respect to the decomposition $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$ is the operator in $\mathscr{L}(\mathfrak{H})$ represented by the upper triangular matrix

$$\begin{bmatrix} T_{11} & T_{12} & \cdots & T_{1n} \\ 0 & T_{22} & \cdots & T_{2n} \\ \vdots & & \ddots & \\ 0 & 0 & \ldots & T_{nn} \end{bmatrix}.$$

Definition 3.1. Let $T\in\mathscr{L}(\mathfrak{H})$. We say that T is a *pseudonilpotent operator* if for every $\varepsilon>0$ there exists a decomposition of $\mathfrak{H}$ into the direct sum of a finite orthogonal family of subspaces $\mathfrak{H}_1, \ldots, \mathfrak{H}_n$ such that the norm of the lower triangular part of T with respect to the decomposition $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$ is less than ε. The set of all pseudonilpotent operators in $\mathscr{L}(\mathfrak{H})$ will be denoted by $P(\mathfrak{H})$.

Remark 3.2. a) By interchanging the subspaces $\mathfrak{H}_1, \ldots, \mathfrak{H}_n$ in definition 3.1 it is easy to see that an operator T is in $P(\mathfrak{H})$ if and only if for every $\varepsilon>0$ there exists a decomposition of $\mathfrak{H}$ into the direct sum of a finite orthogonal family of subspaces such that the norm of the upper triangular part of T with respect to this decomposition is less than ε.

b) From a) it readily follows that $P(\mathfrak{H})=P(\mathfrak{H})^*$.

c) From definition 3.1 and the fact that if $T\in N(\mathfrak{H})$, then there always exists a decomposition $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$ with respect to which the lower triangular part of T has norm zero, we see that the following inclusion formula holds:

$$N(\mathfrak{H})\subset P(\mathfrak{H})\subset \overline{N(\mathfrak{H})}.$$

In the following two theorems we shall see that these inclusions are actually proper.

Theorem 3.3. *Let A be a non-zero positive operator in $\mathscr{L}(\mathfrak{H})$ such that $\sigma(A)$ is connected. Then $A\in\overline{N(\mathfrak{H})}$, but $A\notin P(\mathfrak{H})$.*

Proof. From [5, Theorem 7] we deduce that $A\in\overline{N(\mathfrak{H})}$, thus it remains to show that $A\notin P(\mathfrak{H})$. Let $\mathfrak{H}_1, \dots, \mathfrak{H}_n$ be an orthogonal family of subspaces of $\mathfrak{H}$ such that $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$ and let A be represented by

$$A=\begin{bmatrix} A_{11} & A_{12} \dots A_{1n} \\ A_{21} & A_{22} \dots A_{2n} \\ \vdots & \ddots \vdots \\ A_{n1} & A_{n2} \dots A_{nn} \end{bmatrix}$$

on the decomposition $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$. Let B and C be the operators in $\mathscr{L}(\mathfrak{H})$ defined by

$$B=\begin{bmatrix} A_{11} & 0 & 0 \\ A_{21} & A_{22} & 0 \dots 0 \\ \vdots & & \ddots \\ A_{n1} & A_{n2} & \dots\ A_{nn} \end{bmatrix}, \quad C=\begin{bmatrix} A_{11} & 0 & \dots & 0 \\ 0 & A_{22} & 0 \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & A_{nn} \end{bmatrix}.$$

It follows that $A+C=B+B^*$. Since C is a positive operator we infer that

$$\|A\| = \sup_{\substack{x\in\mathfrak{H}\\ \|x\|=1}} (Ax, x) \leqq \sup_{\substack{x\in\mathfrak{H}\\ \|x\|=1}} ([A+C]x, x) = \|A+C\| = \|B+B^*\| \leqq 2\|B\|,$$

and hence $\|B\|\geqq\|A\|/2$. Observing that B is the lower triangular part of A with respect to the decomposition $\mathfrak{H}=\sum_{j=1}^{n}\oplus\mathfrak{H}_j$, and since the family $\mathfrak{H}_1, \dots, \mathfrak{H}_n$ is arbitrary we conclude that $A\notin P(\mathfrak{H})$.

Theorem 3.4. *If K is a quasinilpotent compact operator on $\mathfrak{H}$, then $K\in P(\mathfrak{H})$.*

Proof. Let K be any quasinilpotent compact operator in $\mathscr{L}(\mathfrak{H})$. Then there exists an increasing sequence $\{P_n\}$ in $\mathscr{L}(\mathfrak{H})$ of finite rank projections tending strongly to the identity such that $\lim_{n\to\infty} \|K-P_nKP_n\|=0$. From the upper semicontinuity of the spectrum, given $\varepsilon>0$ there exists a positive integer n_0 such that if $n>n_0$, then $\sigma(P_nKP_n)$ is contained in the disk of center zero and radius ε. Let $m>n_0$ so that $\|K-P_mK\|<\varepsilon$. Since $P_n\mathfrak{H}$ is finite dimensional there exists a basis $e_1, \ldots, e_k$ of P_m on which the representing matrix of the operator $P_mK|P_m\mathfrak{H}$ is in the upper triangular form. Observe that the diagonal elements of this matrix are in absolute value less than ε. Letting $\mathfrak{H}_j$ be the span of the vector e_j, $1\leqq j\leqq k$ and defining $\mathfrak{H}_{k+1}=\mathfrak{H}\ominus P_m\mathfrak{H}$, we deduce that the lower triangular part of K with respect to the decomposition $\mathfrak{H}=\sum_{j=1}^{k+1}\oplus\mathfrak{H}_j$ has norm less than 3ε. Since ε is arbitrary we conclude that $K\in P(\mathfrak{H})$.

As a consequence of the next theorem we shall see that there are operators in $P(\mathfrak{H})$ which are not quasinilpotent.

In the remainder of the paper $\{e_n\ (n=1, 2, \ldots)\}$ will be a fixed orthonormal basis of $\mathfrak{H}$. A weighted shift S with positive weights α_n $(n=1, 2, \ldots)$ on the basis $\{e_n\}$ is defined by $Se_n=\alpha_n e_{n+1}$ $(n=1, 2, \ldots)$.

Theorem 3.5. *Let S be a weighted shift on the basis $\{e_n\}$ with positive weights α_n $(n=1, 2, \ldots)$ such that for every $\varepsilon>0$ there exists a positive integer k satisfying $\alpha_{nk}<\varepsilon$, for $n=1, 2, \ldots$. Then $S\in P(\mathfrak{H})$.*

Proof. Let $\varepsilon>0$ and let k be a positive integer greater than 1 such that $\alpha_{nk}<\varepsilon$, for $n=1, 2, \ldots$. Furthermore, let $\mathfrak{H}_j$ be the span of the vectors e_{j+ik} $(i=0, 1, 2, \ldots)$. Then $\mathfrak{H}_j$ is infinite dimensional, $1\leqq j\leqq k$, and the representing matrix of S on the decomposition $\mathfrak{H}=\sum_{j=1}^{k}\oplus\mathfrak{H}_j$ has the form

$$S=\begin{bmatrix} 0 & 0 & \cdots\cdots & S_k \\ S_1 & 0 & \cdots\cdots & 0 \\ 0 & S_2 & \cdots\cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots\ S_{k-1} & 0 \end{bmatrix},$$

where, for $1\leqq j\leqq k-1$, the bounded, linear transformation $S_j\colon \mathfrak{H}_j\to\mathfrak{H}_{j+1}$ is unitarily equivalent to a diagonal operator in $\mathscr{L}(\mathfrak{H})$ whose diagonal terms are α_{j+ik} $(i=0, 1, 2, \ldots)$ and $S_k\colon \mathfrak{H}_k\to\mathfrak{H}_1$ is a bounded linear transformation unitarily equivalent to a weighted shift with weights α_{nk}. Thus $\|S_k\|<\varepsilon$ and hence $S^{\prime}\in P(\mathfrak{H})$. Therefore $S\in P(\mathfrak{H})$ and our assertion is established.

Corollary 3.6. *There exists an operator in $P(\mathfrak{H})$ whose spectrum coincides with D and hence is not quasinilpotent.*

Proof. Let S be the Kakutani shift on the basis $\{e_n\}$, i.e. S is the weighted shift whose sequence of weights is described as follows: every other weight is one;

every other weight of the remaining weights is 1/2; every other weight of these weights is 1/4; etc. For the sake of clarity we list the first few terms of the sequence of weights:

$$1, 1/2, 1, 1/4, 1, 1/2, 1, 1/8, 1, 1/2, 1, 1/4, \ldots .$$

From Theorem 3.5 it follows that $S\in P(\mathfrak{H})$. On the other hand, as is well known, KAKUTANI proved that $\sigma(S)=D$ [7, p. 282].

In view of the results of this section and the comment made at the end of Section 2 it is natural to pose the following two questions.

Problem 1. Is every quasinilpotent operator on $\mathfrak{H}$ in $P(\mathfrak{H})$?

Problem 2. Does every operator in $P(\mathfrak{H})$ have a non-trivial invariant subspace?

Addendum: The results proved in the present note were obtained in the Spring of 1973 and were communicated to several mathematicians interested in the subject during the Wabash International Conference on Banach spaces held in June 1973. After this paper was written C. Apostol, C. Foiaş and D. Voiculescu announced that they established the validity of the conjectures stated at the end of section 2. This announcement was recently communicated to the author by C. Apostol via a personal letter.

Added in proof (May 5, 1975). The results referred to in Addendum appeared in C. APOSTOL, C. FOIAŞ and D. VOICULESCU, On the norm closure of nilpotents. II, *Rev. Roum. Math. Pures et Appl.*, **19** (1974), 549—577, and D. VOICULESCU, Norm-limits of algebraic operators, *Rev. Roum. Math. Pures et Appl.*, **19** (1974) 371—378.

References

[1] C. APOSTOL, C. FOIAŞ, and D. VOICULESCU, Some result on non-quasitriangular operators. IV, *Rev. Roum. Math. Pures et Appl.*, **18** (1973), 487—514.

[2] P. R. HALMOS, *A Hilbert space problem book*, Van Nostrand (Princeton, N. J., 1967).

[3] P. R. HALMOS, Ten problems in Hilbert space, *Bull. Amer. Math. Soc.*, **76** (1970), 887—933.

[4] JAMES H. HEDLUND, Limits of nilpotent and quasinilpotent operators, *Michigan Math. J.*, **19** (1972), 249—255.

[5] DOMINGO HERRERO, Normal limits of nilpotent operators, *Indiana U. Math. J.*, **23** (1974), 1097—1108.

[6] C. PEARCY and N. SALINAS, Compact perturbations of seminormal operators, *Indiana U. Math. J.*, **22** (1973), 789—793.

[7] C. E. RICKART, *General theory of Banach algebras*, Van Nostrand (Princeton, N. J., 1960).

[8] NORBERTO SALINAS, Operators with essentially disconnected spectrum, *Acta Sci. Math.*, **33** (1972), 193—205.

UNIVERSITY OF MICHIGAN

(Received January 20, 1974)

Eine Kennzeichnung der endlichen einfachen Gruppe der Ordnung 604 800

Von VOLKER STINGL in Mainz (BRD)

§ 1. Einleitung

Im Jahre 1967 entdeckte Z. JANKO eine neue sporadische einfache Gruppe der Ordnung 604 800. Diese Gruppe, die wir mit J_2 bezeichnen wollen, enthält genau zwei Konjugiertenklassen von Involutionen. Der Zentralisator einer Involution, die nicht im Zentrum einer Sylow-2-Untergruppe von J_2 vorkommt, ist dabei isomorph zum direkten Produkt einer Vierergruppe mit PSL (2, 5).

Das Ziel der vorliegenden Arbeit ist es, die Gruppe J_2 durch den Zentralisator einer nicht 2-zentralen Involution zu kennzeichnen.

Für die Problemstellung und zahlreiche wertvolle Hinweise und Ratschläge möchte ich Herrn Prof. Dr. D. HELD hiermit noch einmal herzlichst danken.

Wir beweisen nun das folgende Resultat:

Satz. *Sei G eine endliche einfache Gruppe und t eine Involution in G, so daß $C_G(t)/O(C_G(t))$ isomorph ist zum direkten Produkt einer Vierergruppe mit $PSL(2, q)$, die Primzahlpotenz q sei kongruent drei oder fünf modulo acht. Dann ist G isomorph zu J_2.*

Mit J_2 sei stets die in [6] beschriebene endliche einfache Gruppe der Ordnung 604 800 gemeint.

Im weiteren bezeichne G immer eine Gruppe, die die Voraussetzungen des Satzes erfüllt, und t sei eine festgewählte Involution in G, deren Zentralisator die oben angegebene Struktur besitzt.

Die Bezeichnungsweise folgt im wesentlichen [1] und [5]. Ferner werden folgende Symbole benutzt:

$\|X\|_2$ (bzw. $\|X\|_{2'}$)	2-Anteil (bzw. 2′-Anteil) der Ordnung von X	
D_n	Diedergruppe	der Ordnung n
Q_n	verallg. Quaternionengruppe	der Ordnung n
Z_n	zyklische Gruppe	der Ordnung n
E_n	elementar abelsche Gruppe	der Ordnung n

$\mathrm{Syl}_p(X)$	Menge der Sylow-p-Untergruppen von X
$X \pmod N)_Y$	volles Urbild der Untergruppe X von Y/N in Y

Es sei $N(X)=N_G(X)$ bzw. $C(X)=C_G(X)$ für Teilmengen X von G und $C=C(t)$. Wir setzen $C/O(C)=E\times P$ mit $E\cong E_4$ und $P\cong PSL(2,q)$, q sei kongruent drei oder fünf modulo acht.

§ 2. Die Berechnung von $N(A)/C(A)$

Lemma 2.1. *Es sei A eine Sylow-2-Untergruppe von C. Es kann A geschrieben werden als direktes Produkt zweier Vierergruppen V und W mit $V\in\mathrm{Syl}_2(E(\mathrm{mod}\ O(C))_C)$ und $W\in\mathrm{Syl}_2(P(\mathrm{mod}\ O(C))_C)$. Die Involution t liegt in V. Wir setzen $V=\langle t,u\rangle$ und $W=\langle i,z\rangle$. Es gilt: $|N(A)/C(A)|=6n$, $1\leqq n\leqq 6$. Es existiert ein Element ϱ der Ordnung drei, unter dessen Operation die* 15 *Involutionen aus A in folgende Konjugiertenklassen zerfallen:*

$$\{i,z,iz\},\quad \{t\},\quad \{ti,tz,tiz\},\quad \{u\},\quad \{ui,uz,uiz\},\quad \{ut\},\quad \{uti,utz,utiz\}.$$

Beweis. Aufgrund eines Ergebnisses von WALTER [9] kann A keine Sylow-2-Untergruppe von G sein, und damit teilt zwei die Ordnung von $N(A)/C(A)$. Aus der Voraussetzung des Satzes erhalten wir: $|N_{C/O(C)}(AO(C)/O(C))|=3$. Mit Hilfe des Frattini-Argumentes folgt, daß auch drei ein Teiler der Ordnung von $N(A)/C(A)$ ist. Außerdem kann in $N(A)\cap C/C(A)$ ein Element $\varrho\neq 1$ gewählt werden mit $t^\varrho=t$, $u^\varrho=u$, $i^\varrho=z$, $z^\varrho=iz$.

Da A echt in einer Sylow-2-Untergruppe T von G enthalten ist, muß $Z(T)$ echt in A enthalten sein. Folglich sind nicht alle Involutionen aus A in G konjugiert. Die Anzahl der Konjugierten von t unter $N(A)$ wird durch $|N(A)/C(A): N(A)\cap C/C(A)|$ geliefert. Also ist die Ordnung von $N(A)/C(A)$ kleiner als 45. Nach dem oben bewiesenen Teil erhalten wir insgesamt $|N(A)/C(A)|=6n$, wobei n zwischen eins und sieben liegt. Da die Gruppe $GL(4,2)$ keine Untergruppe der Ordnung 42 enthält, scheidet der Fall $n=7$ aus. Das Lemma ist bewiesen.

Lemma 2.2. *Für jede Involution α aus $N(A)/C(A)$ gilt $t^\alpha\notin W$.*

Beweis. Wir nehmen an, die Behauptung sei falsch. Es gibt also eine Involution α in $N(A)/C(A)$, die t in W abbildet. Da t in W^α liegt und die Elemente aus W^α in G konjugiert sind, ist $W\cap W^\alpha=\langle 1\rangle$, folglich muß A direktes Produkt von W und W^α sein. Es ist t im Durchschnitt von V und W^α enthalten. Da die Involution α in A mindestens eine Vierergruppe zentralisiert, rechnet man leicht nach, daß sogar $W^\alpha=V$ und $V^\alpha=W$ gilt.

Unter der Operation von α und ϱ zerfällt A in zwei Konjugiertenklassen von Involutionen mit den Vertretern t und ti, die Länge der Klassen beträgt 6 bzw. 9.

Das erzwingt $|N(A)/C(A)|=18$. Eine Sylow-2-Untergruppe S von $N(A)$ hat die Ordnung 2^5, die Operation von α auf A bewirkt $|Z(S)|=4$. Also ist A charakteristisch in S, dies bedeutet, daß S schon Sylow-2-Untergruppe von G ist. Mit Hilfe von [3, Lemma 2, Seite 389] sieht man, daß G nicht einfach ist. Dies widerspricht der Voraussetzung des Satzes. Die Annahme zu Beginn des Lemmas ist falsch, die Behauptung daher richtig.

Lemma 2.3. *Wir unterscheiden zwei Möglichkeiten der Operation von Involutionen aus $N(A)/C(A)$ auf A, nämlich:*

(i) *t^α liegt in V für jede Involution α aus $N(A)/C(A)$,*

(ii) *es existiert eine Involution in $N(A)/C(A)$, die t in $A\setminus(V\cup W)$ abbildet. Im ersten Falle gilt $|N(A)/C(A)|=6$ oder 24, im zweiten Falle enthält $N(A)/C(A)$ eine zu A_4 isomorphe Untergruppe.*

Beweis. Liegt Fall (i) vor, so besitzt eine Sylow-2-Untergruppe von $N(A)/C(A)$ genau eine Involution. Diese normalisiert V, ohne t zu zentralisieren. Mit Hilfe von Lemma 2.1 sehen wir, daß die Anzahl a_t der zu t unter $N(A)$ konjugierten Involutionen zwischen 2 und 12 liegt. Außerdem ist a_t kongruent null modulo zwei und kongruent zwei modulo drei. Es folgt, daß t unter $N(A)$ zwei oder acht Konjugierte besitzt. Die Behauptungen für den Fall (i) sind damit bewiesen.

Sei $M=\{\{ti, tz, tiz\}, \{ui, uz, uiz\}, \{uti, utz, utiz\}\}$ und M_1 ein Element aus M. Gibt es eine Involution α in $N(A)/C(A)$ mit $t^\alpha\in M_1$ und $m^\alpha\in M_1$ für ein von t^α verschiedenes Element m aus M_1, so operiert die von α und ϱ erzeugte Gruppe der Ordnung zwölf als Permutationsgruppe auf der Ziffernmenge $\{t\}\cup M_1$, und die Behauptung ist bewiesen.

Wir können also annehmen: $t^\alpha\in M_1$, $m^\alpha\notin M_1$ für ein von t^α verschiedenes Element m aus M_1. Setze $U=\langle\varrho, \alpha\rangle$ und a_t=Anzahl der Konjugierten von t unter U. Offensichtlich ist a_t größer als vier. Hat a_t den Wert sechs, so sind gerade die Involutionen aus V und M_1 zu t konjugiert, insbesondere ist $(V^\#)^\alpha=M_1$. Das liefert einen Widerspruch, da V Gruppe ist $M\cup\{1\}$ jedoch nicht.

Sei $a_t=8$, dies bedeutet, daß U die Ordnung 24 besitzt. Daraus ergibt sich $o(\alpha\cdot\varrho)=4$ und $U\cong S_4$ oder $o(\alpha\cdot\varrho)=6$ und $U\cong A_4\times Z_2$.

Ist $a_t=10$, so hat U die Ordnung 30 und besitzt eine normale Sylow-3-Untergruppe. Dies widerspricht jedoch der Tatsache, daß U von einer Involution und einem Element der Ordnung drei erzeugt wird.

Sei schließlich $a_t=12$. Bis auf i, z, iz sind nun alle Involutionen aus A zu t konjugiert. Für ein von t^α verschiedenes Element m aus M_1 gilt $mm^\alpha\notin\{i, z, iz\}$, aber $\alpha\in C(mm^\alpha)$. Dies liefert einen Widerspruch.

Wir haben gesehen, daß a_t nur den Wert acht annehmen kann, in diesem Falle ist aber die Behauptung des Lemmas richtig.

Lemma 2.4. *Liegt der Fall* (i) *aus Lemma* 2.3 *vor, so haben wir:*

(i)$_1$ $N(A)/C(A)\cong Z_6$ *oder* (i)$_2$ $N(A)/C(A)\cong SL(2,3)$.

