ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA SCIENTIARUM MATHEMATICARUM

ADIUVANTIBUS
L. KALMÁR, L. RÉDEI ET K. TANDORI
REDIGIT
B. SZ.-NAGY

TOMUS XXII
FASC. 1—2

SZEGED, 1961

INSTITUTUM BOLYAIANUM UNIVERSITATIS SZEGEDIENSIS

A SZEGEDI TUDOMÁNYEGYETEM KÖZLEMÉNYEI

ACTA SCIENTIARUM MATHEMATICARUM

KALMÁR LÁSZLÓ, RÉDEI LÁSZLÓ ÉS TANDORI KÁROLY
KÖZREMŰKÖDÉSÉVEL
SZERKESZTI
SZŐKEFALVI-NAGY BÉLA

22. KÖTET
1—2. FÜZET

SZEGED, 1961. MÁJUS HÓ

SZEGEDI TUDOMÁNYEGYETEM BOLYAI-INTÉZETE

Sur une propriété d'interpolation remarquable dans la théorie des ensembles partiellement ordonnés

Par MIHAÏL BENADO à Bucarest (Roumanie)

A Monsieur le Professeur László Rédei, à l'occasion de son 60-ième anniversaire

§ 1. Introduction

On doit à FRÉDÉRIC RIESZ la découverte d'une propriété d'interpolation des ensembles partiellement ordonnés (dans la suite, propriété (IR); cf. par exemple [7] Chap. IV, § 3), dont il a montré l'importance pour la théorie des groupes partiellement ordonnés, la théorie des opérations linéaires etc. (Cf. [7] Chap. XIV et XV.)

Dans le § 2 de mon rapport [1] j'ai attiré l'attention au fait que la propriété (IR) préfigure la notion de *structure géométrique rieszienne* d'une configuration quelconque (cf. aussi [2], 2.2, Exemple 3). Effectivement, pour qu'une configuration[1]) satisfasse à la propriété (IR) *il faut* (et au cas où elle est filtrante, *il suffit*) que sa structure géométrique rieszienne coïncide (au sens de [1] 3.4.1) avec sa structure géométrique discrète ([2] 2.5.1). J'ai indiqué également les relations de la structure géométrique rieszienne aux structures géométriques *dédékindienne* et *hausdorffienne* ([1] 3.2 et [2] 2.2 et 2.3).

Les treillis ([7] Chap. II, § 1) satisfont toujours, comme on sait, à la propriété (IR). Par contre, les multitreillis [3], [4] ne la vérifient pas toujours; mais tout multitreillis *filtrant*, satisfaisant à la propriété (IR), est un treillis. (Cf. [3] 1.4.1.)

Il y a cependant des multitreillis, tels les multitreillis distributifs ([3] § 6 et [4], § 3), qui vérifient une propriété d'interpolation remarquable, d'ailleurs plus faible que la propriété (IR), notamment la *propriété d'interpolation cartésienne* (dans la suite, propriété (IC)), que j'ai découverte à l'occasion de mes recherches sur la fonction de Möbius (cf. [5] § 3 et [6]).

---

[1]) Quant aux notations et aux définitions, je renvoie le lecteur à ma note [2] dont je présuppose la connaissance. Voir aussi [1] § 3 et le § 2 du présent travail.

Mon but dans le présent travail est de faire valoir la propriété (IC) pour les structures géométriques $\mathcal{G}$-distributives d'une configuration quelconque, attendu que certaines suppositions „d'incidence" ([1] § 4) soient vérifiées.

Je vais notamment prouver la proposition suivante:

Théorème. *Toute structure géométrique analytique, fermée et $\mathcal{G}$-distributive d'une configuration, est à interpolation cartésienne.*

Le théorème 3.3 de [5] est un cas particulier du théorème ci-dessus dont la démonstration est, du reste, calquée sur celle que j'ai donnée du théorème cité, bien que, dans les détails, elle en diffère sensiblement sur quelques points.

§ 2. Quelques définitions

2.1. Par *configuration* et par *ensemble partiellement ordonné* ([7] Chap. I, § 1), j'entends la même chose. Dans tout ce qui suit, $\mathcal{S}$ désigne une configuration quelconque par rapport à l'ordre partiel $\geqq$ ou $\leqq$.

2.2. Soient Υ une *relation de divisibilité* et Σ une *relation de multiplicabilité* ([2] 2.1) définies dans $\mathcal{S}$.[2]) Je dirai que $\mathcal{S}$ *est munie d'une* (Υ, Σ)-*structure géométrique*, lorsqu'il existe au moins un quadruple d'éléments (non nécessairement distincts deux à deux) $a, b, d, m \in \mathcal{S}$ tels que

$$d\Upsilon\{a, b\}, \quad m\Sigma\{a, b\}. \tag{1}$$

Cette définition est un peu plus large que celle que j'ai donnée dans ma note [2], 2.5, axiome $SD1$. Dans tout ce qui suit, je suppose que $\mathcal{S}$ est munie de quelque (Υ, Σ)-structure géométrique (= structure géométrique, tout court).