Im Falle (ii) *aus Lemma* 2.3 *sei* U *eine zu* A_4 *isomorphe Untergruppe und* $S_1\in \mathrm{Syl}_2(U(\mathrm{mod}\ C(A))_{N(A)})$. *Dann gilt:*

(ii)$_1$ $Z(S_1)=\langle ut\rangle$, $N(A)/C(A)\cong A_4$, S_4 *oder* $A_4\times Z_2$,

(ii)$_2$ $Z(S_1)=W$, $N(A)/C(A)\subseteq A_4$, S_4 *oder* $A_4\times Z_3$,

(ii)$_3$ $Z(S_1)=\langle ut\rangle\times W$, $N(A)/C(A)\cong A_4$, S_4 *oder* $A_4\times Z_2$.

Beweis. Es liege zunächst der Fall (i) vor mit $|N(A)/C(A)|=6$. Wir setzen $N(A)/C(A)=\langle\varrho,\alpha\rangle$, wobei α eine Involution sei und ϱ den Automorphismus der Ordnung drei aus Lemma 2.1 bezeichne. Wir können o. B. d. A. annehmen, daß $t^\alpha=u$ gilt. Die Involution α zentralisiert in A mindestens eine Gruppe der Ordnung acht, da andernfalls wie in Lemma 2.2 ein Widerspruch zur Einfachheit von G folgt. Ist $W^\alpha\neq W$, so gilt $W\in\{\{ti, tz, tiz\}, \{ui, uz, uiz\}, \{uti, utz, utiz\}\}$, was aber einen Widerspruch liefert, da W Gruppe ist. Es wird also W von α normalisiert, insbesondere erhalten wir $C_A(\alpha)=\langle ut\rangle\times W$. Die Elemente α und ϱ sind auf den vier Erzeugenden t, u, i, z von A vertauschbar, die Behauptung (i)$_1$ ist richtig.

Sei nun im Fall (i) von Lemma 2.3 die Ordnung von $N(A)/C(A)$ gleich 24. Dann sind die Sylow-2-Untergruppen von $N(A)/C(A)$ isomorph zu Q_8. Eine Sylow-3-Untergruppe von $N(A)/C(A)$ liegt nicht normal, da es in GL(4, 2) keine Elemente der Ordnung zwölf gibt. Man rechnet nun nach, daß die Sylow-2-Untergruppe von $N(A)/C(A)$ normal liegt und daher die Behauptung $N(A)/C(A)\cong SL(2,3)$ folgt.

In Lemma 2.3 haben wir bewiesen, daß es im Falle (ii) eine zu A_4 isomorphe Untergruppe in $N(A)/C(A)$ gibt. Es ist $|N(A)/C(A)|=12$, 24 oder 36. Gilt $|N(A)/C(A)|=24$, so können die Sylow-2-Untergruppen von $N(A)/C(A)$ nur isomorph zu D_8 oder E_8 sein. Im ersten Falle ergibt sich $N(A)/C(A)\cong S_4$, im zweiten Falle folgt $N(A)/C(A)\cong A_4\times Z_2$. Gilt $|N(A)/C(A)|=36$, so liegt die Vierergruppe aus der zu A_4 isomorphen Untergruppe normal in $N(A)/C(A)$, mithin folgern wir $N(A)/C(A)\cong A_4\times Z_3$.

Sei U die zu A_4 isomorphe Untergruppe von $N(A)/C(A)$, die den Automorphismus ϱ von A aus Lemma 2.1 enthält. Wir wählen uns $S_1\in\mathrm{Syl}_2(U(\mathrm{mod}\ C(A))_{N(A)})$. Das Zentrum von S_1 ist echt in A enthalten. Unter der Annahme $Z(S_1)\cong E_8$ erhalten wir $Z(S_1)\cap V\neq\langle 1\rangle$. Ohne Beschränkung der Allgemeinheit sei $Z(S_1)\cap V=\langle ut\rangle$. Mit Hilfe des Frattini-Argumentes sehen wir, daß $Z(S_1)$ das direkte Produkt von $\langle ut\rangle$ und W ist. Die Involution t kann in A maximal acht Konjugierte besitzen, es schneidet der Fall $N(A)/C(A)\cong A_4\times Z_3$ aus.

Ist $Z(S_1)\cong E_4$, so schließt man leicht, daß $Z(S_1)$ gleich W ist. Jede Involution aus U zentralisiert in A genau die Gruppe W. Unter U haben t, u und ut jeweils vier Konjugierte in A. Die Konjugiertenklassen sind: $\{t, ti, tz, tiz\}$, $\{u, ui, uz, uiz\}$, $\{uti, utz, utiz, ut\}$. Es gibt eine Involution α in U mit $t^\alpha=ti$, $tz^\alpha=tiz$, $u^\alpha=uz$ und

$ui^\alpha = uiz$. Man rechnet nun leicht nach, daß es keine mit α vertauschbare Involution β gibt, die t auf u abbildet und W zentralisiert. Eine solche Involution müßte aber im Falle $N(A)/C(A) \cong A_4 \times Z_2$ existieren, also tritt dieser Fall nicht auf, wenn $Z(S_1)$ die Ordnung vier hat.

Ist $Z(S_1)$ isomorph zu Z_2, so liegt $Z(S_1)$ in V. Ohne Beschränkung der Allgemeinheit sei $\langle ut \rangle = Z(S_1)$. Es ist klar, daß eine Involution aus U nur eine Vierergruppe in A zentralisiert. Außerdem wird W von keiner Involution aus U normalisiert. Damit ergibt sich, daß eine Involution aus W unter U genau sechs Konjugierte hat und von einem 2-Element aus U zentralisiert wird. Also hat t in A nicht mehr als acht Konjugierte, der Fall $N(A)/C(A) \cong A_4 \times Z_3$ ist nicht möglich.

§ 3. Der Fall $(i)_1$ aus Lemma 2.4

Lemma 3.1. *Sei S eine Sylow-2-Untergruppe von $N(A)$ und $N(A)/C(A)$ sei isomorph zu Z_6. Dann ist S isomorph zum direkten Produkt einer Diedergruppe der Ordnung acht und einer Vierergruppe.*

Beweis. Wir wissen schon, daß S die Ordnung 2^5 hat und $Z(S)$ in A enthalten ist, weiterhin ist $Z(S)$ von der Ordnung acht. Gibt es in $S \setminus A$ keine Involutionen, so liegt A charakteristisch in S und S ist schon Sylow-2-Untergruppe von G. Es sei x ein Element aus $S \setminus A$. Die Anwendung von [8, Lemma 5.38, Seite 411, Thompson Transfer Lemma] auf die maximale Untergruppe $\langle x, Z(S) \rangle$ von S und die Involution t liefert einen Widerspruch zur Einfachheit von G.

Es gibt nun Involutionen in $S \setminus A$, und die Behauptung des Lemmas folgt.

Lemma 3.2. *Im Falle $N(A)/C(A) \cong Z_6$ ist eine Sylow-2-Untergruppe von G isomorph zum direkten Produkt einer Diedergruppe und einer Vierergruppe.*

Beweis. Ist eine Sylow-2-Untergruppe S von $N(A)/C(A)$ schon Sylow-2-Untergruppe von G, so folgt die Behauptung mit Hilfe von Lemma 3.1.

Es sei nun T eine Sylow-2-Untergruppe von G, die S enthält, und T_0 maximal in T bezüglich folgender Eigenschaften:

(i) $S \subseteqq T_0$, (ii) $T_0 = T_1 \times T_2$ mit $T_1 \cong D_{2m}$ $3 \leqq m$, und $T_2 \cong E_4$.

Wir nehmen nun an, daß T_0 echt in T enthalten sei. Es enthält T_0 genau zwei Konjugiertenklassen von elementar abelschen Untergruppen der Ordnung 16. Wir finden ein Element x in $N_T(T_0) \setminus T_0$, dessen Quadrat in T_0 liegt. Sind in der Nebenklasse xT_0 keine Involutionen vorhanden, so ergibt sich $\langle x, T_0 \rangle \in \mathrm{Syl}_2(G)$. Es sei T_Z die maximale zyklische Untergruppe von T_1. Die Gruppe $\langle x, T_Z \times T_2 \rangle$ ist maximal in $\langle x, T_0 \rangle$ und enthält t nicht. Mit Hilfe des Thompson Transfer Lemmas erhalten wir einen Widerspruch zur Einfachheit von G.

Es gibt Involutionen in xT_0, o. B. d. A. sei $x^2=1$. Wir wählen in T_0 zwei Involutionen u und b, die in T_0 nicht konjugiert sind und folgende Eigenschaften besitzen: $a^x=b$, $\langle a, b\rangle \cong D_2m$. Das Erzeugnis von x und a ist dann isomorph zu D_2m+1. Man stellt fest, daß x zentralisierend auf $Z(T_1)\times T_2$ operiert. Die Gruppe $\langle x, T_0\rangle$ ist demnach isomorph zum direkten Produkt einer Diedergruppe mit einer Vierergruppe, was der maximalen Wahl von T_0 widerspricht. Folglich gilt $T_0=T$, die Behauptung ist bewiesen.

Lemma 3.3. *Der Fall $N(A)/C(A)\cong Z_0$ tritt nicht auf.*

Beweis. Da nach Lemma 3.2 eine Sylow-2-Untergruppe T von G isomorph zum direkten Produkt einer Diedergruppe mit einer Vierergruppe ist und G mindestens zwei Konjugiertenklassen von Involutionen besitzt, folgt mit Hilfe des Thompson Transfer Lemmas ein Widerspruch zur Einfachheit von G.

§ 4. Der Fall $(i)_2$ aus Lemma 2.4

Lemma 4.1. *Es sei $N(A)/C(A)$ isomorph zu $SL(2, 3)$ und α die zentrale Involution in $N(A)/C(A)$. Mit B bezeichnen wir das volle Urbild von $\langle\alpha\rangle$ in $N(A)$. Es sei S_1 eine Sylow-2-Untergruppe von B und S eine Sylow-2-Untergruppe von $N(A)$, die S_1 enthält. Dann gilt: $N(A)/B\cong A_4$, $S/S_1\cong E_4$, $S_1\cong D_8\times E_4$, $Z(S_1)=\langle ut\rangle\times W$. Es operiert $N(A)/B$ treu auf $Z(S_1)$, aber trivial auf $\langle ut\rangle$.*

Beweis. Es ist $SL(2, 3)/Z(SL(2, 3))=PSL(2, 3\cong A_4$ und die beiden ersten Behauptungen folgen. Da A ein maximaler elementar abelscher Normalteiler von S ist, gibt es eine Gruppe A_0 der Ordnung acht in A, die ebenfalls normal in S liegt. Die Involution α aus $N(A)/C(A)$ operiert trivial auf A_0. Wir wissen, daß t^α in V ist, o. B. d. A. sei $t^\alpha=u$. Unter $N(A)$ hat t außer sich selbst und u noch genau sechs weitere Konjugierte. Es folgt $A_0=\langle ut, i, z\rangle$. Gibt es in $S_1\setminus A$ keine Involutionen, so liegt A charakteristisch in S, es ist S eine Sylow-2-Untergruppe von G. Seien y_1 und y_2 aus $S\setminus S_1$ so gewählt, daß S von A, y_1 und y_2 erzeugt wird. Die maximale Untergruppe $\langle y_1, y_2, A_0\rangle$ von S enthält t nicht ,wir erhalten einen Widerspruch zur Einfachheit von G. Ist nun x eine Involution in $S_1\setminus A$, so ergibt sich: $S_1=$ $=\langle x, t\rangle\times W\cong D_8\times E_4$.

Da der Automorphismus ϱ aus $N(A)/C(A)$ nichttrivial auf $Z(S_1)$, aber trivial auf $\langle ut\rangle$ operiert, genügt es zu zeigen, daß ein Element β der Ordnung vier aus $N(A)/C(A)$ nichttrivial auf $Z(S_1)$, aber trivial auf $\langle ut\rangle$ wirkt, um die letzte Behauptung von Lemma 4.1 zu beweisen. Dies ist aber richtig, da tt^β in A_0 liegt und von $(tt^\beta)^\beta$ verschieden ist. Außerdem liegt $\langle ut\rangle$ charakteristisch in S_1. Damit haben wir alle Behauptungen bewiesen.

Lemma 4.2. *Es sei wieder* $N(A)/C(A)$ *isomorph zu* $SL(2, 3)$. *Mit* T *bezeichnen wir eine Sylow-2-Untergruppe von* G, *die* $S \in \mathrm{Syl}_2(N(A))$ *enthält. Die Untergruppe* S_1 *von* S *sei wie in Lemma* 4.1 *definiert. Es gilt:* $C_T(Z(S_1))$ *ist isomorph zum direkten Produkt einer Diedergruppe mit einer Vierergruppe.*

Beweis. Wir wissen schon, daß $C_S(Z(S_1)) = S_1$ isomorph zu $D_8 \times E_4$ ist. Im Falle $C_T(Z(S_1)) = C_S(Z(S_1))$ ist die Behauptung richtig. Sei nun $S_1 \subsetneqq C_T(Z(S_1))$, mit T_0 sei eine Untergruppe maximaler Ordnung von $C_T(Z(S_1))$ bezeichnet, die S_1 enthält und isomorph zum direkten Produkt einer Diedergruppe mit einer Vierergruppe ist. Wir nehmen an, daß T_0 echt in $C_T(Z(S_1))$ ist. Es existiert ein Element x in $C_T(Z(S_1)) \setminus T_0$ mit $T_0^x = T_0$ und $x^2 \in T_0$. Aufgrund der maximalen Wahl von T_0 gibt es in xT_0 keine Involutionen. Alle elementar abelschen Untergruppen der Ordnung 16 von $\langle x, T_0 \rangle$ liegen daher schon in T_0 und sind unter $\langle x, T_0 \rangle$ konjugiert. Es folgt $\langle x, T_0 \rangle = C_T(Z(S_1))$. Wir wählen Elemente y_1 und y_2 in $S \setminus S_1$, so daß $\langle y_1, y_2, S_1 \rangle = S$ wird. Dann gilt $\langle x, T_0, y_1, y_2 \rangle = T \in \mathrm{Syl}_2(G)$. Es sei D eine maximale Diedergruppe in T_0 und D_Z der zyklische Normalteiler vom Index zwei in D. Die Gruppe $\langle D_Z \times W, y_1, y_2, x \rangle$ hat den Index zwei in T und enthält t nicht. In $\langle D_Z \times W, y_1, y_2, x \rangle$ gibt es keine elementar abelschen Untergruppen der Ordnung 16, aber der Zentralisator einer jeden Involution in dieser Gruppe ist mindestens von der Ordnung 16. Dies zeigt, daß ein Widerspruch zur Einfachheit von G folgt. Also gilt $T_0 = C_T(Z(S_1))$, und die Behauptung ist bewiesen.

Lemma 4.3. *Wir übernehmen die Voraussetzungen und Bezeichnungen aus Lemma* 4.2. *Wir setzen* $T_0 = C_T(Z(S_1))$ *und* $T_1 = \langle T_0, y_1, y_2 \rangle$, *wobei* y_1 *und* y_2 *Elemente aus* $S \setminus S_1$ *sind mit* $\langle S_1, y_1, y_2 \rangle = S$. *Es gibt nun eine echte Untergruppe* T_2 *von* $T \in \mathrm{Syl}_2(G)$, *die die folgenden Eigenschaften besitzt:* (i) $|T_2 : T_1| = 2$, (ii) T_0 *ist normal in* T_2 *und* T_2/T_0 *ist isomorph zu* D_8, (iii) *es gibt eine Involution* x *in* $T_2 \setminus T_1$ *und eine Involution* a *in* T_0, *so daß* $\langle x, a \rangle$ *isomorph zu einer Diedergruppe ist und* $T_2 = \langle x, a, W, y_1, y_2 \rangle$ *gilt,* (iv) *jede Vierergruppe aus* $\langle x, a \rangle$ *liegt in genau einer elementar abelschen Untergruppe der Ordnung* 16 *von* T_2.

Beweis. Mit Hilfe der Techniken im Beweis von Lemma 4.2 berechnen wir, daß T_1 noch keine Sylow-2-Untergruppe von G sein kann. Es sei x ein Element aus $T \setminus T_1$, das T_1 normalisiert und dessen Quadrat in T_1 liegt. Die beiden Konjugiertenklassen von elementar abelschen Untergruppen der Ordnung 16 in T_1 werden durch x verbunden, also normalisiert x die Gruppe $Z(S_1)$, aber zentralisiert sie nicht. Es folgt. $\langle x, T_1 \rangle = N_T(Z(S_1))$ und $\langle x, T_1 \rangle / T_0 = D_8$. Wir setzen $T_2 = \langle x, T_1 \rangle$.

Wir nehmen an, daß es in xT_1 keine Involutionen gibt. Es ergibt sich nun leicht: $T_2 = T \in \mathrm{Syl}_2(G)$. In T_0 gibt es einen maximalen Normalteiler $D_Z \times W$, der t nicht enthält. Die Involution t kann nicht in die maximale Untergruppe $\langle D_Z \times W, y_1, y_2, x \rangle$ von T_2 konjugiert werden, was der Einfachheit von G widerspricht.

Es gibt Involutionen in xT_1, o. B. d. A. sei $x^2=1$. Da x die beiden Konjugiertenklassen von elementar abelschen Untergruppen der Ordnung 16 von T_0 miteinander verbinden muß, gibt es Involutionen a und b in T_0, die unter T_0 nicht konjugiert sind, die in T_0 eine Diedergruppe maximaler Ordnung erzeugen und durch x aufeinander abgebildet werden. Es wird dann $\langle x, a\rangle$ isomorph zu einer Diedergruppe, in der $\langle a, b\rangle$ vom Index zwei enthalten ist. Die Behauptung (iii) von Lemma 4.3 folgt.

Wie oben sieht man, daß t nicht in die maximale Untergruppe $\langle ax, W, y_1, y_2\rangle$ von T_2 konjugiert werden kann, also liegt T_2 echt in T. Ein Element y aus $N_{T'}(T_2)\setminus T_2$ mit $y^2\in T_2$ existiert und bewirkt, daß T_2 mindestens doppelt so viele elementar abelsche Untergruppen der Ordnung 16 besitzt wie T_1. Das ist aber nur möglich, wenn jede Vierergruppe aus $\langle x, a\rangle$ in mindestens einer elementar abelschen Gruppe der Ordnung 16 von T_1 liegt. Da t zu jeder nichtzentralen Involution von $\langle x, a\rangle$ konjugiert ist, folgt auch die Behauptung (iv) von Lemma 4.3.

Lemma 4.4. *Der Fall* $N(A)/C(A)\cong SL(2, 3)$ *tritt nicht auf.*

Beweis. Wir übernehmen die Voraussetzungen und Bezeichnungen von Lemma 4.3. Es sei y ein Element von $T\setminus T_2$ mit $T_2^y=T_2$ und $y^2\in T_2$. Der Durchschnitt aller elementar abelschen Untergruppen der Ordnung 16 von T_2 hat die Ordnung vier. Das Erzeignis T_E aller elementar abelschen Untergruppen der Ordnung 16 von T_2 hat in T_2 den Index zwei. Die einzigen Involutionen, die ein Element aus yT_2 in T_E zentralisieren kann, liegen schon in $Z(T_E)$. Es folgt, daß die Gruppe $\langle y, T_2\rangle$ genau so viele elementar abelsche Untergruppen der Ordnung 16 besitzt wie T_2. Alle diese Gruppen sind aber in $\langle y, T_2\rangle$ konjugiert. Wir schließen daher, daß $T=\langle y, T_2\in\rangle$ $\in \mathrm{Syl}_2(G)$ gilt.

Um einen endgültigen Widerspruch zu erlangen, konstruiert man wie in den vorausgegangenen Lemmata eine maximale Untergruppe T_M von T, in die die Involution t nicht durch Elemente aus G hineinkonjugiert werden kann.

§ 5. Der Fall $(ii)_1$ aus Lemma 2.4

Lemma 5.1. *Eine Sylow-2-Untergruppe von* $N(A)$ *hat im Falle* $(\mathrm{ii})_1$ *von Lemma* 2.4 *die Ordnung* 2^7.

Beweis. Wir nehmen an, die Behauptung sei falsch. Dann besitzt eine Sylow-2-Untergruppe S von $N(A)$ die Ordnung 2^6, es gilt: $N(A)/C(A)\cong A_4$. Das Zentrum von S liegt in A und hat die Ordnung zwei. Daraus folgert man, daß A die einzige elementar abelsche Untergruppe der Ordnung 16 von S ist. Mithin gilt $S\in \mathrm{Syl}_2(G)$.

Wir wählen Elemente y_1 und y_2 aus $S\setminus A$, die mit A zusammen bereits ganz S erzeugen. Die drei Nebenklassen y_1A, y_2A und y_1y_2A von A in S enthalten jeweils maximal vier Involutionen, der Zentralisator einer Involution aus $S \setminus A$ hat in S mindestens die Ordnung 16 und ist nicht elementar abelsch. Sei A_0 ein in A enthaltener Normalteiler der Ordnung acht in S. Die Gruppe $\langle A_0, y_1, y_2 \rangle$ enthält t nicht und ist maximal in S. Das Thompson Transfer Lemma liefert nun einen Widerspruch.

Lemma 5.2. *Gilt $N(A)/C(A) \cong S_4$, so enthält eine Sylow-2-Untergruppe S von $N(A)$ genau zwei elementar abelsche Untergruppen der Ordnung* 16. *Ist T eine Sylow-2-Untergruppe von G, die S enthält, so haben wir $S \subsetneqq T$.*

Beweis. Es sei U eine zu A_4 isomorphe Untergruppe von $N(A)/C(A)$ und S_1 eine Sylow-2-Untergruppe des vollen Urbildes von U in $N(A)$. Ferner sei die Sylow-2-Untergruppe S von $N(A)$ so gewählt, daß S_1 in S enthalten ist. Wie in Lemma 5.1 ist A die einzige elementar abelsche Untergruppe der Ordnung 16 in S_1. Ist A auch in S charakteristisch, so folgt ähnlich wie im vorhergehenden Lemma ein Widerspruch.

Es gibt nun außer A noch genau eine weitere elementar abelsche Untergruppe der Ordnung 16 in S. Mit x bezeichnen wir ein Element aus dieser Gruppe, das nicht in S_1 liegt. Die beiden Involutionen x und t erzeugen eine Diedergruppe der Ordnung acht, so daß $S = \langle x, t, W, y_1, y_2 \rangle$ wird, wobei y_1 und y_2 Elemente aus $S_1 \setminus A$ sind, die zusammen mit A ganz S_1 erzeugen. Da t in G nicht in die maximale Untergruppe $\langle xt, W, y_1, y_2 \rangle$ von S konjugiert werden kann, darf S noch keine Sylow-2-Untergruppe von G sein.

Lemma 5.3. *Es sei $N(A)/C(A)$ isomorph zu $A_4 \times Z_2$ und α die zentrale Involution in $N(A)/C(A)$. Mit B bezeichnen wir das volle Urbild von $\langle \alpha \rangle$ in $N(A)$. Es sei S_2 eine Sylow-2-Untergruppe von B und S eine Sylow-2-Untergruppe von $N(A)$, die S_2 enthält. Wir erhalten: $N(A)/B \cong A_4$, $S/S_2 \cong E_4$, $S_2 \cong D_8 \times E_4$, $Z(S_2) = \langle ut \rangle \times W$. Es operiert $N(A)/B$ treu auf $Z(S_2)$ und trivial auf $\langle ut \rangle$.*

Beweis. Die beiden ersten Bahauptungen sind trivial. Da A ein maximaler elementar abelscher Normalteiler von S ist, gibt es einen in A enthaltenen Normalteiler A_0 der Ordnung acht in S. Wie in Lemma 4.1 sieht man, daß A_0 das Erzeugnis von ut, i und z sein muß. Es sei U die zu A_4 isomorphe Untergruppe von $A_4 \times Z_2$ und S_1 eine Sylow-2-Untergruppe des vollen Urbildes von U in $N(A)$. Da $Z(S_1) = \langle ut \rangle$ ist, ergibt sich, daß U treu auf A_0 wirkt. Die Automorphismengruppe von A_0 ist isomorph zu $GL(3, 2)$, also operiert α trivial auf A_0. Es folgt $Z(S_2) = \langle ut \rangle \times W$, außerdem sind die beiden letzten Behauptungen von Lemma 5.3 bewiesen. Die Behauptung $S_2 \cong D_8 \times E_4$ folgt wie in Lemma 4.1.

Lemma 5.4. *Der Fall* (ii)$_1$ *aus Lemma* 2.4 *tritt nicht auf.*

Beweis. Mit Hilfe der Lemmata 5.1 bis 5.3 sehen wir, daß im Falle $(\mathrm{ii})_1$ von Lemma 2.4 die Faktorgruppe $N(A)/C(A)$ isomorph zu S_4 oder $A_4 \times Z_2$ ist. Nehmen wir an, daß $N(A)/C(A)$ isomorph zu S_4 ist, so besitzt eine Sylow-2-Untergruppe S von $N(A)$ genau zwei elementar abelsche Untergruppen der Ordnung 16 und hat den Index zwei in einer Sylow-2-Untergruppe T von G. Wir ersetzen im Beweis von Lemma 4.4 die Symbole T_2 bzw. a durch S bzw. t und erzielen wie in Lemma 4.4 einen Widerspruch zur Einfachheit von G. Ist $N(A)/C(A)$ isomorph zu $A_4 \times Z_2$, so haben wir in Lemma 5.3 die gleichen Behauptungen bewiesen wie in Lemma 4.1. Da die Lemmata 4.2 bis 4.4 nur auf Lemma 4.1 aufbauen, können die Beweise von dort wörtlich übernommen werden. Daraus folgt dann sofort die Behauptung des Lemmas.

§ 6. Der Fall $(ii)_2$ aus Lemma 2.4

Lemma 6.1. *Eine Sylow-2-Untergruppe von $N(A)$ hat im Falle* $(\mathrm{ii})_2$ *von Lemma* 2.4 *die Ordnung* 2^6.

Beweis. Wir nehmen an, die Behauptung sei falsch. Eine Sylow-2-Untergruppe S von $N(A)$ hat dann die Ordnung 2^7 und S/A ist isomorph zu D_8. Mit U sei die zu A_4 isomorphe Untergruppe von $N(A)/C(A)$ bezeichnet und mit S_1 eine Sylow-2-Untergruppe des vollen Urbildes von U in $N(A)$, die in S enthalten ist. Das Zentrum von S_1 ist W, ein Element aus $S \setminus S_1$ operiert nicht trivial auf W. In $S_1 \setminus A$ liegen höchstens zwölf Involutionen, in $S \setminus S_1$ höchstens acht. Der Zentralisator einer jeden Involution aus $S \setminus A$ besitzt eine andere 2-Struktur als der Zentralisator von t. Wir können daher t nicht aus A in $S \setminus A$ herauskonjugieren, insbesondere ist S schon Sylow-2-Untergruppe von G. Es sei wieder A_0 ein in A enthaltener Normalteiler der Ordnung acht von S. Die Elemente x und y aus $S \setminus A$ seien so bestimmt, daß S von A, x und y erzeugt wird. Es ist $\langle A_0, x, y \rangle$ eine maximale Untergruppe von S, in die t nicht durch Elemente aus G hineinkonjugiert werden kann. Wir erhalten einen Widerspruch zur Einfachheit von G.

Lemma 6.2. *Die Faktorgruppe $N(A)/C(A)$ ist im Falle* $(\mathrm{ii})_2$ *von Lemma* 2.4 *isomorph zu $A_4 \times Z_3$, die Gruppe G ist isomorph zu J_2.*

Beweis. Eine Sylow-2-Untergruppe S von $N(A)$ hat die Ordnung 2^6, das Zentrum von S ist elementar abelsch der Ordnung vier. Wir nehmen zunächst an, daß S schon eine Sylow-2-Untergruppe von G ist. Aus der Liste aller endlichen einfachen Gruppen in [4], deren Sylow-2-Untergruppen die Ordnung 2^6 haben, entnimmt man, daß G isomorph zu $U_3(4)$ oder $L_3(4)$ sein muß. Da eine Sylow-2-Untergruppe von $U_3(4)$ keinen elementar abelschen Normalteiler der Ordnung 16 besitzt und in einer zu $L_3(4)$ isomorphen Gruppe nur eine Konjugiertenklasse von Involutionen existiert, folgt jedoch ein Widerspruch.

Es sei nun T eine S enthaltenden Sylow-2-Untergruppe von G und x ein Element aus $N_T(S)\setminus S$, dessen Quadrat in S liegt. Wir erhalten für S die folgende Struktur: $S=\langle A, B\rangle$ mit $A\cong B\cong E_{16}$, $W=A\cap B=Z(S)$ und $A^x=B$. Die Gruppe $\langle x, S\rangle$ ist sicher eine Sylow-2-Untergruppe von G, da $\langle x, S\rangle$ genauso viele elementar abelsche Untergruppen der Ordnung 16 enthält wie S. Wir setzen $T=\langle x, S\rangle$, die Gruppe T hat die folgenden Eigenschaften: (i) $|T|=2^7$, (2) T enthält keinen elementar abelschen Normalteiler der Ordnung acht, (3) T besitzt einen elementar abelschen Normalteiler der Ordnung vier, dessen drei Involutionen in G konjugiert sind, (4) T ist Sylow-2-Untergruppe einer endlichen einfachen Gruppe. Aus den Hauptsätzen in [7] ergibt sich, daß T isomorph zu einer Sylow-2-Untergruppe von J_2 sein muß. Aufgrund einer Arbeit von GORENSTEIN und HARADA [2] und der Tatsache, daß G mindestens zwei Konjugiertenklassen von Involutionen besitzt, folgt $G\cong J_2$. Mit Hilfe von [6, Lemma 3.3 (2), Seite 35] erhalten wir schließlich $N(A)/C(A)\cong A_4\times Z_3$.

§ 7. Der Fall $(ii)_3$ aus Lemma 2.4

Lemma 7.1. *Es sei zunächst $N(A)/C(A)$ isomorph zu A_4. Dann besitzt eine Sylow-2-Untergruppe S von $N(A)$ eine zu $Z_4\times Z_4\times Z_2$ isomorphe maximale Untergruppe S_M. In $S\setminus S_M$ liegen nur Involutionen. Wir haben $3=|N(S)/SC(S)|_{2'}$. In $N(S)/SC(S)$ existiert ein Element, das die drei von A verschiedenen elementar abelschen Untergruppen der Ordnung 16 in S verbindet und treu auf W bzw. trivial auf $\langle ut\rangle$ operiert.*

Beweis. Es kann angenommen werden, daß in $S\setminus A$ Involutionen existieren, da andernfalls A charakteristisch in S ist und dann ähnlich wie früher ein Widerspruch zur Einfachheit von G folgt. Mit Hilfe von [3, Lemma 2, Seite 389] sehen wir, daß es in S keine elementar abelsche Untergruppe der Ordnung 2^5 gibt.

Es seien x und y Involutionen in $S\setminus A$ mit $S=\langle A, x, y\rangle$, weiterhin gelte $t^x=ti$ und $t^y=tz$. Man rechnet nach, daß tx und ty die Ordnung vier haben und miteinander vertauschbar sind. Wir setzen $S_M=\langle tx\rangle\times\langle ty\rangle\times\langle ut\rangle$. Da S genau 39 Involutionen enthält, S_M jedoch nur sieben Involutionen besitzt, können in $S\setminus S_M$ nur Involutionen liegen.

Die Faktorgruppe $N(A)/C(A)$ ist isomorph zu A_4 und es existiert ein Element der Ordnung drei in $N(A)/C(A)$, das treu auf W bzw. trivial auf $\langle ut\rangle$ operiert, daher folgen mit Hilfe des Frattini-Argumentes die restlichen Behauptungen von Lemma 7.1.

Lemma 7.2. *Es sei T eine S enthaltende Sylow-2-Untergruppe von G und T_1 Zentralisator von $\langle ut\rangle\times W$ in T. Es hat T_1 folgende Eigenschaften:* (i) *T_1 besitzt eine maximale Untergruppe T_2 mit $T_2\cong Z_{2^n}\times Z_{2^n}\times Z_2$ — $2\leqq n$,* (ii) *in $T_1\setminus T_2$ liegen nur Involutionen,* (iii) *es gibt in T_1 vier Konjugiertenklassen von elementar abelschen*

Untergruppen der Ordnung 16. *In* $N(T_1)/T_1C(T_1)$ *existiert ein Element, das die drei* A *nicht enthaltenden Konjugiertenklassen von elementar abelschen Untergruppen der Ordnung* 16 *in* T_1 *verbindet und treu auf* W *bzw. trivial auf* $\langle ut\rangle$ *operiert. Schließlich ist* $3=|N(T_1)/T_1C(T_1)|_{2'}$.

Beweis. Es sei T_{11} eine S enthaltende Untergruppe von T_1 mit maximaler Ordnung, so daß T_{11} alle in der Behauptung des Lemmas für T_1 geforderten Eigenschaften habe. Es liege T_{12} vom Index zwei in T_{11} mit $T_{12}=Z_2m\times Z_2m\times Z_2$. Wir nehmen an, die Gruppe T_{11} sei echt in T_1 enthalten. Wir wählen nun ein Element y_1, das in $N_{T_1}(T_{11})\setminus T_{11}$ liegt und dessen Quadrat in T_{11} enthalten ist. Dieses Element bewirkt auf den vier Konjugiertenklassen von elementar abelschen Untergruppen der Ordnung 16 in T_{11} eine Permutation der Ordnung zwei. Es sei r ein Element aus $N(T_{11})$ mit $\langle rT_{11}C(T_{11})\rangle\cong Z_3$, dann ist $\langle y_1T_{11}C(T_{11}), rT_{11}C(T_{11})\rangle$ isomorph zu A_4. Eine Sylow-2-Untergruppe T_0 des vollen Urbildes dieser zu A_4 isomorphen Gruppe in $N(T_{11})$ liegt in T_1 und enthält T_{11} mit dem Index vier. Wir wählen zu y_1 noch ein Element y_2 in $T_0\setminus T_{11}$, so daß T_0 von T_{11}, y_1 und y_2 erzeugt wird.

Sind in $T_0\setminus T_{11}$ keine Involutionen vorhanden, so ist T_0 schon Sylow-2-Untergruppe von G und wir erhalten leicht einen Widerspruch zur Einfachheit von G. Sei x eine Involution in $T_0\setminus T_{11}$. Gibt es in xT_{11} weniger als $|T_{11}|/2$ Involutionen, so liegt jede Involution aus $T_0\setminus T_{11}$ in einer elementar abelschen Untergruppe der Ordnung 16 von T_0, deren Normalisator in T_0 mindestens die Ordnung 2^7 besitzt und wie oben folgt ein Widerspruch.

In xT_{11} existieren genau $|T_{11}|/2$ Involutionen. Da x zwei Konjugiertenklassen von elementar abelschen Untergruppen der Ordnung 16 aus T_{11} konjugiert, gibt es zwei Involutionen a und b in T_{11}, die unter T_{11} nicht konjugiert sind, deren Produkt ein Element maximaler Ordnung in T_{12} ist und die durch x verbunden werden. Die Gruppe $\langle T_{12}, xa\rangle$ enthält T_{12} mit dem Index zwei und ist maximal in $\langle x, T_{11}\rangle$. Man rechnet nach, daß in $\langle x, T_{11}\rangle\setminus\langle T_{12}, xa\rangle$ nur Involutionen liegen und $\langle T_{12}, xa\rangle$ isomorph ist zu $Z_2m+1\times Z_2m\times Z_2$.

Sei y eine Involution aus $T_0\setminus\langle x, T_{11}\rangle$, dann gilt $T_0=\langle x, y, T_{11}\rangle$. Da T_0 keine elementar abelschen Untergruppen der Ordnung 32 enthält sind x und y nicht miteinander vertauschbar. Das Element ya besitzt die Ordnung 2^{m+1}, die Gruppe $\langle T_{12}, xa, ya\rangle$ enthält $\langle T_{12}, xa\rangle$ mit dem Index zwei und ist maximal in T_0. Wiederum stellt man durch Abzählen fest, daß es in $T_0\setminus\langle T_{12}, xa, ya\rangle$ nur Involutionen gibt. Dann folgt sofort: $\langle T_{12}, xa, ya\rangle=\langle xa\rangle\times\langle ya\rangle\times\langle ut\rangle\cong Z_2m+1\times Z_2m+1\times Z_2$.

Die Gruppe T_0 hat alle für T_{11} geforderten Eigenschaften und enthält T_{11} echt. Die Annahme $T_{11}\subsetneqq T_1$ ist falsch, die Behauptung des Lemmas richtig.

Lemma 7.3. *Die Gruppe* $W\times\langle ut\rangle$ *ist in einer Sylow-2-Untergruppe* T *von* G, *die* $S\in\mathrm{Syl}_2(N(A))$ *enthält, normal. Außerdem gilt* $T/T_1\cong E_4$, *wobei* T_1 *der Zentralisator von* $W\times\langle ut\rangle$ *in* T *sein soll.*

Beweis. Aus der Struktur von T_1 ergibt sich, daß T_1 noch nicht Sylow-2-Untergruppe von G ist. Es sei x ein Element aus $N_T(T_1)\setminus T_1$, dessen Quadrat in T_1 liegt, und r sei ein Element aus $N(T_1)$, so daß $\langle rT_1C(T_1), xT_1C(T_1)\rangle$ isomorph zu A_4 ist. Es enthält T damit eine Untergruppe T_0 mit $T_0/T_1\cong E_4$. Alle elementar abelschen Untergruppen der Ordnung 16 von T_1 sind unter T_0 konjugiert. Falls es in $T_0\setminus T_1$ Involutionen gibt, hat der Zentralisator einer Involution aus $T_0\setminus T_1$ mindestens die Ordnung 16. Für eine beliebige Involution c in der Menge $T_0\setminus T_1$ ist jedoch $c^g\neq t$ für alle $g\in G$. Daraus schließen wir, daß T_0 gleich T ist, und sämtliche Behauptungen des Lemmas sind bewiesen.

Lemma 7.4. *Der Fall* $N(A)/C(A)\cong A_4$ *aus* (ii)$_3$ *von Lemma* 2.4 *ist nicht möglich.*

Beweis. Es sei T eine Sylow-2-Untergruppe von G, die A enthält, und $T_1=$ $=C_T(\langle ut\rangle\times W)$. Wir wählen zwei Elemente x und y in $T\setminus T_1$, so daß $T=\langle x, y, T_1\rangle$ ist. Es sei T_2 die abelsche Untergruppe vom Index zwei in T_1. Eine Anwendung des Thompson Transfer Lemmas auf die Involution t und die maximale Untergruppe $\langle T_2, x, y\rangle$ von T liefert den gesuchten Widerspruch.

Lemma 7.5. *Es sei* $N(A)/C(A)$ *isomorph zu* S_4. *Mit* U *bezeichnen wir die zu* A_4 *isomorphe Untergruppe von* $N(A)/C(A)$ *und mit* S_1 *eine Sylow-2-Untergruppe des vollen Urbildes von* U *in* $N(A)$. *Die Sylow-2-Untergruppe* S *von* $N(A)$ *enthalte* S_1. *Dann gilt:* S_1 *besitzt eine zu* E_{32} *isomorphe Untergruppe, in* S *liegt außerhalb von* S_1 *noch genau eine weitere elementar abelsche Untergruppe der Ordnung* 16.

Beweis. Gibt es in $S_1\setminus A$ keine Involutionen, so ist A offensichtlich charakteristisch in S_1. Da $N(A)/C(A)$ isomorph zu S_4 ist, folgt sogar A char S, und die Gruppe S ist schon Sylow-2-Untergruppe von G. Die Involution t kann nicht aus A in $S\setminus A$ konjugiert werden. Man erhält einen Widerspruch zur Einfachheit von G. Es existieren also in $S_1\setminus A$ Involutionen.

Wir nehmen an, daß S_1 keine elementar abelsche Untergruppe der Ordnung 2^5 besitzt. Dann folgt wie in Lemma 7.1 die Existenz einer zu $Z_4\times Z_4\times Z_2$ isomorphen Untergruppe von S_1. Es kann t wiederum nicht aus S_1 in $S\setminus S_1$ herauskonjugiert werden. Es sei x ein Element in $S\setminus S_1$. Unter Zuhilfenahme der Beweise von Lemma 7.2 und 7.3 folgt, daß eine Sylow-2-Untergruppe T von G eine Untergruppe T_T vom Index zwei besitzt, die die gleiche Struktur wie die in Lemma 7.3 mit T bezeichnete Gruppe aufweist und für die gilt: $\langle x, T_T\rangle=T$. Es enthält T_T eine maximale Untergruppe T_M, in die t nicht durch Elemente aus G konjugiert werden kann. Dann läßt sich t aber auch nicht in die maximale Untergruppe $\langle x, T_M\rangle$ von T konjugieren.

Die Gruppe S_1 besitzt also einen elementar abelschen Normalteiler S_E der Ordnung 2^5. Da G nach Voraussetzung einfach sein soll, erzwingt das Thompson

Transfer Lemma die Existenz von Involutionen in $S \setminus S_1$. Außerdem finden wir in S noch genau eine zu E_{16} isomorphe Untergruppe, die mit S_1 den Schnitt acht hat.

Lemma 7.6. *Wir verwenden die Bezeichnungen von Lemma 7.5. Es sei T eine S enthaltende Sylow-2-Untergruppe von G. Dann ist der elementar abelsche Normalteiler S_E der Ordnung 2^5 von S_1 auch normal in T und es gilt: $T/S_E \cong D_{2^r}$ mit $2 \leqq r$.*

Beweis. Mit Hilfe von Lemma 7.5 ergibt sich, daß S_E normal in S liegt und die Faktorgruppe S/S_E isomorph zu D_4 ist.