2.2.1. Lorsque pour $a, b, d, m \in \mathcal{S}$ on a (1), je dirai que $(d, m; a, b)$ est un (Υ, Σ)-*quadrilatère*. (Cf. [1] 3.3.)

2.3. Je dirai qu'une structure géométrique est:

A) *analytique*, lorsque, pour tous les $a, b, d, m, x \in \mathcal{S}$ satisfaisant à (1) et à $d \geqq x \geqq m$, il existe des éléments $a_1, a' \in \mathcal{S}$ tels que $d \geqq a_1 \Upsilon\{a, x\}$ et $m \leqq a' \Sigma\{a, x\}$ (cf. [2] 2.5, axiomes $SD2_1$ et $SD2'$);

B) *fermée*, lorsque, pour tous les $a, a_1, a', b, d, m \in \mathcal{S}$ satisfaisant à (1) et à $d \geqq a_1 \geqq a \geqq a' \geqq m$, on a les relations $d\Upsilon\{a_1, b\}$ et $m\Sigma\{a', b\}$ (cf. [1] 4.2);

C) $\mathcal{G}$-*distributive*, lorsque, pour tous les $a, b, b', d, m \in \mathcal{S}$ satisfaisant à (1) et à $d\Upsilon\{a, b'\}$ et $m\Sigma\{a, b'\}$, on a $b = b'$ (cf. [1] 6.3);

---

[2]) Et non nécessairement *duales l'une de l'autre* au sens de ma note [2] 2.4.

D) *à interpolation cartésienne,* lorsque, pour tous les $a, a_1, a', b, b_1, b', d, m \in \mathfrak{S}$ satisfaisant à (1), à

$$d \geqq a_1 \geqq a \geqq a' \geqq m, \quad d \geqq b_1 \geqq b \geqq b' \geqq m \tag{2}$$

et à

$$\begin{cases} a_1 \Upsilon\{a, b'\}, & a' \Sigma\{a, b_1\}, \\ b_1 \Upsilon\{a', b\}, & b' \Sigma\{a_1, b\}, \end{cases} \tag{3}$$

on a[3])

$$(a_1/b') \cap (b_1/a') \neq \emptyset \tag{4}$$

où $\emptyset$ est l'ensemble vide.

C'est cette propriété que j'appelle ici *propriété* (IC) des structures géométriques; cf. [1] 4.4.

§ 3. Démonstration du théorème

3.1. Le m m e. *Toute structure géométrique analytique, fermée et $\mathcal{G}$-distributive est $\mathcal{O}$-modulaire. Cela veut dire que pour tous les $a, a_1, b, b' d, m \in \mathfrak{S}$ satisfaisant à* (1) *et à* $d \geqq a_1 \geqq a$, $b \geqq b' \geqq m$, *la relation* $a_1 \Upsilon\{a, b'\}$ *équivaut à la relation* $b' \Sigma\{a_1, b\}$.

Démonstration. Je démontre seulement que $a_1 \Upsilon\{a, b'\}$ entraîne $b' \Sigma\{a_1, b\}$; quant à la réciproque, il suffit de remarquer que la dualité au sens de [7] (Chap. I, § 3) transforme toute relation de divisibilité Υ (de multiplicabilité Σ) en une relation de multiplicabilité $\Sigma = \check{\Upsilon}$ (de divisibilité $\Upsilon = \check{\Sigma}$), qui lui est duale au sens de [2] 2.4.

Or, d'après la relation $a_1 \Upsilon\{a, b'\}$ et d'après la fermeture (2.3, B), appliquée au (Υ, Σ)-quadrilatère $(d, m; a, b)$ (2.2.1), il est clair que $(a_1, m; a, b')$ est un (Υ, Σ)-quadrilatère. D'autre part, l'analyticité (2.3, A), appliquée également à $(d, m; a, b)$, entraîne l'existence d'un $b'' \in \mathfrak{S}$ tel que

$$m \leqq b'' \Sigma\{a_1, b\}. \tag{5}$$

Il s'ensuit que $a_1 \geqq b'' \geqq m$ et, par conséquent, on peut, en appliquant l'analyticité au (Υ, Σ)-quadrilatère $(a_1, m; a, b')$, trouver un $a_2 \in \mathfrak{S}$ tel que

$$a_1 \geqq a_2 \Upsilon\{a, b''\}. \tag{6}$$

Je dis maintenant qu'on a

$$\begin{matrix} d \Upsilon\{b, a_1\}, & d \Upsilon\{b, a_2\}, \\ b'' \Sigma\{b, a_1\}, & b'' \Sigma\{b, a_2\}. \end{matrix} \tag{7}$$

---

[3]) Pour $u, v \in \mathfrak{S}$ tels que $u \geqq v$, j'entends par u/v le *quotient* de u par v, cela veut dire ([7] Chap. I, § 1) l'ensemble de tous les $x \in \mathfrak{S}$ tels que $u \geqq x \geqq v$.

Or, les relations (7), première ligne, résultent de la fermeture appliquée au (Υ, Σ)-quadrilatère $(d, m; a, b)$ et de ce que, d'après les suppositions du lemme et d'après (6), on a $a_1 \in d/a$ et $a_2 \in d/a$.