Wir nehmen an, die Behauptung in Lemma 7.6 sei falsch und wählen eine Untergruppe T_1 von T, die maximal in T ist bezüglich folgender Eigenschaften: (i) $S \subseteqq T_1$, (ii) S_E liegt normal in T_1, (iii) T_1/S_E ist isomorph zu einer Diedergruppe. Es sei T_Z das volle Urbild von $Z(T_1/S_E)$ in T_1. Dann gilt $T_Z = \langle S_E, xt \rangle$, wobei x eine Involution aus $S \setminus S_1$ ist. Ist v ein Element aus $N_T(T_1) \setminus T_1$, dessen Quadrat in T_1 liegt, so sind alle Involutionen aus $T_1 \setminus T_Z$ unter $\langle v, T_1 \rangle$ konjugiert. Wir sehen nun, daß die Gruppe S_E normal in $\langle v, T_1 \rangle$ liegt. Wie früher folgt die Existenz von Involutionen in vT_1, o. B. d. A. sei v selbst eine Involution. Nun gilt $\langle vS_E, tS_E \rangle = \langle v, T_1 \rangle / S_E$, und diese Gruppe ist isomorph zu einer Diedergruppe. Da T_1 echt in $\langle v, T_1 \rangle$ liegt, ergibt sich ein Widersoruch zur maximalen Wahl von T_1. Die Behauptung in Lemma 7.6 ist richtig.

Lemma 7.7. *Der Fall $N(A)/C(A) \cong S_4$ unter Punkt* (ii)$_3$ *von Lemma* 2.4 *ist nicht möglich.*

Beweis. Die Behauptung folgt unter Verwendung der Aussage von Lemma 7.6 unmittelbar aus der Struktur einer Sylow-2-Untergruppe T von G und der Voraussetzung, daß G einfach sein soll.

Lemma 7.8. *Es sei $N(A)/C(A)$ isomorph zu $A_4 \times Z_2$. Mit U bezeichnen wir die zu A_4 isomorphe Untergruppe von $N(A)/C(A)$ und mit S_1 eine Sylow-2-Untergruppe von $U(\text{mod } C(A))_{N(A)}$. Schließlich sei S eine S_1 enthaltende Sylow-2-Untergruppe von $N(A)$. Dann haben die maximalen elementar abelschen Untergruppen von S alle die Ordnung* 16.

Beweis. Wir haben $Z(S_1) = Z(S) = \langle ut \rangle \times W$. Der Zentralisator einer jeden Involution enthält daher eine elementar abelsche Untergruppe der Ordnung 16. Es genügt also zu zeigen, daß S keine zu E_{32} oder E_{64} isomorphe Untergruppen besitzt. Gibt es in S eine elementar abelsche Gruppe S_{E6} der Ordnung 2^6, so liefert [3, Lemma 2, S. 389] einen Widerspruch.

Es sei nun S_{E5} eine elementar abelsche Untergruppe der Ordnung 2^5 in S. Falls S_{E5} nicht in S_1 enthalten ist, hat der Zentralisator einer jeden Involution aus $S \setminus A$ in G eine Untergruppe der Ordnung 2^5. Es ist S dann schon Sylow-2-Untergruppe von G. Man ermittelt wieder eine maximale Untergruppe in S, in die die Involution t nicht durch Elemente aus G konjugiert werden kann.

Wir haben bewiesen, daß S_{E5} schon in S_1 gelegen ist. Offensichtlich wird S_{E5} von ganz S normalisiert, es folgt $S/S_{E5} \cong E_4$. Unter Verwendung der Beweise von Lemma 7.6 und 7.7 folgt erneut ein Widerspruch zur Einfachheit von G. Insgesamt ist die Behauptung in Lemma 7.8 richtig.

Lemma 7.9. *Wir verwenden die Voraussetzungen und Bezeichnungen des letzten Lemmas. Die Sylow-2-Untergruppe S von $N(A)$ besitzt eine zu $Z_4 \times Z_4 \times Z_4$ isomorphe Untergruppe S_Z, so daß in $S \setminus S_Z$ nur Involutionen liegen.*

Beweis. Es seien a, b und c Elemente in $S \setminus A$, die zusammen mit A ganz S erzeugen. Die Gruppe $\langle Z(S), a, b, c \rangle$ enthält t nicht und ist maximal in S. Da G nach Voraussetzung einfach ist, kann S noch keine Sylow-2-Untergruppe von G sein.

In jeder nichttrivialen Nebenklasse von A in S liegen höchstens acht Involutionen, daher gibt es in S höchstens acht elementar abelsche Untergruppen der Ordnung 16. Wir erhalten: $2 \leqq |N(S)/SC(S)|_2 \leqq 2^3$. Liegen in S genau acht elementar abelsche Untergruppen der Ordnung 16, dann zeigt eine ähnlich wie in Lemma 7.1 verlaufende Rechnung sofort, daß S die in der Aussage von Lemma 7.9 angegebene Struktur besitzt.

Wir nehmen nun an, S habe weniger als acht zu E_{16} isomorphe Untergruppen. Dann gilt $|N(S)/SC(S)|_2 \leqq 4$. Es sei zunächst $|N(S)/SC(S)|_2 = 4$. Mit S_1 bezeichnen wir wieder eine in S enthaltene Sylow-2-Untergruppe des vollen Urbildes der zu A_4 isomorphen Untergruppe von $N(A)/C(A)$ in $N(A)$. Es gibt eine Sylow-2-Untergruppe T_1 von $N(S)$, die die maximale Untergruppe S_1 von S normalisiert. Damit erhalten wir: Es gibt in S_1 eine zu $Z_4 \times Z_4 \times Z_2$ isomorphe Untergruppe, außerhalb dieser Untergruppe liegen in S_1 nur Involutionen. Von den vier elementar abelschen Ulntergruppen der Ordnung 16 in S_1 sind die drei von A verschiedenen durch ein Eement der Ordnung drei aus $N(S)/SC(S)$ konjugiert. Ein Element der Ordnung zwei von $N(S)/SC(S)$ operiert ebenfalls nichttrivial auf den vier elementar abelschen Untergruppen der Ordnung 16 in S_1. Daher wird $N(S)/SC(S)$ isomorph zu A_4. Die Anzahl der nicht in S_1 liegenden elementar abelschen Untergruppen der Ordnung 16 von S ist eins oder drei. Im letzteren Falle sind die drei Gruppen durch ein Element aus G konjugiert. Es folgt, daß die Ordnung des Normalisators einer zu E_{16} isomorphen Untergruppe von S, die nicht in S_1 liegt, mindestens von 16 geteilt wird. Die Involution t kann also nicht aus S_1 in $S \setminus S_1$ herauskonjugiert werden. Wie im zweiten Absatz des Beweises von Lemma 7.5 ergibt sich dann, daß eine Sylow-2-Untergruppe T von G eine maximale Untergruppe besitzt, in die man die Involution t aus T nicht durch Elemente von G hineinkonjugieren kann. Dies widerspricht der Einfachheit der Gruppe G.

Es sei nun $|N(S)/SC(S)|_2 = 2$. In diesem Falle ist S_1 in einer Sylow-2-Untergruppe T_1 von $N(S)$ nicht normal. Für ein Element y aus $T_1 \setminus S$ wird $\langle S_1, S_1^y \rangle = S$.

Ist $B=A^y$, so wird $\langle A, B\rangle = D$ isomorph zu $D_8 \times E_4$. Wir wählen zwei Elemente a und b in $S_1 \setminus A$, die zusammen mit A bereits S_1 erzeugen. Dann wird S von D, a und b erzeugt. Außerhalb von D liegen in S drei elementar abelsche Untergruppen der Ordnung 16, die alle in G konjugiert sind, oder aber es gibt keine zu E_{16} isomorphen Untergruppen außerhalb von D in S. Wiederum erhalten wir, daß die Ordnung des Normalisators einer zu E_{16} isomorphen Untergruppe von S, die nicht in D liegt, mindestens von 16 geteilt wird. Die Involution t kann in G nicht aus D in $S \setminus D$ herauskonjugiert werden. Von der Gruppe D ausgehend kann man unter Zuhilfenahme der Beweisverfahren von Paragraph drei wieder mittels Induktion nachweisen, daß eine Sylow-2-Untergruppe T von G eine maximale Untergruppe enthält, in die sich die Involution t nicht durch Elemente aus G konjugieren läßt. Mit Hilfe des Thompson Transfer Lemmas ergibt sich ein Widerspruch zur Einfachheit von G.

Die Annahme, S habe weniger als acht elementar abelsche Untergruppen der Ordnung 16, hat sich als falsch erwiesen. Mit den Ergebnissen zu Beginn des Beweises folgt die Behauptung des Lemmas.

Lemma 7.10. *Es sei T eine Sylow-2-Untergruppe von G. Es liege außerdem wieder der Fall $N(A)/C(A) \cong A_4 \times Z_2$ vor. Dann hat T folgende Struktur:* (i) *T besitzt eine maximale Untergruppe, die isomorph zum direkten Produkt dreier zyklischer Gruppen ist,* (ii) *außerhalb dieser maximalen Untergruppe liegen in T nur Involutionen.*

Beweis. Es sei T so gewählt, daß die Sylow-2-Untergruppe S von $N(A)/C(A)$ in T liegt. Mit T_0 bezeichnen wir eine S enthaltende Untergruppe maximaler Ordnung von T, so daß T_0 eine zum direkten Produkt dreier zyklischer Gruppen isomorphe Untergruppe T_{0Z} vom Index zwei hat und in $T_0 \setminus T_{0Z}$ nur Involutionen liegen. Die Gruppe T_0 besitzt genau acht Konjugiertenklassen von elementar abelschen Untergruppen der Ordnung 16, daher gilt $|N_T(T_0): T_0| \leqq 8$.

Wir nehmen nun an, T_0 liege echt in T. Da T_0 maximal in T gewählt wurde, gibt es in $N_T(T_0)$ außer T_0 selbst keine weitere zu T_0 isomorphe Untergruppe. Es liegt somit T_0 normal mit dem Index zwei, vier oder acht in T.

Es sei zuerst $|T: T_0| = 2$. Gibt es in $T \setminus T_0$ keine Involution, so wählen wir uns ein Element x aus $T \setminus T_0$ und sehen, daß t nicht in die maximale Untergruppe $\langle T_{0Z}, x\rangle$ von T konjugiert werden kann. Existiert in $T \setminus T_0$ eine Involution y, dann kann t nicht in die maximale Untergruppe $\langle T_{0Z}, yt\rangle$ von T konjugiert werden. In beiden Fällen folgt mit Hilfe des Thompson Transfer Lemmas ein Widerspruch zur Einfachheit von G.

Es sei nun $|T: T_0| = 4$. Ist T/T_0 isomorph zu Z_4, dann wählen wir uns ein Element a, das in T modulo T_0 die Ordnung vier hat. Es kann t wiederum nicht in die maximale Untergruppe $\langle T_{0Z}, a\rangle$ von T konjugiert werden. Im Falle $T/T_0 \cong E_4$ können wir nach dem bisher bewiesenen annehmen, daß es Involutionen x und y in $T \setminus T_0$ gibt, so daß T von T_0, x und y erzeugt wird. Es kann t nicht durch Elemente aus G in die maximale Untergruppe $\langle T_{0Z}, xt, yt \rangle$ von T konjugiert werden, wieder ergibt sich ein Widerspruch zur Einfachheit von G.

Schließlich gelte $|T: T_0| = 8$. Ist T/T_0 isomorph zu Z_8, Q_8, D_8 oder $Z_4 \times Z_2$, so folgt aufgrund der bisherigen Ergebnisse dieses Lemmas erneut die Existenz einer maximalen Untergruppe von T, in die die Involution t nicht durch Elemente aus G hineinkonjugiert werden kann. Im Falle $T/T_0 \cong E_8$ können wir annehmen, daß Involutionen x, y und w in $T \setminus T_0$ existieren, die zusammen mit T_0 ganz T erzeugen. Auch in diesem Falle ist t nicht in die maximale Untergruppe $\langle T_{0Z}, xt, yt, wt \rangle$ von T konjugierbar.

Die Annahme, daß T_0 echt in T liegt, hat sich als falsch erwiesen, die Behauptung des Lemmas ist richtig.

Lemma 7.11. *Der Fall* $N(A)/C(A) \cong A_4 \times Z_2$ *tritt nicht auf.*

Beweis. Es sei S eine Sylow-2-Untergruppe von $N(A)$ und T eine S enthaltende Sylow-2-Untergruppe von G. Mit Hilfe von Lemma 7.10 sehen wir, daß T eine maximale Untergruppe enthält, in die t nicht durch Elemente aus G hineinkonjugiert werden kann. Wir erhalten einen endgültigen Widerspruch zur Einfachheit von G.

Literatur

[1] D. Gorenstein, *Finite Groups*, Harper and Row (1968).

[2] D. Gorenstein and K. Harada, A characterization of Janko's two new simple groups, *J. Fac. Science, Univ. Tokyo*, Sec I, **16** (1970), 331—406.

[3] K. Harada, Finite simple groups whose Sylow-2-subgroups are of order 2^7, *J. of Algebra*, **14** (1970), 386—404.

[4] K. Harada, Finite simple groups whose Sylow-2-subgroups are of order 2^8, *unveröffentlicht*.

[5] B. Huppert, *Endliche Gruppen*. I, Springer (1967).

[6] Z. Janko, Some new simple groups of finite order, *Symposia Math. Roma* (1968), 25—64.

[7] A. MacWilliams, On 2-groups with no normal abelian subgroup of rank 3, and their occurrence as Sylow-2-subgroups of finite simple groups, *Trans. Amer. Math. Soc.*, **150** (1970), 345—408.

[8] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, *Bull. Amer. Math. Soc.*, **74** (1968), 383—437.

[9] J. H. Walter, The characterization of finite groups with abelian Sylow-2-subgroups, *Ann. of Math.*, **89** (1969), 405—576.

(Eingegangen am 18. Februar 1974)

Characterization of some related semigroups of universal algebras

By L. SZABÓ in Szeged

§ 1. Introduction

In [3], B. JÓNSSON gave a necessary and sufficient condition for a group of permutations of a set A to be the automorphism group of an (universal) algebra whose base set is A. In [2], G. GRÄTZER characterized those abstract semigroups that are isomorphic to the endomorphism semigroup of some simple algebra. These results are often referred to as the solution of the concrete characterization problem of automorphism groups of algebras and that of the abstract characterization problem of endomorphism semigroups of simple algebras.

In this note we are going to solve the concrete characterization problems of

a) inverse semigroups of partial automorphisms of algebras (Theorem 1), and

b) semigroups of endomorphisms of simple algebras (Theorem 2)

in the above sense*).

Let us consider a set $A (|A| \geqq 2)$, which will be fixed in the sequel. By a 1—1 partial transformation of A we mean a 1—1 mapping from a subset of A into A. The semigroup of all 1—1 partial transformations of A, called in [1] the symmetric inverse semigroup of A, will be denoted by I_A. For any $\varphi \in I_A$ let $D(\varphi)$ be the domain of φ, and $\varphi | B$ the restriction of φ to B, where $B \subseteqq A$.

By the equalizer of any $\varphi, \psi \in I_A$ we mean the set $E(\varphi, \psi)$ defined by

$$E(\varphi, \psi) = \langle a \mid a \in D(\varphi) \cap D(\psi) \text{ and } a\varphi = a\psi \rangle.$$

For any $M \subseteqq I_A$ and $B \subseteqq A$, put

$$\Gamma_M(B) = \bigcap \langle E(\varphi, \psi) \mid \varphi, \psi \in M \text{ and } B \subseteqq E(\varphi, \psi) \rangle.$$

*) *(Added May 23, 1974)* The originally submitted version of the article contained also a solution for the concrete characterization problem of semigroups of 1—1 endomorphisms of algebras. It was omitted as in the meantime the solution of this problem was published by J. JEŽEK in *Coll. Math.*, 29 (1974), 61—69 (Theorem 2).

B. M. SCHEIN kindly informed us that our Theorem 1 was obtained independently also by D. A. BREDIHIN in Saratov.

Then Γ_M is a closure operator and we may speak of a Γ_M-closed subset of A. Note that $D(\varphi)$ is a Γ_M-closed set for any $\varphi \in M$, (indeed, $E(\varphi, \varphi)=D(\varphi)$), and thus $B \subseteqq D(\varphi)$ implies $\Gamma_M(B) \subseteqq D(\varphi)$. Furthermore, if the identity transformation of A belongs to M then $a \in \Gamma_M(\emptyset)$ if and only if $a \in D(\varphi)$ and $a=a\varphi$ for all $\varphi \in M$.

By a partial automorphism of an algebra (A, F) we mean an isomorphism of a subalgebra of (A, F) into (A, F). The empty transformation $0\colon \emptyset \to \emptyset$ is considered to be partial automorphism if and only if (A, F) has no nullary operation. $\mathrm{Aut}_p(A, F)$ denotes the set of all partial automorphisms of (A, F).

We shall often write x instead of $(x_1, \ldots, x_n)$ and, similarly, $x\varphi$ instead of $(x_1\varphi, \ldots, x_n\varphi)$ for any mapping φ. Then, $x^{\urcorner}$ stands for the set of all components of any $x \in A^n$. Finally, $\nu(f)$ denotes the arity of the operation f (i.e., f maps $A^{\nu(f)}$ into A).

§ 2. Results

We start with two simple lemmas.

Lemma 1. *For any algebra (A, F), the semigroup $\mathrm{Aut}_p(A, F)$ is an inverse subsemigroup of I_A. Furthermore, (B, F) $(B \subseteqq A)$ is a subalgebra of (A, F) if and only if B is a $\Gamma_{\mathrm{Aut}_p(A,F)}$-closed set.*

Proof. The first statement is trivial. Suppose that (B, F) is a subalgebra of (A, F). If $B \neq \emptyset$ then let ε be the identity automorphism of (B, F). Clearly, $\varepsilon \in \mathrm{Aut}_p(A, F)$ and $E(\varepsilon, \varepsilon)=B$. Thus $\Gamma_{\mathrm{Aut}_p(A,F)}(B)=B$. If $B=\emptyset$ then (A, F) has no nullary operation, and thus the empty transformation 0 belongs to $\mathrm{Aut}_p(A, F)$. Then $E(0, 0)=\emptyset$, which implies $\Gamma_{\mathrm{Aut}_p(A,F)}(\emptyset)=\emptyset$. The converse follows from the fact that $(E(\varphi, \psi), F)$ is a subalgebra of (A, F) for any $\varphi, \psi \in \mathrm{Aut}_p(A, F)$.

Lemma 2. *Let M be an inverse subsemigroup of I_A; $\varphi \in M$ and $B \subseteqq D(\varphi)$. Then $\Gamma_M(B\varphi)=\Gamma_M(B)\varphi$.*

Proof. From the definition of Γ_M it follows that $u \in \Gamma_M(B)$ $(B \subseteqq A)$ if and only if for any $\sigma, \tau \in M$, $B \subseteqq D(\sigma) \cap D(\tau)$ and $\sigma | B=\tau | B$ implies $u \in D(\sigma) \cap D(\tau)$ and $u\sigma=u\tau$.

If $\sigma | B\varphi=\tau | B\varphi$ $(\sigma, \tau \in M;\ B\varphi \subseteqq D(\sigma) \cap D(\tau))$ then $\varphi\sigma | B=\varphi\tau | B$, and thus $\varphi\sigma | \Gamma_M(B)=\varphi\tau | \Gamma_M(B)$, whence $\sigma | \Gamma_M(B)\varphi=\tau | \Gamma_M(B)\varphi$. Hence, $\Gamma_M(B)\varphi \subseteqq \Gamma_M(B\varphi)$. Write $B\varphi$ and φ^{-1} instead of B and φ, respectively. Then we get $\Gamma_M(B\varphi)\varphi^{-1} \subseteqq$ $\subseteqq \Gamma_M((B\varphi)\varphi^{-1})=\Gamma_M(B)$, which implies $\Gamma_M(B\varphi) \subseteqq \Gamma_M(B)\varphi$, Q.E.D.

For any $M \subseteqq I_A$, we say that $\varphi (\in I_A)$ belongs to M locally if for any finite set $B \subseteqq D(\varphi)$ there is a $\psi \in M$ such that $\varphi | B=\psi | B$.

Theorem 1. *Let M be an inverse subsemigroup of I_A, which contains the identity transformation of A. The following two statements are equivalent:*

I. *There is an algebra (A, F) such that $M = \mathrm{Aut}_p(A, F)$.*

II. (α) *Γ_M is an algebraic closure operation,*

(β) *if for $\varphi \in I_A$, $D(\varphi)$ is a Γ_M-closed set and φ belongs to M locally, then $\varphi \in M$,*

(γ) *all 1—1 partial transformations $\varphi\colon \{a\} \to \{b\}$, for which $\{a\}$ and $\{b\}$ are Γ_M-closed sets, belong to M.*

Proof. I⇒II. According to Lemma 1 we get (α) and (γ) immediately. Suppose that $\varphi \in I_A$ satisfies the condition of (β). Since $D(\varphi)$ is a $\Gamma_{\mathrm{Aut}_p(A,F)}$-closed set, by Lemma 1, we have that $(D(\varphi), F)$ is a subalgebra of (A, F). If $D(\varphi) \neq \emptyset$ (i.e., $\varphi \neq 0$), then let $f \in F$ and $x \in A^{\nu(f)}(x^{\urcorner} \subseteq D(\varphi))$. Then there exists a $\psi \in \mathrm{Aut}_p(A, F)$ which agrees with φ on $x^{\urcorner} \cup \{f(x)\}$. Thus $f(x\varphi) = f(x\psi) = f(x)\psi = f(x)\varphi$, whence $\varphi \in \mathrm{Aut}_p(A, F)$. If $D(\varphi) = \emptyset$ (i.e., $\varphi = 0$), then by Lemma 1 $(\emptyset, F)$ is a subalgebra of (A, F). Therefore, (A, F) has no nullary operation, and thus $0 \in \mathrm{Aut}_p(A, F)$.

II⇒I. We shall construct the desired algebra (A, F). For any $x = (x_1, \dots, x_n) \in A^n$ $(n = 1, 2, \dots)$ and $u \in \Gamma_M(x^{\urcorner})$, let $f_{x,u}\colon A^n \to A$ be defined by

$$f_{x,u}(x\varphi) = u\varphi, \quad \text{for all} \quad \varphi \in M,$$

$$f_{x,u}(y) = y_1, \quad \text{if} \quad y = (y_1, \dots, y_n) \in A^n \setminus xM.$$

From $u \in \Gamma_M(x^{\urcorner})$ it follows that the definition of $f_{x,u}$ is correct. Put $F = \{f_{x,u} \mid x \in A^n;$ $n = 1, 2, \dots$ and $u \in \Gamma_M(x^{\urcorner})\} \cup \Gamma_M(\emptyset)$. (The elements of $\Gamma_M(\emptyset)$ are exactly the nullary operations of (A, F).) We prove that $M = \mathrm{Aut}_p(A, F)$.

Let $\varphi \in M$, $\varphi \neq 0$. First we show that $(D(\varphi), F)$ is subalgebra of (A, F). It is clear that $\Gamma_M(\emptyset) \subseteq D(\varphi)$. Let $f_{x,u} \in F$ and $y \in A^{\nu(f_{x,u})}$, $y^{\urcorner} \subseteq D(\varphi)$. If $y = x\psi$ for some $\psi \in M$, then $f_{x,u}(y) = f_{x,u}(x\psi) = u\psi$. By Lemma 2, $u \in \Gamma_M(x^{\urcorner})$ implies $u\psi \in \Gamma_M(x^{\urcorner}\psi) = \Gamma_M(y^{\urcorner})$. But $y^{\urcorner} \subseteq D(\varphi)$, and thus $u\psi \in \Gamma_M(y^{\urcorner}) \subseteq \Gamma_M(D(\varphi)) = D(\varphi)$. If $y \in A^{\nu(f_{x,u})} \setminus xM$, then $f_{x,u}(y) = y_1 \in D(\varphi)$. Hence, $D(\varphi)$ is closed under $f_{x,u}$. To prove that φ is an isomorphism let $f_{x,u} \in F$ and $y \in A^{\nu(f_{x,u})}$, $y^{\urcorner} \subseteq D(\varphi)$. If y can be written in the form $x\psi$ $(\psi \in M)$, then $f_{x,u}(y\varphi) = f_{x,u}((x\psi)\varphi) = f_{x,u}(x(\psi\varphi)) = u(\psi\varphi) = (u\psi)\varphi = f_{x,u}(x\psi)\varphi = f_{x,u}(y)\varphi$. If $y \in A^{\nu(f_{x,u})} \setminus xM$, then $y\varphi \in A^{\nu(f_{x,u})} \setminus xM$, and thus $f_{x,u}(y\varphi) = y_1\varphi = f_{x,u}(y)\varphi$. It is evident that all elements of $\Gamma_M(\emptyset)$ remain fixed under φ. If the empty transformation belongs to M, then $\Gamma_M(\emptyset) = \emptyset$, i.e., (A, F) has no nullary operation. Thus $0 \in \mathrm{Aut}_p(A, F)$.

Suppose that $\varphi \in I_A$, $\varphi \neq 0$, but $\varphi \notin M$. If $D(\varphi)$ is not a Γ_M-closed set, then $(D(\varphi), F)$ is not a subalgebra of (A, F). To show this statement let $u \in \Gamma_M(D(\varphi))$ and $u \notin D(\varphi)$. Since Γ_M is an algebraic closure operator thus there is a finite set $B \subseteq D(\varphi)$ such that $u \in \Gamma_M(B)$. Arrange the elements of B into a one-to-one sequence x. Then $f_{x,u}(x) = u$ showing that $D(\varphi)$ is not closed under $f_{x,u}$.

If $D(\varphi)$ is a Γ_M-closed set then, by (β), there exists a finite set $B \subseteqq D(\varphi)$ such that no element of M agrees with φ on B. If $|D(\varphi)| \geqq 2$, then we can assume that $|B| \geqq 2$. Arrange the elements of B into a one-to-one sequence x. Then $f_{x,x_2}(x\varphi) = x_1\varphi \neq x_2\varphi = f_{x,x_2}(x)\varphi$. If $|D(\varphi)|=1$, i.e., $\varphi\colon \{a\} \to \{b\}$ for some $a, b \in A$, then by (γ), $\{b\}$ is not a Γ_M-closed set. Thus there is a $u \in \Gamma_M(\{b\})$ such that $u \neq b$. Furthermore, a cannot be written in the form $a = b\psi$ ($\psi \in M$) as, by Lemma 2, from $a = b\psi$ we get $\Gamma_M(\{b\}) = \Gamma_M(\{a\}\psi^{-1}) = \Gamma_M(\{a\})\psi^{-1} = \{a\}\psi^{-1} = \{b\}$, which is a contradiction. Thus $f_{b,u}(a\varphi) = f_{b,u}(b) = u \neq b = a\varphi = f_{b,u}(a)\varphi$.

If $0 \notin M$ then, by (β), $\Gamma_M(\emptyset) \neq \emptyset$, i.e., (A, F) has nullary operation. Thus $0 \notin \mathrm{Aut}_p(A, F)$. Q.E.D.

For any $M \subseteqq I_A$, the inverse subsemigroup of I_A generated by M is denoted by $\tilde{M}$. Further, for any transformation semigroup S of A, the images of the constant transformations of S will be referred to as the constants of S.

Theorem 2. *For any transformation monoid S of A, the following two statements are equivalent:*

I. *There exists a simple algebra (A, F) such that $S = \mathrm{End}\,(A, F)$.*

II. (α) *$S = M \cup C$, where M contains only 1—1 and C contains only constant transformations,*

(β) *if a 1—1 transformation φ of A belongs to $\tilde{M}$ locally, then $\varphi \in M$,*

(γ) *the set of all constants of S is closed under any $\varphi \in \tilde{M}$,*

(δ) *all $a \in A$ such that $\{a\}$ is a Γ_M-closed set are constants of S.*

Proof. I$\Rightarrow$II. (α) is trivial, (β) follows from Theorem 1, (γ) is valid because the product of homomorphisms is also a homomorphism, and (δ) follows from the fact that $(\{a\}, F)$ is a subalgebra of (A, F) whenever $\{a\}$ is a $\Gamma_{\tilde{M}}$-closed subset in A.

II$\Rightarrow$I. We construct the desired algebra (A, F). For any $x = (x_1, \ldots, x_n) \in A^n$ ($n = 2, 3, \ldots$) let $f_x\colon A^n \to A$ be defined by

$$f_x(x\varphi) = x_2\varphi, \quad \text{for all} \quad \varphi \in \tilde{M},$$

$$f_x(y) = y_1, \quad \text{if} \quad y = (y_1, \ldots, y_n) \in A^n \setminus x\tilde{M}.$$

Furthermore, for any $a \in A$ such that a is not a constant of S and $u \in \Gamma_{\tilde{M}}(\{a\})$, let $h_{a,u}\colon A \to A$ be defined by

$$h_{a,u}(a\varphi) = u\varphi, \quad \text{for all } \varphi \in \tilde{M}$$

$$h_{a,u}(x) = x, \quad \text{if} \quad x \in A \setminus a\tilde{M}.$$

Let F be the set of all operations of form f_x as well as $h_{a,u}$. We shall prove that $S = \mathrm{End}\,(A, F)$ and (A, F) is a simple algebra.

Let $\varphi \in S$. If $\varphi \in M$, then to prove that φ commutes with all operations of F we may proceed similarly as we put it in the proof of Theorem 1. If $\varphi \in C$, i.e., $\varphi: A \to \{d\}$ $(d \in A)$, then φ commutes with any $f_x \in F$ because f_x is an idempotent operation. Let $h_{a,u} \in F$ and $x \in A$. Then $d \in A \setminus a\tilde{M}$ because from $a\psi = d (\psi \in \tilde{M})$ we get $a = d\psi^{-1}$ and, by (γ), this implies that a is a constant of S, which is a contradiction. Thus $h_{a,u}(x\varphi) = h_{a,u}(d) = d = h_{a,u}(x)\varphi$.

Let φ be a transformation of A and $\varphi \notin S$. If φ is one-to-one then, by (β), for some $n (\geqq 2)$ there exists an $x \in A^n$ such that $x\varphi \in A^n \setminus x\tilde{M}$. Thus $f_x(x\varphi) = x_1\varphi \neq$ $\neq x_2\varphi = f_x(x)\varphi$. If φ is a constant transformation, i.e., $\varphi: A \to \{d\}$ $(d \in A)$, then d is not a constant of S, and thus, by (δ), we have $\Gamma_{\tilde{M}}(\{d\}) \neq \{d\}$. Therefore, for a suitable $u \in \Gamma_{\tilde{M}}(\{d\})$ we get $u \neq d$. Then $h_{d,u}(d\varphi) = h_{d,u}(d) = u \neq d = h_{d,u}(d)\varphi$. If φ is neither 1—1 nor a constant transformation, then there are x_1, x_2, x_3 and x_4 in A with $x_3 \neq x_4$ such that $x_1\varphi \neq x_2\varphi$ and $x_3\varphi = x_4\varphi$. Put $x = (x_1, x_2, x_3, x_4)$. It is clear that $x\varphi \in A^4 \setminus x\tilde{M}$, and thus $f_x(x\varphi) = x_1\varphi \neq x_2\varphi = f_x(x)\varphi$.

Now we have to prove only that (A, F) is simple algebra. Let Θ be a congruence relation of (A, F), and suppose that $a \equiv b(\Theta)$ for some $a, b \in A$, $a \neq b$. We claim that $c \equiv d(\Theta)$ for all $c, d \in A$. Put $x = (c, d, a, a)$ and $y = (c, d, a, b)$. Since a and b are distinct thus, $y \in A^4 \setminus x\tilde{M}$, whence $d = f_x(x) \equiv f_x(y) = c(\Theta)$ follows. Q.E.D.

Remark. It can be shown without any difficulty that none of the conditions (α), (β) and (γ) in Theorem 1 is implied by the two others; a similar statement is valid for the conditions (β), (γ) and (δ) in Theorem 3.

References

[1] A. H. CLIFFORD and G. B. PRESTON, *The algebraic theory of semigroups*, Vol. I, AMS (Providence, 1961).

[2] G. GRÄTZER, On the endomorphism semigroup of simple algebras, *Math. Ann.*, **170** (1967), 334—338.

[3] B. JÓNSSON, Algebraic structures with prescribed automorphism groups, *Coll. Math.*, **19** (1968), 1—4.

[4] E. PLONKA, A problem of B. Jónsson concerning automorphisms of a general algebra, *Coll. Math.*, **19** (1968), 5—8.

(Received March 9, 1974)

Derivations of lattices

By G. SZÁSZ in Budapest

1. Introduction. A mapping $a \to a'$ of a ring R into itself is called a *derivation* of R if the equations

$$(a+b)' = a'+b', \quad (ab)' = a'b+ab'$$

hold for any pair a, b of R. As a generalization of this definition it offers itself the following one: A mapping $a \to a'$ of an algebra A with two (arbitrary) binary operations $+$, $\cdot$ into itself is called a derivation of A if (1) and (2) are true for any elements a, b of A.

In this note we investigate the derivations of lattices with the aid of our earlier results in [2] concerning translations of lattices. For the concepts not defined here see [1] or [3].

2. Preliminaries. According to what have been said in the introduction we introduce the following

Definition 1. A single-valued mapping φ of a lattice L into itself is called a *derivation* of L if

(1) $$\varphi(x \smile y) = \varphi(x) \smile \varphi(y) \quad \text{and} \quad \varphi(x \frown y) = (\varphi(x) \frown y) \smile (x \frown \varphi(y))$$

for every pair of elements x, y of L.

Examples:

1. In every lattice L, the identity mapping ι defined by $\iota(x) = x$ for each $x \in L$ is a derivation of L.

2. Let L be a lattice with least element o. Then the mapping ω defined by $\omega(x) = o$ for each $x \in L$ is a derivation of L.

3. To every neutral element n of a lattice L there corresponds a derivation generated by n, namely the mapping φ_n defined by $\varphi_n(x) = n \frown x$ for each $x \in L$.

In [2] we defined the translations of a lattice and established their basic properties. In studying the derivations we shall need the dual concept. Therefore we distinguish now join-translations and meet-translations as follows:

Definition 2. A single-valued mapping λ of a lattice L into itself is called a *join-translation* if

$$\lambda(x \smile y) = \lambda(x) \smile y \tag{2}$$

and a *meet-translation* if

$$\lambda(x \frown y) = \lambda(x) \frown y \tag{3}$$

for each pair of elements x, y of L.

It was shown in [2] that the only mapping of L into itself which is a join-translation as well as a meet-translation is the identity mapping of L.

For sake of completeness of this note we formulate all those results of [2] that will be applied here.

Proposition 1. *Every meet-translation of a lattice L is an idempotent meet-endomorphism* (that is, a meet-endomorphism λ for which $\lambda(\lambda(x)) = \lambda(x)$ identically).

Proposition 2. *The fixed elements of a meet-translation λ of a lattice L form an ideal I_λ of L and, for any two meet-translations λ_1, λ_2 of L, $\lambda_1 \neq \lambda_2$ implies $I_{\lambda_1} \neq I_{\lambda_2}$.*

Proposition 3. *Any two meet-translations of a lattice are permutable.*

Proposition 4. *A lattice L is distributive if and only if every meet-translation of L is (not only a meet-endomorphism, but) an endomorphism of L.*

3. Relations between the class of derivations and other classes of lattice mappings. Every derivation of a lattice L is a join-endomorphism of L, by definition; we show that it is a meet-endomorphism, too, by proving the

Theorem 1. *Every derivation of a lattice L is a meet-translation of L.*

Corollary 1. *Every derivation of a lattice L is an idempotent endomorphism of L.*

Corollary 2. *The fixed elements of a derivation of a lattice L form an ideal of L and the ideal of fixed elements determines uniquely the derivation in question.*

We reach to Theorem 1 by proving the following lemmas concerning any derivation φ of a lattice L:

Lemma 1. *$\varphi(x) \leqq x$ for any element x of L.*

Lemma 2. *$x \leqq y$ implies $\varphi(x) \leqq \varphi(y)$ $(x, y \in L)$.*

Lemma 3. *$x \leqq y$ implies $\varphi(x) = x \frown \varphi(y)$ $(x, y \in L)$.*

Proof. We have by (1)

$$\varphi(x) = \varphi(x \frown x) = (\varphi(x) \frown x) \smile (x \frown \varphi(x)),$$

i.e. $\varphi(x) = \varphi(x) \frown x$ for any element x of L which is equivalent to the assertion of Lemma 1.

If $x \leqq y$, then (1) implies

$$\varphi(y) = \varphi(x \smile y) = \varphi(x) \smile \varphi(y),$$

i.e. $\varphi(x) \leqq \varphi(y)$, as asserted in Lemma 2.

Let $x \leqq y$ again. Then $\varphi(x) \leqq x \leqq y$ by Lemma 1. Consequently

$$\varphi(x) = \varphi(x \frown y) = (\varphi(x) \frown y) \smile (x \frown \varphi(y)) = \varphi(x) \smile (x \frown \varphi(y)),$$

i.e. $x \frown \varphi(y) \leqq \varphi(x)$. On the other hand, $\varphi(x) \leqq x$ by Lemma 1 and $\varphi(x) \leqq \varphi(y)$ by Lemma 2. Therefore

$$x \frown \varphi(y) \geqq \varphi(x),$$

too, completing the proof of Lemma 3.

Applying Lemma 3 to the case $x = u \frown v$, $y = u$ we get

$$\varphi(u \frown v) = u \frown v \frown \varphi(u) = \varphi(u) \frown v$$

for any elements u, v of L (since $u \frown \varphi(u) = \varphi(u)$ by Lemma 1). Thus every derivation of L identically satisfies (3) and therefore it is a meet-translation of L, indeed.

Corollary 1 follows from Definition 1 and Proposition 1. Corollary 2 follows from Proposition 2. Thus Theorem 1 and the corollaries following it have been proved.

As a simple consequence of Lemma 3 we have also the

Corollary 3. *Every derivation φ of a lattice L is of the form*

$$\varphi(x) = c \frown x \tag{4}$$

with a suitably chosen $c \in L$ if and only if L has a greatest element.

Proof. If i is the greatest element of L, then $\varphi(x) = x \frown \varphi(i)$ for each $x \in L$, by Lemma 3. If, however, L has no greatest element, then the identity mapping of L cannot be represented in the form (4), because $c \frown x \neq x$ for $x > c$.

It is easy to see that *the class of all derivations of a lattice L at least of two elements is a proper subclass of all endomorphisms of L.* In fact, given an element c different from the least element (eventually existing) of L, the mapping $\gamma(x)$ define by

$$\gamma(x) = c \quad \text{for each} \quad x \in L$$

is an endomorphism of L which is no derivation because there exists at least one element d in L such that $c>d$ and thus $\gamma(d)>d$. Hence Lemma 1 does not hold for this mapping γ.

Now we are going to give a fuller characterization of the derivations among the meet-translations and the endomorphisms.

Theorem 2. *Let D, T, J, E denote the set of all derivations, meet-translations, join-endomorphisms and endomorphisms, respectively, of a lattice L. Then*

$$D = T \cap J = T \cap E.$$

In other words, a meet-translation of a lattice is a derivation if and only if it is a join-endomorphism (or equivalently, an endomorphism) of that lattice.

Corollary 4. *Let I be an ideal of the lattice L and φ an endomorphism of L onto I such that $\varphi(x)=x$ for each $x \in I$. Then φ is a derivation of L.*

Corollary 5. *A lattice is distributive if and only if $D=T$.*

Proof. $D \subseteqq T$ by Theorem 1 and $D \subseteqq J$ by Definition 1. Therefore $D \subseteqq T \cap J$.

On the other hand, the second *equation* (1) *is identically satisfied by any meet-translation of a lattice.* For, if φ is a meet-translation of the lattice L, then

$$\varphi(x \frown y) = \varphi(x) \frown y \quad \text{and} \quad \varphi(x \frown y) = \varphi(y \frown x) = \varphi(y) \frown x = x \frown \varphi(y)$$

for any elements x, y of L whence the second equation (1) trivially follows. This means that any mapping $\varphi \in T \cap J$ satisfies (1). Consequently, $T \cap J \subseteqq D$. Thus the equation $D = T \cap J$ has been verified.

Let M denote the set of all meet-endomorphisms of L. Then, by Proposition 1, $T = T \cap M$. Hence $T \cap J = T \cap M \cap E = T \cap E$, completing the proof of Theorem 2.

Now, let φ be an endomorphism of L that satisfies the conditions in Corollary 4. Since I is, a fortiori, an ideal of the meet-semilattice $L^{\frown}$ of L, the mapping φ is a translation of $L^{\frown}$ by Theorem 2 of [3]. Hence, φ is (not only an endomorphism but) a meet-translation of L.

Corollary 5 is an immediate consequence of Theorem 2 and Proposition 4.

Remark. One can derive also immediately from Lemma 3 that every derivation is idempotent (by taking $x=\varphi(t)$ and $y=t$) and that the fixed elements form an ideal (by taking $x \leqq y = \varphi(y)$).

4. Basic properties of the multiplication of derivations. By the product $\varrho\sigma$ of two mappings ϱ and σ of a set S into itself we mean, as usual, the mapping π defined by $\pi(x) = \varrho(\sigma(x))$ $(x \in S)$.

Theorem 3. *The set of all derivations of a given lattice forms a commutative sermigoup with respect to the multiplication of mappings.*

Proof. It is well-known that the multiplication of mappings is associative. Furthermore, any two derivations of a lattice are permutable by Theorem 1 and Proposition 3. Thus we have only to show that the product of any two derivations of a lattice is again a derivation of that lattice.

Let φ and ψ be arbitrary derivations, x and y arbitrary elements of a lattice L. Then, by the first equation (1) we have

$$\varphi\psi(x\smile y) = \varphi(\psi(x)\smile\psi(y)) = \varphi\psi(x)\smile\varphi\psi(y),$$

that is, $\varphi\psi$ is a join-endomorphism of L. Moreover, by both equations (1) we get

$$\varphi\psi(x\frown y) = \varphi((\psi(x)\frown y)\smile(x\frown\psi(y))) = \varphi(\psi(x)\frown y)\smile\varphi(x\frown\psi(y)),$$

whence, by the second equation (1),

(5) $$\varphi\psi(x\frown y) = (\varphi\psi(x)\frown y)\smile(\psi(x)\frown\varphi(y))\smile(\varphi(x)\frown\psi(y))\smile(x\frown\varphi\psi(y)).$$

In order to prove the theorem we have to show that the right-hand side of (5) reduces to

$$(\varphi\psi(x)\frown y)\smile(x\frown\varphi\psi(y)).$$

We shall achieve this purpose by verifying the inequalities

(6) $$\psi(x)\frown\varphi(y) \leqq x\frown\varphi\psi(y),$$

(7) $$\varphi(x)\frown\psi(y) \leqq \varphi\psi(x)\frown y.$$

By Corollary 1, φ and ψ are endomorphisms of L. Therefore

$$\varphi\psi(x\frown y) = \varphi\psi(x)\frown\varphi\psi(y).$$

Combining this equation with (5) we see that

(8) $$\psi(x)\frown\varphi(y) \leqq \varphi\psi(x)\frown\varphi\psi(y).$$

Since $\varphi\psi(x)\leqq\psi(x)\leqq x$ by Lemma 1, (8) implies (6). Inequality (7) can be derived similarly.

5. On the fixed ideal and the kernel of a derivation. By Theorem 1 and Proposition 2, the fixed elements of a derivation φ (that is, the elements x such that $\varphi(x)=x$) of a lattice L form an ideal of L. This ideal will be called the *fixed ideal* of φ and denoted by $\mathrm{Fix}\,\varphi$.

Let L be a lattice with least element o. Then, by the *kernel* of φ we mean the set of all elements x of L such that $\varphi(x)=o$. The kernel of φ will be denoted by $\mathrm{Ker}\,\varphi$.

We make some comments on the relations between the fixed ideal and the kernel of a derivation φ of a lattice L with least element o.

Remark 1. $\mathrm{Fix}\,\varphi\cap\mathrm{Ker}\,\varphi=\{o\}$.

Remark 2. Fix $\varphi=\{o\}$ implies Ker $\varphi=L$.

Remark 3. If L has at least two elements, then Ker $\varphi=\{o\}$ implies Fix $\varphi\supset\{o\}$.

Remark 4. There exist lattices L with least element o such that Ker $\varphi\supset\{o\}$ and Fix $\varphi\supset\{o\}$.

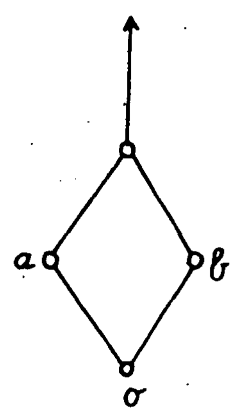
Proof.

1. If $x\in$ Fix $\varphi\cap$ Ker φ, then $x=\varphi(x)=o$.

2. By Corollary 1, $\varphi(x)\in$ Fix φ for each $x\in L$. Thus, Fix $\varphi=\{o\}$ implies that $\varphi(x)=o$ for each $x\in L$.

3. If L has at least two elements, then there exists an element $c\in L$ such that $c\neq o$. Suppose Ker $\varphi=\{o\}$. Then $\varphi(c)\neq o$ and $\varphi(c)\in$ Fix φ, by Corollary 1.

4. Consider the lattice of the diagram below where the arrow directed upward denotes an arbitrary chain (with or without a greatest element). Then the mapping



defined by $\varphi(x)=a\frown x$ is a derivation of the lattice for which Fix $\varphi=(a]$ and Ker $\varphi=(b]$.

References

[1] G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Coll. Publ. **25**, third edition (New York, 1967).
[2] K. Iséki, On endomorphism with fixed element on algebra, *Proc. Japan Acad.*, **40** (1964), 403.
[3] G. Szász, Die Translationen der Halbverbände, *Acta Sci. Math.*, **17** (1956), 165—169.
[4] G. Szász, Translationen der Verbände, *Acta Fac. Rer. Nat. Univ. Comenianae*, **5** (1961), 53—57.
[5]. G. Szász, *Introduction to lattice theory* (Budapest, 1963).

(Received July 19, revised September 13, 1974)

An application of dilation theory to hyponormal operators

By BÉLA SZ.-NAGY in Szeged and CIPRIAN FOIAŞ in Bucharest

Dedicated to our friend Professor K. Tandori on his 50th anniversary

Among the classes of operators extending the class of *normal* operators one of the most interesting is the class of *hyponormal* operators, i.e. operators H such that

(1) $$H^*H \geqq HH^*$$

(see [1], § 160). The aim of this Note is to exhibit a connection between these two classes, by applying the theory of isometric dilations of contractions (see [2], Chapter II). We shall prove namely the following

Theorem. *For every hyponormal operator H on a Hilbert space $\mathfrak{H}$ there exist a normal operator N and a unitary operator U on some Hilbert space $\mathfrak{G}$, and a contraction X of $\mathfrak{H}$ into $\mathfrak{G}$, such that*

(a) $H = X^*NX$,

(b) $\|N\| = \|H\|$,

(c) $NU = UN = N^*$,

(d) $\|X^*Ug\| \leqq \|X^*g\|$ *for all* $g \in \mathfrak{G}$,

(e) *the manifolds* $\mathfrak{L}_n = U^n X\mathfrak{H}$ $(n = 0, 1, \ldots)$ *form a non-decreasing sequence and span* $\mathfrak{G}$,

(f) *for any complex scalars* α, β,

$$\sigma(\alpha N + \beta N^*) \subset \sigma_l(\alpha H + \beta H^*) \quad (\sigma_l\text{: “left spectrum”}).$$

Remark. This theorem has a rather trivial converse. Indeed, suppose H is any operator on $\mathfrak{H}$ which derives from operators N, U on a space $\mathfrak{G}$ and from a contraction $X: \mathfrak{H} \to \mathfrak{G}$ in such a way that conditions (a), (c) and (d) hold. Then H is hyponormal. Indeed, we have for $h \in \mathfrak{H}$

$$\|H^*h\| \overset{a}{=} \|X^*N^*Xh\| \overset{c}{=} \|X^*UNXh\| \overset{d}{\leqq} \|X^*NXh\| \overset{a}{=} \|Hh\|,$$

and the inequality $\|H^*h\| \leqq \|Hh\|$ for all $h \in \mathfrak{H}$ is equivalent to (1).

1. From the assumption that H is a hyponormal operator on $\mathfrak{H}$ it immediately follows that there exists a contraction T on $\mathfrak{H}$ such that

(2) $$H^* = TH;$$

T is uniquely determined by H if we require that it be 0 on the orthogonal complement of the range of H.

From (2) we deduce $H=(TH)^*=H^*T^*=THT^*$, and hence,

(3) $$H = T^n H T^{*n} \quad (n = 0, 1, \ldots).$$

Let V be the minimal isometric dilation of the contraction T, acting on a Hilbert space $\mathfrak{K}(\supset \mathfrak{H})$. Then we have

(4) $$T^n P_{\mathfrak{H}} = P_{\mathfrak{H}} V^n \quad (n = 0, 1, \ldots),$$

where $P_{\mathfrak{H}}$ denotes orthogonal projection from $\mathfrak{K}$ onto $\mathfrak{H}$. The minimality property means that

(5) $$\mathfrak{K} = \bigvee_{n \geqq 0} V^n \mathfrak{H}.$$

It is well-known that the subspace

(6) $$\mathfrak{G} = \bigcap_{n \geqq 0} V^n \mathfrak{K}$$

reduces V to its *unitary* part

(7) $$U = V|\mathfrak{G}.$$

Denote by $P_{\mathfrak{G}}$ the orthogonal projection $\mathfrak{K} \to \mathfrak{G}$. Since $P_{\mathfrak{G}}$ commutes with V we infer from (5) and (7) that

(8) $$\mathfrak{G} = P_{\mathfrak{G}} \mathfrak{K} = \bigvee_{n \geqq 0} P_{\mathfrak{G}} V^n \mathfrak{H} = \bigvee_{n \geqq 0} U^n X \mathfrak{H},$$

where we set

(9) $$X = P_{\mathfrak{G}} | \mathfrak{H}.$$

Now the following representation is valid for X (see [2] Chapter III):

(10) $$X = \lim_{n \to \infty} V^n T^{*n},$$

whence

(11) $$V^m X T^{*m} = X \quad (m = 0, 1, \ldots).$$

This implies that the linear manifolds

(12) $$\mathfrak{L}_n = V^n X \mathfrak{H} = U^n X \mathfrak{H} \quad (n = 0, 1, \ldots)$$

form a non-decreasing sequence; their union

$$\mathfrak{L} = \bigcup_{n \geqq 0} \mathfrak{L}_n$$

is, on account of (8), dense in $\mathfrak{G}$.

2. Next we prove that the (strong) limit

$$X_H = \lim_{n\to\infty} V^n H T^{*n} \tag{13}$$

also exists. Indeed, from (3) and (4) we deduce, for $n \geqq m \geqq 0$ and $h \in \mathfrak{H}$:

$$(V^n HT^{*n}h, V^m HT^{*m}h) = (V^{n-m}HT^{*n}h, HT^{*m}h) = (T^{n-m}HT^{*n}h, HT^{*m}h) =$$
$$= (T^{n-m}HT^{*n-m}T^{*m}h, HT^{*m}h) = (HT^{*m}h, HT^{*m}h),$$

and hence,

$$\|V^n HT^{*n}h - V^m HT^{*m}h\|^2 = \|HT^{*n}h\|^2 - \|HT^{*m}h\|^2;$$

the assertion follows if we observe that the sequence $\|HT^{*n}h\|$ $(n=0, 1, \ldots)$ is convergent. This sequence is namely bounded by $\|H\|\cdot\|h\|$, and non-decreasing by the above relation.

In analogy to (11) we obtain from (13)

$$V^m X_H T^{*m} = X_H \quad (m = 0, 1, \ldots). \tag{14}$$

Note that (14) implies, in particular,

$$X_H \mathfrak{H} \subset V^m X_H \mathfrak{H} \subset V^m \mathfrak{K} \quad (m = 0, 1, \ldots)$$

and therefore,

$$X_H \mathfrak{H} \subset \mathfrak{G}. \tag{15}$$

3. Now we are ready to define the operator N. Let $U^{n_i}Xh_i$ $(i=1, \ldots, s)$ be elements of the linear manifold $\mathfrak{L}$ and form the sums

$$\varphi = \sum_i U^{n_i}Xh_i \quad \text{and} \quad \varphi_H = \sum_i U^{n_i}X_H h_i \quad (\in \mathfrak{G}, \text{ by } (15)).$$

Use (10) and (14) to obtain

$$\varphi = \lim_{r\to\infty} \sum_i V^{n_i}V^{r-n_i}T^{*r-n_i}h_i = \lim_{r\to\infty} V^r \sum_i T^{*r-n_i}h_i$$

and

$$\varphi_H = \lim_{r\to\infty} \sum_i V^{n_i}V^{r-n_i}HT^{*r-n_i}h_i = \lim_{r\to\infty} V^r H \sum_i T^{*r-n_i}h_i.$$

Hence we infer

$$\|\varphi_H\| \leqq \|H\|\cdot\|\varphi\|.$$

Because $\mathfrak{L}$ is dense in $\mathfrak{G}$ we conclude that there is an operator N on $\mathfrak{G}$, uniquely determined by the conditions

$$N\colon U^n Xh \to U^n X_H h \quad (h \in \mathfrak{H};\ n = 0, 1, \ldots), \tag{16}$$

and we have

$$\|N\| \leqq \|H\|. \tag{17}$$

As $NU\cdot U^nXh = NU^{n+1}Xh = U^{n+1}X_Hh = U\cdot NU^nXh$, we have

$$NU = UN. \tag{18}$$

Moreover, using (3) we obtain for $h, h' \in \mathfrak{H}$; $s=0, 1, \ldots$, and $n=0, 1, \ldots$:

$$(Hh, T^{*s}h') = (T^n HT^{*n}h, T^{*s}h') = (HT^{*n}h, T^{*s+n}h') =$$
$$= (V^s V^n HT^{*n}h, V^{s+n}T^{*s+n}h');$$

letting $n \to \infty$ this implies

$$(T^s Hh, h') = (U^s X_H h, Xh') \quad (h, h' \in \mathfrak{H};\ s = 0, 1, \ldots). \tag{19}$$

Consider any two elements of $\mathfrak{L}$; we may assume that both are in the same manifold $\mathfrak{L}_n$, thus can be written as

$$g = U^n Xh, \quad g' = U^n Xh'.$$

Using (2), (16) and (19) (for $s=1$, $s=0$) we get

$$(NUg, g') = (NU^{n+1}Xh, U^n Xh') = (U^{n+1}X_H h, U^n Xh') = (UX_H h, Xh') = (THh, h') =$$
$$= (H^*h, h') = (h, Hh') = (Xh, X_H h') = (U^n Xh, U^n X_H h') = (g, Ng').$$

This proves that

$$N^* = NU. \tag{20}$$

Relations (18) and (20) imply in particular that N is *normal.*

Again from (16), (19) ($s=0$) we deduce

$$(Hh, h') = (X_H h, Xh') = (NXh, Xh') = (X^* NXh, h');$$

whence,

$$H = X^* NX. \tag{21}$$

From the definition (9) of X we readily obtain that

$$X^* = P_{\mathfrak{H}}|\mathfrak{G}. \tag{22}$$

As both X and X^* are *contractions*, a comparison of (17) with (21) yields:

$$\|N\| = \|H\|. \tag{23}$$

Next observe that (4) implies $\|P_{\mathfrak{H}} Vg\| = \|TP_{\mathfrak{H}}g\| \leqq \|P_{\mathfrak{H}}g\|$ for all $g \in \mathfrak{K}$, and in particular for $g \in \mathfrak{G}$, so we have by (22)

$$\|X^*Ug\| \leqq \|X^*g\| \quad \text{for} \quad g \in \mathfrak{G}. \tag{24}$$

4. On account of the definitions (16) and (13) we have

$$NXh = \lim_{n\to\infty} V^n HT^{*n}h \quad (h \in \mathfrak{H}).$$

Hence, using (18), (20), and (2), we deduce

$$N^*Xh = UNXh = \lim_{n\to\infty} V^{n+1}HT^{*n}h = \lim_{n\to\infty} V^{n+1}(H^*T^*)T^{*n}h =$$
$$= \lim_{n\to\infty} V^{n+1}H^*T^{*n+1}h.$$

If we also recall (10) we conclude that for any complex scalars α, β, λ:

(25) $$(\alpha N+\beta N^*-\lambda I)Xh = \lim_{n\to\infty} V^n(\alpha H+\beta H^*-\lambda I)T^{*n}h.$$

Hence, setting $N_{\alpha\beta}=\alpha N+\beta N^*$ and $H_{\alpha\beta}=\alpha H+\beta H^*$, we have

(26) $$\|(N_{\alpha\beta}-\lambda I)Xh\| = \lim_{n\to\infty} \|(H_{\alpha\beta}-\lambda I)T^{*n}h\|.$$

Suppose λ is a point of "regular type" for $H_{\alpha\beta}$, i.e. that the inequality

(27) $$\|(H_{\alpha\beta}-\lambda I)h\| \geqq \varepsilon\|h\|$$

holds for some $\varepsilon>0$ and for all $h\in\mathfrak{H}$. Then by (26) and (10) we have

$$\|(N_{\alpha\beta}-\lambda I)Xh\| \geqq \varepsilon\cdot\lim_{n\to\infty}\|T^{*n}h\| = \varepsilon\cdot\|Xh\|,$$

and as U commutes with N and N^* we have

$$\|(N_{\alpha\beta}-\lambda I)U^nXh\| \geqq \varepsilon\|U^nXh\| \quad (h\in\mathfrak{H};\ n=0, 1, \ldots)$$

as well. As the manifolds $\mathfrak{L}_n$ are nested and span $\mathfrak{G}$ we conclude that

(28) $$\|(N_{\alpha\beta}-\lambda I)g\| \geqq \varepsilon\|g\| \quad \text{for all} \quad g\in\mathfrak{G}.$$

This implies that λ is in the resolvent set of the (normal) operator $N_{\alpha\beta}$.

Passing to the complement of the set of the above points λ we conclude that

$$\sigma(N_{\alpha\beta})\subset\sigma_l(H_{\alpha\beta}).$$

The proof of the Theorem is complete.

References

[1] P. R. Halmos, *A Hilbert Space Problem Book*, Van Nostrand (Princeton—Toronto—London, 1967).

[2] B. Sz.-Nagy—C. Foiaş, *Harmonic Analysis of Operators on Hilbert Space*, Akadémiai Kiadó — North Holland (Budapest—Amsterdam, 1970).

(Received October 1, 1974)

A generalization of Gaschütz's theorem of sylowizers

By G. ZAPPA in Florence and J. SZÉP in Budapest

Let G be a finite group and R a p-subgroup of G. The subgroup S of G is a sylowizer of R if R is a Sylow p-group in S and S is maximal with this property (in G) [1]. GASCHÜTZ has given two sufficient conditions such that all sylowizers of R in G are conjugate. ISAACS has given an example where the sylowizers of a p-group R in a finite group G are not conjugate, that is, the conjugacy of the sylowizers of R is not true in general. In the first result GASCHÜTZ proves that if G is a solvable (finite) group, P is a Sylow p-group of G and $R \lhd P$, then all sylowizers of R in G are conjugate. As it is well known if G is a finite solvable group then the sylowizer of R has the factorization RC where $(|R|, |C|)=1$, that is, C is a complement of R in the sylowizer. In this note we give a generalization of the theory of GASCHÜTZ.

1. Let G be a finite group. Π the set of all prime divisors of $|G|$, $\pi \subset \Pi$, $\pi' = \Pi \setminus \pi$. We say that G satisfies the condition $D_{\pi'}$ of HALL if G has a Hall π'-subgroup H and every π'-subgroup of G is contained in a conjugate of H.

A relation ϱ defined on the set of the subgroups of G is said to be a *T-relation* if 1) $R \varrho C$ implies that R is a π-subgroup and C is a π'-subgroup; 2) $R \varrho \{1\}$ for every π-subgroup R; 3) if $\langle C_1, C_2 \rangle$ is a π'-subgroup then $R\varrho G$, $R \varrho C_2$ imply $R \varrho \langle C_1, C_2 \rangle$; 4) $R \varrho C$ and $a \in G$ imply $(a^{-1}Ra)\varrho(a^{-1}Ca)$.

Furthermore, let ϱ be a T-relation defined in G, and R a π-subgroup in G. A subgroup C of G is an *absolute ϱ-complement* of R if: 1) $R\varrho C$ holds; 2) C is maximal with respect to 1), that is, there does not exist a π'-subgroup such that $C \subset D$ and $R \varrho D$.

Let H be a Hall π'-subgroup of G. The subgroup C of G is a *relative ϱ-complement* of R in H if: 1) $C \subseteq H$; 2) $R \varrho C$ holds; 3) C is maximal with respect to 1) and 2).

Remark 1. If R is a π-subgroup of G, C is an absolute ϱ-complement of R, H is a Hall π'-subgroup of G and $C \subseteq H$, then C is at the same time a relative ϱ-complement of R.

Remark 2. If R is a π-subgroup and H is a Hall π'-subgroup of G then there exists exactly one relative ϱ-complement of R in H.

To show this, consider the set Σ of subgroups X of H for which $R\varrho X$. Then for $X_1, X_2 \in \Sigma$ we have (by the definition of the T-relations) $\langle X_1, X_2 \rangle \in \Sigma$ and so there exists only one relative ϱ-complement of R in H.

Examples for T-relations:

$R\varrho_1 C$ if C is permutable with R,
$R\varrho_2 C$ if C is permutable with all elements of R,
$R\varrho_3 C$ if all elements of C are permutable with R,
$R\varrho_4 C$ if all elements of C are permutable with all elements of R.

Theorem 3. *Let G be a finite group with property $D_{\pi'}$, P a Hall π-subgroup of G and R a subgroup of P. Let ϱ be a T-relation between the π-subgroups and π'-subgroups of G and C an absolute ϱ-complement of R of maximal order. The relative ϱ-complements of R (in various Hall π'-subgroups of G) are all conjugates of C with respect to P and so are all absolute ϱ-complements of C if and only if $a^{-1}Ra\varrho C$ for every $a \in P$.*

Proof. It is easy to see that the condition is necessary. Indeed, consider an element $a \in P$. By hypothesis it is true that $R\varrho aCa^{-1}$ whence $a^{-1}Ra\varrho C$.

The condition is sufficient. By hypothesis $a^{-1}Ra\varrho C$ for every $a \in P$. First of all we prove that aCa^{-1} is a relative ϱ-complement for every $a \in P$ (in a convenient Hall π'-subgroup of G). Because $a^{-1}Ra\varrho C$ and ϱ is a T-relation, $R\varrho aCa^{-1}$ holds. Since $D_{\pi'}$ is true, there exists a Hall π'-subgroup H in G which contains the subgroup C, that is, $aCa^{-1} \subseteqq aHa^{-1}$ where aHa^{-1} is a Hall π'-subgroup of G. By Remark 2 there is only one relative ϱ-complement $\bar{C}$ of R in aHa^{-1}. The subgroup $\bar{C}$ is contained in an absolute ϱ-complement $\bar{\bar{C}}$ of R. Thus we get $aCa^{-1} \subseteqq \bar{C} \subseteqq \bar{\bar{C}}$ and $C \subseteqq a^{-1}\bar{C}a \subseteqq a^{-1}\bar{\bar{C}}a$. But C is an absolute ϱ-complement of R from which $C = a^{-1}\bar{\bar{C}}a$ follows. So we have $aCa^{-1} = \bar{\bar{C}}$. The subgroup aCa^{-1} is a conjugate of C with respect to P and so every conjugate of C with respect to P is an absolute ϱ-complement of R. Finally (by Remark 1) aCa^{-1} is a relative ϱ-complement in every Hall π'-subgroup of G which contains it.

It remains to prove that, conversely, if $\bar{C}$ is a relative ϱ-complement of R contained in a Hall π'-subgroup $\bar{H}$ of G then $\bar{C}$ is a conjugate of C with respect to P. $D_{\pi'}$ holds in G, so we have $C \subseteqq d^{-1}\bar{H}d$ $(d \in G)$. The subgroup $H = d^{-1}\bar{H}d$ is a Hall π'-subgroup of G and we have the factorisation $G = PH$ $(P \cap H = 1)$. Hence $d = ab$ $(a \in P, b \in H)$ from which $\bar{H} = dHd^{-1} = abHb^{-1}a^{-1} = aHa^{-1}$, that is, $H = a^{-1}\bar{H}a$ $(a \in P)$. Since $C \subseteqq H = a^{-1}\bar{H}a$ one gets $aCa^{-1} \subseteqq \bar{H}$. Because $a \in P$ and by hypothesis $a^{-1}Ra\varrho C$ therefore (ϱ being a T-relation) $R\varrho aCa^{-1}$. Because $aCa^{-1} \subseteqq \bar{H}$ and since $\bar{C}$ is the only relative ϱ-complement of R in $\bar{H}$ (by Remark 2) we get $aCa^{-1} \subseteqq \bar{C}$. The subgroup $\bar{C}$ is contained in an absolute ϱ-complement $\bar{\bar{C}}$ of R and therefore $C \subseteqq a^{-1}\bar{C}a \subseteqq a^{-1}\bar{\bar{C}}a$.

But then $C=a^{-1}\bar{\bar{C}}a$ because C is supposed to be an absolute ϱ-complement of R. So we get $aCa^{-1}=\bar{C}=\bar{\bar{C}}$, and Theorem 3 is proved.

Corollary 4. *Let G be a finite group with property $D_{\pi'}$, P a Hall π-subgroup of G and R a normal subgroup of P. Let ϱ be a T-relation between π- and π'-subgroups. Then the relative ϱ-complements of R (in the various Hall π'-subgroups of G) are conjugate with respect to P (and so are absolute ϱ-complements, too).*

Proof. Let C be an absolute ϱ-complement of R. Then $R\varrho C$ and $a^{-1}Ra\varrho C$ for every $a\in P$ ($a^{-1}Ra=R$). By Theorem 3 all relative ϱ-complements of R (in the various Hall π'-subgroups of G) are conjugates of C with respect to P and thus they are absolute ϱ-complements of R, too.

2. Consider now the T-relation ϱ_1. Let G be a finite group and R a π-subgroup of G. We say that the subgroup S of G is a *π-sylowizer* of R if 1) R is a Hall π-subgroup of S, 2) S is maximal with respect to 1). If π contains only one prime number p then the π-sylowizer coincides with the sylowizer concept of GASCHÜTZ [1].

Theorem 5. *Let G be a finite group such that every subgroup of G has the property $D_{\pi'}$. Let R be a π-subgroup of G. Then S is a π-sylowizer of R if and only if $S=RC$ where C is an absolute ϱ_1-complement of R.*

Proof. Let C be an absolute ϱ_1-complement of R, that is, C and R are permutable and RC is a subgroup of G. R is a π-subgroup, C is a π'-subgroup which means that R is a Hall π-subgroup in RC. We prove now that RC is a sylowizer of R. Otherwise there would be a subgroup S of G such that $RC\subset S$ and R is a Hall π-subgroup of S. But by hypothesis S satisfies $D_{\pi'}$, that is, C is contained in a Hall π'-subgroup $\bar{C}$ in S with $S=R\bar{C}$. Hence $R\varrho_1\bar{C}$, and because of $C\neq\bar{C}$ we have a contradiction since C is an absolute ϱ_1-complement of R.

Conversely, suppose that S is a π-sylowizer of R. Since every subgroup has property $D_{\pi'}$, so does a Hall π'-subgroup C. By hypothesis R is a Hall π-subgroup of S from which we have $S=RC$, that is, $R\varrho_1 C$. We prove that C is an absolute ϱ_1-complement of R. Otherwise C would be contained in an absolute ϱ_1-complement $\bar{C}$ of R. Because of $R\varrho_1\bar{C}$ the subgroup $\bar{C}$ is permutable with R and in the same time $S=RC\subset R\bar{C}$ where R is a Hall π-subgroup of $R\bar{C}$. This is a contradiction because by hypothesis S is a sylowizer of R. It follows that C is an absolute ϱ_1-complement of R.

Theorem 6. *Let G be a finite group such that every subgroup of G has the property $D_{\pi'}$. Let P be a Hall π-subgroup of P. Then the π-sylowizers of R are conjugate with respect to P.*

Proof. Let S_1 and S_2 be two π-sylowizers of R. By Theorem 5 we have $S_1=$ $=RC_1$, $S_2=RC_2$ where C_1 and C_2 are absolute ϱ_1-complements of R. By Corollary 4 there exists an element $a \in P$ such that $a^{-1}C_1a=C_2$. It follows $a^{-1}S_1a=a^{-1}RC_1a= =(a^{-1}Ra)(a^{-1}C_1a)=RC_2=S_2$, that is, S_1 and S_2 are conjugate with respect to P.

In particular, the conditions of Theorem 6 are satisfied for solvable groups. If π contains only one prime number then we get Theorem 1 of Gaschütz [1].

Theorem 7. *Let G be a finite group such that every subgroup of G has the property $D_{\pi'}$. Let P be a Hall π-subgroup of G and R a subgroup of P. Suppose that $G=PH$ where H is a Hall π'-subgroup of G. Then the π-sylowizers of R are conjugate if one of the following conditions is satisfied:*

a) $G=N_G(R)\cdot N_G(H)$,

b) $G=N_G(C_1)\cdot N_G(H)$,

c) $G=N_G(R)\cdot N_G(C_1)\cdot N_G(H)$,

where C_1 is a relative ϱ_1-complement of R in a sylowizer of R.

Proof. a) Let S_1 and S_2 be two sylowizers of R. By Theorem 5 we have $S_1=RC_1$, $S_2=RC_2$. We may suppose that $C_1\subseteqq H$ (property $D_{\pi'}$). Again by property $D_{\pi'}$ the subgroup C_2 is contained in a conjugate $a^{-1}Ha$ where $a\in N_G(R)$ in virtue of a). However then C_1 and C_2 as the only relative ϱ_1-complements in H and in $a^{-1}Ha$, respectively, are also conjugate: $C_2=a^{-1}C_1a$, that is, $S_2=RC_2= =Ra^{-1}C_1a=a^{-1}Ra\,a^{-1}C_1a=a^{-1}S_1a$.

b) In this case we prove that $S_1=RC_1$ is the only sylowizer of R in G. Suppose that R has two sylowizers $S_1=RC_1$, $S_2=RC_2$ $(C_1\subseteqq H)$. By hypothesis C_2 is contained in $b^{-1}Hb$ where $b\in N_G(C_1)$. It follows $C_1\subseteqq H\cap b^{-1}Hb$. But RC_1 and RC_2 are sylowizers of R and C_1, C_2 are contained in $b^{-1}Hb$. So we have $C_1=C_2$.

c) Again let $S_1(=RC_1)$ and $S_2(=RC_2)$ be two sylowizers of R in G and $C_1\subseteqq H$. By hypothesis (property $D_{\pi'}$) there are two elements $a\in N_G(R)$, $b\in N_G(C_1)$ such that $C_2\subseteqq abHb^{-1}a^{-1}$ from which we get $C_2=ab\;C_3b^{-1}a^{-1}$ with $C_3\subseteqq H$. Hence $a^{-1}Ra=R$ is permutable with bC_3b^{-1}. But $bC_3b^{-1}\subseteqq bHb^{-1}$, that is, C_1 and bC_3b^{-1} are relative ϱ_1-complements of R in bHb^{-1}, that is, $C_1=C_3$. Thereby we get $C_2= aC_1a^{-1}$.

Reference

[1] W. Gaschütz, Sylowizatoren, *Math. Z.*, **122** (1971), 319—320.

(Received March 22, revised June 17, 1974)

Bibliographie

J. L. Bauer—G. Goos, Informatik, Teil I—II (Heidelberger Taschenbücher, Sammlung Informatik, Bd. 80—91), XII+213, XII+200 Seiten, Berlin—Heidelberg—New York, Springer Verlag, 1971.

Die stürmische Entwicklung der elektronischen Rechenanlagen in den letzten 15 Jahren hat an vielen Universitäten und Hochschulen die neue Studienrichtung Informatik (oder „computer science") zum Leben gerufen. Das vorliegende Buch ist aus den an der TU München gehaltenen. Vorlesungen der Verfasser und anderer prominenter Persönlichkeiten der Informatik entstanden. Sein Ziel ist, wie auch der Untertitel betont, „eine einführende Übersicht" über diesen neuen Wissenschaftszweig, und seine Querverbindungen zu anderen Disziplinen zu schaffen.

Die Darstellung geht vom Allgemeinen zum Speziellen, primär ist die Programmierung und sekundär die Maschine. Diese „top-down" Aufbau möchte ungewöhnlich sein für diejenigen, die ihre Kenntnisse parallel mit der Entwicklung der Computerwissenschaft erworben haben, man muß aber bedenken, daß das Buch für eine andere Generation geschrieben wurde. Großer Vorteil des Buches ist, daß die Verfasser die mit der Darstellung formaler Sprachen oft verbundene Schwerfälligkeit vermeiden konnten, ohne die Exaktheit zu beeinträchtigen. Um außer einer einführenden Übersicht eine wirkliche Einführung in die Informatik zu bekommen, soll der Anfänger auch viele Übungsaufgaben lösen, selbstständig Programme schreiben. In das Buch sind keine Aufgaben aufgenommen, jedoch wird es in Aussicht gestellt, daß das entsprechende Übungmaterial in einem separaten Band derselben Reihe herausgegeben wird.

Die Ausstattung des Buches ist übersichtlich, die vielen Abbildungen und Programmbeispiele erhöhen wesentlich die Verständlichkeit.

Die Kapiteltitel sind: 1. Information und Nachricht; 2. Begriffliche Grundlagen der Programmierung; 3. Maschinenorientierte algorithmische Sprachen; 4. Schaltnetze und Schaltwerke; 5. Dynamische Speicherverteilung; 6. Hintergrundspeicher und Verkehr mit der Außenwelt, Grundprogramme; 7. Automaten und formale Sprachen; 8. Syntaktische und semantische Definition algorithmischer Sprachen. Anhänge über Datenendgeräte und Geschichte der Informatik vervollständigen das Buch.

D. Vermes (Szeged)

Sterling K. Berberian, Lectures in Functional Analysis and Operator Theory (Graduate Texts in Mathematics, Vol. 15), IX+345 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1974.

This book is a useful introduction to several chapters of Functional Analysis and Operator Theory, in which the author's personal style blends with the styles of such masters of exposition as Halmos, Kaplansky, and Bourbaki. It begins with an "apéritif": Gelfand's functional analytic proof of Wiener's theorem on the reciprocal of an absolutely convergent Fourier series. Chapters:

1. Topological Groups; 2. Topological Vector Spaces, 3. Convexity; 4. Normed Spaces, Banach Spaces, Hilbert Spaces; 5. Category; 6. Banach Algebras; 7. C^*-Algebras; 8. Miscellaneous Applications. Among these applications we find e.g. a formulation of the spectral theorem for normal operators, introduction to von Neumann algebras, group representations, the character group of an LCA group. (Spectral measure and spectral integral representation are nowhere mentioned.) There are many 'exercises' listed. A *10* page 'Hints, Notes, and References' and a Bibliography of *150* titles conclude the book.

Béla Sz.-Nagy (Szeged)

János Bognár, Indefinite Inner Product Spaces (Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 78), IX+223 pages, Berlin—Heidelberg—New York, Springer-Verlag, 1974. — DM. 48 —.

This book is an excellent foundation of the theory of indefinite inner product spaces, and gives a good starting point for studying special topics and applications of this area. Results of a number of authors are discussed in a clear, elegant manner.

The book consists of nine chapters preceeded by a short "Preface". In Chapter I the basic notions are introduced and analysed. In Chapter II linear operators are discussed in an indefinite inner product space without topology (among others: isometric and symmetric operators, plus-operators and Cayley transformations). In Chapter III and IV several topologies are introduced, their connections to each other and to the inner product are explained. Relations are studied between the topologies and the orthogonal companion, the existence of projections, etc. Chapter V deals with the geometry of Krein spaces (non-degenerate, decomposable, complete spaces). The main topic of Chapter VI is unitary and selfadjoint operators in Krein spaces, especially their continuity and the location of their spectra. In Chapter VII positive operators (especially plus-operators) are discussed in Krein spaces. Chapter IX is devoted to Pontrjagin spaces and their operators.

At the end of each chapter there are given Notes which contain partly historical and other comments related to the main text, partly a survey of the literature of advanced topics and applications not detailed in this book. A carefully prepared list of references is included.

The book is a complete introduction, contains all of the necessary definitions and gives full proofs. However, it is advantageous for the reader to be familiar with the basic facts of linear algebra, topology, and Hilbert and Banach space theory.

The material of the book is lucidly arranged and the exposition is clear. A great number of illustrating examples makes the understanding easier.

E. Durszt (Szeged)

5th Conference on Optimization Techniques, Part I—II (Lecture Notes in Computer Science 3—4), Edited by **R. Conti** and **A. Ruberti,** XIII+565, XIII+389 pages, Berlin—Heidelberg— New York, Springer-Verlag, 1973.

These Proceedings contain the papers presented at the Conference of the International Federation of Information Processing (IFIP) held in Rome, May 7—11, 1973. The authors' manuscripts are reproduced photographically.

The first part contains the papers of more theoretical nature from the following fields: System modelling and identification, distributed systems, game theory, pattern recognition, optimal control, stochastic control, mathematical programming, numerical methods. The second part is devoted to application areas as urban and society systems, computer and communication networks, environmental systems, economic models, biological systems.

The nearly 100 papers of authors from all parts of the globe cover most part of optimization theory and related areas, and give a good insight into the fields of recent research.

D. Vermes (Szeged)

John B. Conway, Functions of one complex variable (Graduate Text in Mathematics, Band 11), XI+313 pages, New York—Heidelberg—Berlin, Springer-Verlag, 1973.

This book is a good introduction to the theory of functions of one complex variable. It is intended as a textbook for students, familiar with elementary real analysis. In fact, the actual prerequisites for reading the book are quite minimal: mathematical maturity to understand and execute $\varepsilon-\delta$ arguments.

The text consists of twelve chapters. The first three chapters summarize the basic definitions and facts on the complex number system, metric spaces and the topology of the field of complex numbers, and elementary properties of analytic functions. Chapter 4 is devoted to complex integration, which is fundamental in the study of analytic functions. Chapter 5 contains the classification of singularities of functions that are analytic in a punctured disk. The next chapter starts with the maximum modulus theorem and presents various extensions and applications such as Hadamard's three circles theorem and the Phragmén-Lindelöf theorem. In Chapter 7 a metric is put on the set of all analytic functions on a fixed region, and compactness and convergence properties are discussed. Proofs of the Riemann mapping theorem and the Weierstrass factorization theorem are obtained as applications. Chapters 1 through 7 are basic and used repeatedly in the rest of the book.

The remaining chapters are independent topics and may be studied in any desired order. Chapter 8 presents Runge's theorem and, as a consequence, a more general form of Cauchy's theorem. A theorem of Mittag-Leffler on the existence of meromorphic functions with prescribed poles and singular parts is also proved. Chapter 9 studies the problem of analytic continuation and introduces the reader to the theory of analytic manifolds and covering spaces. Chapter 10 is devoted to the questions of harmonic functions, including a solution of the Dirichlet problem and the introduction of Green's functions. The subject of the last two chapters is a short outline of the theory of entire functions. Chapter 11 gives a complete proof of Hadamard's factorization theorem, while in Chapter 12 the great theorem of Picard is proved.

The author's guiding principle is that all definitions, theorems, etc. should be clearly and precisely stated. The proofs are given in detail, the connections are pointed out perfectly. Each section is followed by exercises, which help the reader understand the ideas presented, extend the theory or give applications to other parts of mathematics. The book is supplemented by an appendix on the calculus of complex valued functions defined on an interval.

F. Móricz (Szeged)

D. H. Fremlin, Topological Riesz Spaces and Measure Theory, XIV+266 pages, Cambridge University Press, 1974.

The development of the theory of Riesz spaces (vector lattices) was extremely fast (because of its connections with functional analysis), however a relatively long time passed until the publication of the first monographs on the theory. Both in theory and applications Luxemburg's and Zaanen's book can be regarded as the first monograph on the subject; in the field of further applications this was followed by Fremlin's book reviewed here. In the preface the author writes: "My aim ... is to identify those concepts in measure theory which have most affected functional analysis and to integrate them into the latter subject in a way consistent with its own structure and habits of thought". Since the principal Banach spaces which measure theory has contributed to functional analysis are all Riesz spaces in a natural way, and since many of their special properties can be derived from their (topological) Riesz space structure, the author presents the material within the framework of an abstract theory dealing with topological Riesz spaces.

Chapters 1 and 2 elaborate the basic concepts and results of the theory of topological Riesz spaces, in particular, of L- and M-spaces.

Chapters 3 to 5 are devoted to the study of dual spaces, Riesz spaces over Boolean rings and measure algebras, respectively. By using the results of the previous chapters, the last three chapters deal with measure theory and, among others, include the Radon—Nikodým theorem and the Riesz theorem concerning the integral representability of linear functionasl on spaces of continuous functions.

The elaboration of the book is rigorously exact.

A. P. Huhn (Szeged)

H. G. Garnir—M. de Wilde—F. Schmets, Analyse fonctionnelle. Théorie constructive des espaces linéaires à semi-normes. Tome I: Theorie générale, X+562 pages, 1968. **Tome II: Mesure et intégration dans l'espace euclidien,** 287 pages, 1972. (Lehrbücher und Monographien aus dem Gebiete der Exakten Wissenschaften, Mathematische Reihe, Bd. 36—37.) Basel—Stuttgart, Birkhäuser Verlag.

Le tome I expose la théorie générale des espaces linéaires à semi-normes ou espaces vectoriels topologiques localement convexes. L'intention des auteurs est ce que la lecture de l'ouvrage exige seulement une connaissance d'analyse élémentaire et ils réussissent à la réaliser par l'utilisation systématique des semi-normes et en évitant les moyens topologiques tant que possible. Les raisonnements sont constructifs, ils suivent l'épigraphe de l'Introduction: „Il faut attacher une bien autre importance aux exemples qui n'utilisent pas l'axiome de Zermelo qu'à ceux qui l'utilisent.“ D'autre part, l'ouvrage renferme tous les résultats importants de la théorie; quelques titres nous en convainquent: Limite inductive, produit, quotient; Prolongement des fonctionnelles linéaires bornées; Ensembles équibornés; Duaux particuliers; Espaces nucléaires; Fonctionnelles bilinéaires et produits tensoriels; Espaces d'opérateurs bornés; Théorie spectrale des opérateurs bornés.

Cependent, on peut douter que l'exclusion de la topologie soit justifiée. La topologie n'est pas une théorie étrange de nos jours. Beaucoup de notions et relations introduites dans le livre seraient simplement liées entre elles justement par la théorie de la topologie. D'autre part, il est déplorable que la définition des applications linéaires bornées resp. continues n'est pas celle qu'on emploit usuellement. Aussi, beaucoup de notations ne sont pas celles familières et on peut reprocher le manque d'un tableau de notations.

Il n'y a aucun exemple dans le tome I. Le tome III — à paraître — est prédestiné à servir des exemples, traitant de la théorie des espaces linéaires à semi-normes particulières et des espaces Hilbertiens.

Le tome II sert de base à l'étude des espaces de suites, de fonctions, de distributions, qui feront l'objet du tome III. La pluspart de ce volume est indépendente du tome I. Les mesures sont définies à priori sur les semi-intervalles dans un ouvert d'un espace euclidien et sont à valeurs complexes. Partant des fonctions étagées sur les semi-intervalles, on définit les fonctions intégrables et on démontre leurs propriétés essentielles par la méthode des suites de Cauchy. On passe ensuite à un traitement des fonctions et des ensembles boréliens. Un chapitre est consacré aux relations entre mesures et on considère aussi l'intégration de fonctions à valeurs dans un espace linéaire à semi-normes et des mesures à valeurs dans un espace linéaire à semi-normes.

T. Matolcsi (Szeged)

K. P. Hadeler, Mathematik für Biologen (Heidelberger Taschenbücher, Bd. 129), IX+232 Seiten, Berlin—Heidelberg—New York, Springer-Verlag, 1974.

Die heutigen biologischen Wissenschaften brauchen immer mehr mathematische Hilfsmittel, dementsprechend enthält dieses kleine Buch auch eine ausgebreitete mathematische Einführung. Neben dem systematischen Aufbau der Differential- und Integralrechnung und der linearen Algebra findet man mehrere Paragraphen über Differentialgleichungen und einige über Wahrscheinlichkeitsrechnung und mathematische Statistik.

Das Buch folgt eine moderne und exakte Terminologie; Sätze, deren Beweise tiefliegender sind, werden natürlich ohne Beweis mitgeteilt. Die interessantesten Teile sind aber die biologischen Anwendungen der mathematischen Hilfsmittel: Räuber—Beute-Modelle, Selektionsmodelle, ein Nervenmodell, die Entwicklung der Populationen, die Gleichgewichtszustände und ihre Stabilitätsfragen werden ausführlich diskutiert.

K. Tandori (Szeged)

P. R. Halmos,

Finite-Dimensional Vector Spaces (Undergraduate Texts in Mathematics), VIII+200 pages.
Naive Set Theory (Undergraduate Texts in Mathematics), VII+104 pages.
Lectures on Boolean Algebras, VII+147 pages.
Measure Theory (Graduate Texts in Mathematics, Vol. 18), XI+304 pages.
A Hilbert Space Problem Book (Graduate Texts in Mathematics, Vol. 19), XVII+365 pages.
New York—Heidelberg—Berlin, Springer-Verlag, 1974.

The books are new editions of the well-known earlier ones. Seven, eleven, sixteen, and twenty four years after their first editions the books kept to be modern, interesting and brilliant.

From a preface of the author: "The only way to learn mathematics is to do mathematics." "The right way to read mathematics is first to read the definitions of the concepts and the statements of the theorems and then, putting the book aside, to try discover the appropriate proofs." We can add that the right way to teach mathematics is to give such lectures and to write such books that the listeners or readers be able to understand easily the motivation of definitions and to grasp the core of the statements. The high popularity of Halmos' books proves that the author succeeded in teaching mathematics to his readers in the right way.

One of the greatest merits of Halmos' texts lies in their clear structure, simple draft, consequent and suggestive notations which set them up as a model for modern texts and monographs in mathematics.

T. Matolcsi (Szeged)

Ronald Larsen, An Introduction to the Theory of Multipliers (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Bd. 175), XX+282 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1971.

The concept of a multiplier first appears in attempts to describe those sequences $\{c_n\}$ for which $\Sigma c_n a_n e^{int}$ is a Fourier series whenever $\Sigma a_n e^{int}$ is such. Multipliers enjoy much past and recent attention. There are now several definitions of a multiplier and one can be meaningful while the other is not; however, in many important cases they are all meaningful and equivalent. It is not generally known if any two of them are equivalent, provided that they are meaningful. One possible definition (in the commutative case) is the following: Let G be a locally compact Abelian group and X, Y topological linear spaces of (equivalence classes of) functions or measures defined on G. Then a multiplier for the pair (X, Y) is any continuous linear mapping of X into Y which commutes with the operators that the group translations induce in X and Y. In many cases the functions or measures f considered have Fourier transforms $\hat{f}$ (on the dual group $\hat{G}$). In these cases, by another customany definition, a multiplier is a linear transformation T from X to Y such that $(Tf)^{\hat{}}=\varphi\hat{f}$ for each $f\in X$ and some function φ on $\hat{G}$. Still another definition determines a multiplier for a commutative Banach algebra as a mapping T of the algebra under consideration into itself for which $T(xy)=x(Ty)$ holds for any elements x, y of the algebra. This definition is not as a rule meaningful or valid in all cases mentioned above; however, it can often be established for certain subsets of X and Y.

The book concentrates on the characterization problem of multipliers from the functional analytic point of view. Only the commutative version of the theory is presented; however, some non-commutative results are also treated and there are references to such results. The first chapter is a prologue, in which the multipliers for the pair $(L_1(G), L_1(G))$ are studied. Two subsequent chapters discuss multipliers of Banach algebras and commutative H^*-algebras. After this the book studies in five chapters the multipliers for the pairs (X, Y) where X and Y are the spaces $L_p(G)$ $(1\leqq p\leqq\infty)$, the space $C_0(G)$ of all complex valued continuous functions which vanish at infinity, the dual space of $C_0(G)$ with the weak-star topology, the space of bounded regular complex valued Borel measures on G, the Banach algebras $A_p(G)$ of elements in $L_1(G)$ whose Fourier transforms belong to $L_p(\hat{G})$, and the Hardy spaces of compact connected Abelian groups with ordered duals. At the end of each chapter the author indicates some sources of the material developed in the chapter in question. Some applications of the theory of multipliers are also presented. A number of appendices facilitates the reading of the book.

J. Szűcs (Szeged)

Fonctions analytiques de plusieurs variables et analyse complexe (Série „Agora Mathematica" dirigée par **P. Lelong,** vol. 1), VIII+272 pages, Gauthier-Villars, Paris, 1974.

Ce volume contient les exposés des communications faites au Colloque International du C. N. R. S., organisé sur l'initiative de P. Lelong à Paris, 14—20 juin 1972. Les 29 exposés, écrits par des spécialistes, recouvrent une grande partie des recherches actuelles dans le domaine d'Analyse complexe. Ils se dirigent en particulier vers les sujets suivants: a) Fonctions analytiques de n variables complexes; géométrie analytique; singularités. b) Analyse complexe, fonctions plurisousharmoniques et functions analytiques dans les espaces vectoriels topologiques. c) Problèmes de cohomologie à croissance et solutions constructives.

Béla Sz.-Nagy (Szeged)

J. and **R. Nevanlinna, Absolute Analysis** (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, Band 102), II+270 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1973.

This second edition is a translation of the authors' monograph which appeared in 1959 in German.

It presents a systematic account of an absolute, coordinate and dimension free infinitesimal vector calculus. The elimination of coordinates signifies a gain not only in a formal sense. It leads to a greater unity and simplicity in the theory of functions of arbitrarily many variables; the algebraic structure of analysis is clarified, the geometric aspects of linear algebra become more prominent, and these promote the formation of new ideas and methods.

The presentation is in general restricted to the finite dimensional case, i.e., to the theory of finitely many variables. At the same time it lies in the nature of the methods that they can be applied, either directly or with certain simple modifications, to the case of Hilbert or Banach spaces of infinitely many dimensions.

The book consists of six chapters, an index, and a short but effective bibliography. Chapter I contains the fundamentals of linear algebra and analytic geometry of finite dimensional spaces. The central problems of differential calculus are developed in Chapter II. Because of the great significance of the theory of implicit functions, two different methods for the inversion problem are presented. Chapter III is devoted to integral calculus and Chapter IV to the theory of differential equations. As an application of the preceding chapters, the basic features of the classical curve theory and of the Gaussian surface theory are presented in Chapter V. In this new edition, a survey of the elements of Riemannian geometry has been added in Chapter VI. This edition also differs at several other points from the first one. In particular, the theory of implicit functions in Chapters II and IV on differential equations have been substantially reworked and extended.

The presentation of the book is concise but always clear and well-readable. It can be recommended to everybody familiar with the usual, coordinate-based, structure of the elements of infinitesimal calculus. It seems that the absolute infinitesimal calculus can be advantageously used not only in mathematics, but also in theoretical physics.

F. Móricz (Szeged)

J. C. Oxtoby, Maß und Kategorie (Hochschultext), VII+111 Seiten, Berlin—Heidelberg—New York, Springer-Verlag, 1971.

Der Bairesche Kategorie-Satz erlaubt uns mathematische Objekte, die sonst schwer zu sehen wären, sichtbar zu machen, und er kann bei der Formulierung von Existenzsätzen besonders nützlich sein. Das Kategorie-Studium dient jedoch auch noch einem anderen Zweck, namentlich fügt es der Maßtheorie neue Perspektiven hinzu.

Das Buch behandelt hauptsächlich zwei Themenkreise: den Baireschen Kategorie-Satz als Hilfsmittel für Existenzbeweise, sowie die „Dualität" zwischen Maß und Kategorie. Es gibt auch eine kurze Einführung in die Grundlagen der Baireschen Kategorie-Theorie und in die grundlegenden Eigenschaften des Lebesgueschen Maßes. Außerdem werden einige Begriffe aus der metrischen und der allgemeinen Topologie eingeführt, um viele Beispiele für die Anwendung der Baireschen Kategorie-Methoden geben zu können.

Vom Leser werden lediglich grundlegende Kenntnisse aus der Analysis und eine gewisse Vertrautheit mit der Mengenlehre vorausgesetzt.

T. Matolcsi (Szeged)

G. Preuss, Allgemeine Topologie (Hochschultext), VIII+488 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1972.

This book is based on lectures held by the author at the University of Berlin during the summers 1970—71. It is intended as an introduction into set theoretical topology, without special prerequisites. Thus it is offered to anyone interested in topology and mature enough to understand abstract mathematical thinking.

The book consists of 11 Chapters. Chapter 0 presents the set theoretical background needed for the rest of the book. Chapter 1 introduces the notion of topological spaces (it gives several different mutually equivalent definitions), and then defines continuity. This chapter also deals with the category theoretical foundations of topology. Chapter 2 brings to the reader the modern theory of limit: it presents the fundamentals of filter convergence and ultrafilters. Chapter 3 deals with weakest and finest topologies and their category theoretical aspects. Chapter 4 is devoted to the systematic study of separation axioms. Chapter 5 studies the classical concept of connectedness and its generalizations. Chapter 6 is devoted to the study of the interplay between separation and connectedness. After this, in Chapter 7, an account is given of several concepts of compactness, and quasicompact and locally compact spaces are studied. This chapter ends with a quite detailed study of compactifications. Chapter 8 is devoted to some modern aspects of set theoretical topology. The reader can skip this chapter for the first reading of the book without disturbing the study of the remaining chapters. Chapter 9 summarizes the basic notions and results concerning uniform spaces. It also treats the problem of uniformibility and metrizability. The concluding chapter 10 is devoted to the study of proximity spaces.

The book ends with a rich collection of exercises, which help the reader understand the main text.

László Gehér (Szeged)

H. Rademacher, Topics in Analytic Number Theory (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, Band 169), IX+320 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1973.

At the time of Professor Rademacher's death in 1969, the manuscript of the present work was already completed. The editors had only to supply a few bibliographical references and to correct a few misprints and errors.

The text consists of four parts, divided into fifteen chapters. The book is supplemented with the editors' notes, a short but effective bibliography, and an index.

The first five chapters constitute Part I, which is devoted to the basic analytic tools employed, such as the Bernoulli polynomials and numbers, the Euler—MacLaurin sum formula, the Γ-function and Mellin's theory, the Phragmén—Lindelöf theorem, the Poisson sum formula, and various applications of these topics.

Part II deals with the special functions that are of fundamental importance in analytic number theory. Particular attention is paid to the Riemann ζ-function and to the connection between the prime-number theorem and the zeros of the ζ-function. The proof of the prime number theorem and the role that the location of the zeros of $\zeta(z)$ in the "critical strip" $0<\mathrm{Re}(z)<1$ plays in the whole theory of the distribution of prime numbers are treated in Chapters 6—7. The error term in the prime-number theorem is obtained with the aid of Dirichlet series. In Chapter 8 Eisenstein series and modular forms are considered. Chapter 9 introduces the notion of the Dedekind function $\eta(\tau)$ and the Dedekind sums, and proves the formula of reciprocity of the Dedekind sums. The close connection between the reciprocity formula for Dedekind sums and the Jacobi residue symbol is also indicated. In Chapter 10 the theory of ϑ-functions is developed, while Chapter 11 contains the main properties of elliptic functions and their applications to number theory.

The results of Part III are mainly based on the method of formal power series. This method compares the coefficients of two different expansions of the same function and interpretes them in an arithmetical way, where the question of convergence plays no role, since the arguments are purely formal and concern only formal power series. The formal power series themselves form a commutative ring with unit and without zero divisors, provided the coefficients are taken from a ring of the same type. In Chapter 12 the connection between formal power series and the theory of partitions is described. Chapter 13 is a detailed account of Ramanujan's congruences and identities. The proofs, following Ramanujan, are given by means of formal power series. Independently, Schur had rediscovered these identities and employed the important "Gaussian polynomials" in his proof. Schur's proof gives some deeper arithmetical insight into the structure of these formulae.

If one replaces the indeterminate by a complex variable z, the formal power series becomes a power series in the usual sense to which the concept of convergence applies. Convergent power series represent analytic functions and the formal identities become equations for analytic functions. This step opens the whole store of analytic tools for the treatment of arithmetical problems in additive number theory. Part IV contains the description of the analytic theory of partitions (Chapter 14) as well as the application of the circle method to modular forms of positive dimension (Chapter 15).

The book has been carefully and accurately written. The style is tight, with hardly a word wasted. There is a lack of motivation at some places, and some of the theorems are stated without background explanations.

The work contains a wealth of information in a concise and polished form, accurate from the viewpoint of rigorous analysis. It can be used as a textbook for students of graduate courses, but it is a useful reading also for mature mathematicians interested in analytic number theory.

F. Móricz (Szeged)

Leopold Schmetterer, Introduction to Mathematical Statistics (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Bd. 202), VII+502 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1974.

This is an English translation of the second German edition of the author's book "Einführung in die mathematische Statistik" published also by Springer-Verlag. Some changes had been made during the preparation of the translation: misprints hade been corrected, proofs had been altered, new results had been included and the bibliography had been supplemented with new references. The book, as it is now presented, is a very accurate and systematic introduction into the modern theory of mathematical statistics. It can be recommended especially to those who have already acquired sufficient knowledge from real function theory and linear algebra and want to put their knowledge of mathematical statistics on a wider and more solid base.

K. Tandori (Szeged)

D. R. Smart, Fixed point theorems (Cambridge Tracts in Mathematics, Volume 66), VIII+93 pages, Syndics of the Cambridge University Press, Cambridge, 1974.

The book is an introduction, from the point of view of the functional analyst, to fixed point theorems and their applications. The only prerequisite it requires is a minimal knowledge of functional analysis, so it will be very useful for graduate students. For its small size the book deals with a considerably wide range of results. It presents several fixed point theorems for individual (one- and many-valued) mappings of different kinds, commuting and non-commuting families of mappings and also for mappings obtained by continuous deformation. Among others, fixed points of contractions of several kinds; Brouwer's fixed point theorem and its generalizations: the theorems of Schauder, Tychonoff and Rothe; furthermore, the fixed point theorems of Browder—Potter, Krasnoselskii, Leray—Schauder, Schaefer, Kakutani—Markov, and Ryll—Nardzewski are discussed. Fixed point theorems are applied to differential equations, the theory of games and are used to prove the existence of some invariant means such as the Haar measure on compact groups, the invariant mean on almost periodic functions, and the Banach limit.

In the book algebraic topology is used only in Chapter 10 where the discussion is only intuitive with references to rigorous arguments. Proofs are mostly complete and always easy to understand. However, there are a few incomplete proofs (for example, the first proof of Brouwer's theorem relies on the fact that the n-sphere is non-contractible, which is not proved in the book). In such cases references to complete proofs are always provided.

The book consists of 11 chapter, most of them also contain exercises. An index and a bibliography are included.

J. Szűcs (Szeged)

B. L. van der Waerden, Group Theory and Quantum Mechanics (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Bd. 214), VIII+211 pages, Springer-Verlag, Berlin—Heidelberg—New York, 1974.

The original, German edition of this book appeared in 1932, in the same series. It is with nostalgy that the reviewer recalls how he was influenced, as a young student, by reading this book. Not only did he learn from it this — at that time so novel — method, the role of group representations in the theory of atomic and molecular spectra, but he was also fascinated by the clear and concise way of exposition.

The present English edition is not a mere translation. Indeed, the whole volume was rewritten so that it has become longer by a third, and a large amount of newer development is taken into consideration. (Curiously enough, Chapter 6, on Molecule Spectra, which "was too much condensed in the German edition", has become shorter by a third.)

Béla Sz.-Nagy (Szeged)

E. S. Wentzel—L. A. Owtscharow, Aufgabensammlung zur Wahrscheinlichkeitsrechnung, 353 Seiten, Berlin, Akademie Verlag, 1973.

Das vorliegende Buch ist eine stark überarbeitete Übersetzung des russischen Originals. Es besteht aus zehn Kapiteln, die außer des Standard-Stoffes der Wahrscheinlichkeitsrechnung auch die Gebiete der stationären und Markowschen Prozesse umfassen. Neben den wohlbekannten Würfel- und Urnenproblemen behandeln viele Aufgaben auch reale Anwendungen z. B. aus dem Militärwesen, Technik und Bedienungstheorie, jedoch kann man nicht sagen, daß durch Lösung dieser Aufgaben der Leser einen Überblick über alle Anwendungsgebiete der Wahrscheinlichrechnung erhält.

Am Anfang jedes Kapitels werden die wichtigsten theoretischen Grundlagen zusammengefaßt. Zu jeder Aufgabe wird das Ergebnis, bei komplizierteren Problemen auch die ganze Lösung angegeben. Damit eignet sich die Aufgabensammlung gut zum Selbststudium. Auswahl und Schwierigkeit der Aufgaben sind an die Erfordernisse der Ingenieur-Ausbildung abgestimmt. Tabellen der Poisson- und Normalverteilung vervollständigen das Buch.

D. Vermes (Szeged)

INDEX — TARTALOM

Csákány, B., Varieties of affine modules 3
Klukovits, L., Hamiltonian varieties of universal algebras 11
Csákány, B.—Megyesi, L., Varieties of idempotent medial quasigroups 17
Csákány, B., Varieties in which congruences and subalgebras are amicable 25
Csákány, B., On affine spaces over prime fields 33
Fried, E., Equational classes which cover the class of distributive lattices 37
Гохберг И. Ц.—Хайниг Г., Результантная матрица и ее обобщения I. Результаный оператор матричных полиномов 41
Hively, G. A., Wiener—Hopf operators induced by multipliers 63
Jakubík, J., Modular lattices of locally finite length 79
Lee Sin-Min, Equational classes of rings generated by zero rings and Galois fields 83
Leindler L., On the strong approximation of orthogonal series 87
Márki, L., On locally regular Rees matrix semigroups 95
Niederreiter, H., On a paper of Blum, Eisenberg, and Hahn concerning ergodic theory and the distribution of sequences in the Bohr group 103
Putnam, C. R., Dissipative *J*-self-adjoint operators and associated *J*-isometries 109
Rédei, L. B., An identity for Laguerre polynomials 115
Salinas, N., Subnormal limits of nilpotent operators 117
Stingl, V., Eine Kennzeichnung der endlichen einfachen Gruppe der Ordnung 604 800 125
Szabó, L., Characterization of some related semigroups of universal algebras 143
Szász, G., Derivations of lattices 149
Sz.-Nagy, B. and Foiaş, C., An application of dilation theory to hyponormal operators 155
Zappa, G. and Szép, J., A generalization of Gaschütz's theorem on sylowizers 161
Bibliographie 165

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)

INDEX: 26024

75-71 — Szegedi Nyomda

Felelős szerkesztő és kiadó: Szőkefalvi-Nagy Béla
A kézirat a nyomdába érkezett: 1975. január 7.
Megjelenés: 1975. június hó

Példányszám: 1200. Terjedelem: 15,4 (A/5) ív
Készült monószedéssel, íves magasnyomással,
az MSZ 5601-24 és az MSZ 5602-55 szabvány szerint