Quant aux relations (7), deuxième ligne, la première de celles-ci résulte immédiatement de (5). Pour ce qui est de la deuxième, elle résulte de ce que, *toujours d'après* (5) *et d'après la première relation de* (7)[4]), le quadrilatère $(d, b''; a_1, b)$ est également un (Υ, Σ)-quadrilatère, auquel il ne reste plus qu'à appliquer la fermeture, compte tenu de ce que, d'après (6), on a $a_2 \in a_1/b''$.

Maintenant, on tire des (7) et de la $\mathcal{G}$-distributivité, l'égalité $a_1 = a_2$ laquelle, d'après (6), entraîne la relation

$$a_1 \Upsilon \{a, b''\}. \tag{6'}$$

Or, d'après la fermeture appliquée au (Υ, Σ)-quadrilatère $(d, m; a, b)$ on a encore

$$m \Sigma \{a, b'\}, \quad m \Sigma \{a, b''\}. \tag{8}$$

Les relations (6'), (8) et la supposition $a_1 \Upsilon \{a, b'\}$ prouvent, d'après la $\mathcal{G}$-distributivité, qu'on a $b' = b''$ ce qui, d'après (5), entraîne $b' \Sigma \{a_1, b\}$. Ceci achève la démonstration du lemme.

3.2. Je démontre maintenant le théorème. Il s'agit de prouver que les relations (1), (2), (3) entraînent la relation (4). (Je remarque en passant que, d'après le lemme 3.1, les relations (3) ne sont pas toutes indépendantes les unes des autres; ainsi, par exemple, les deux dernières sont toujours une conséquence des deux premières, etc.)

Or, d'après les suppositions (1)—(3) et d'après la fermeture, les quadrilatères $(d, a'; a, b_1)$ et $(a_1, m; a, b')$ sont des (Υ, Σ)-quadrilatères; il s'ensuit d'après l'analyticité appliquée à ces (Υ, Σ)-quadrilatères respectivement, les relations

$$a' \leqq x_1 \Sigma \{a_1, b_1\}, \quad a_1 \geqq x' \Upsilon \{a', b'\}, \quad (x_1, x' \in \mathfrak{S}), \tag{9}$$

ce qui, d'après le lemme 3.1, appliqué aux mêmes $(d, a'; a, b_1)$ et $(a_1, m; a, b')$ respectivement, entraîne

$$a_1 \Upsilon \{a, x_1\}, \quad a' \Sigma \{a, x'\}. \tag{10}$$

D'autre part, on a, compte tenu des (9) et de la fermeture appliquée toujours aux (Υ, Σ)-quadrilatères $(d, a'; a, b_1)$ et $(a_1, m; a, b')$,

$$a' \Sigma \{a, x_1\}, \quad a_1 \Upsilon \{a, x'\}. \tag{10'}$$

---

[4]) Argument de M. Gábor Szász (lettre à l'auteur, le 15 juillet 1960). Mon argument originel faisait inutilement intervenir ici la propriété de fermeture (appliquée à $(d, m; a, b)$).

Maintenant, on tire de (10), (10′) et de la $\mathcal{G}_f$-distributivité, l'égalité $x_1 = x'(= x)$ ce qui, d'après (9), prouve que $x \in (a_1/b') \cap (b_1/a')$. Ceci achève la démonstration du théorème.

3.3. Remarque. On peut montrer, en s'appuyant toujours sur la $\mathcal{G}_f$-distributivité, que l'ensemble (non vide) $(a_1/b') \cap (b_1/a')$ n'a qu'un seul élément.

Le développement complet de ces questions forme l'objet de la troisième partie de mon travail *in extenso* sur la théorie des structures géométriques des configurations, où je traite de la classification et des propriétés des structures géométriques distributives.

Remarque (ajoutée le 13 février 1961). M. GÁBOR SZÁSZ m'a fait signaler que la propriété de $(d, b''; a_1, b)$ d'être un (Γ, Σ)-quadrilatère découle directement de (5) et de la première assertion de (7).

Références

[1] M. BENADO, Sur la théorie générale des ensembles partiellement ordonnés. (Rapport destiné au Colloque international de Théorie des ensembles ordonnés, Oberwolfach, 26—30 Octobre 1959.) *Publ. Sci. Univ. Alger*, 7 (1960).

[2] ——— Sur la théorie générale des ensembles partiellement ordonnés, *Comptes Rendus Acad. Sci. Paris*, **247** (1958), 2265—2268.

[3] ——— Les ensembles partiellement ordonnés et le théorème de raffinement de Schreier. II (Théorie des multistructures), *Czechoslov. Math. Journal*, **5 (80)** (1955), 308—344.

[4] ——— La théorie des multitreillis et son rôle en Algèbre et en Géométrie. (Rapport destiné au Colloque international de Théorie des ensembles ordonnés, Oberwolfach, 26—30 Octobre 1959.) *Publ. Sci. Univ. Alger*, 7 (1960).

[5] ——— Bemerkungen zur Theorie der Vielverbände. IV (Über die Möbius'sche Funktion), *Proceedings Cambridge Phil. Soc.*, **56** (1960), 291—317.

[6] ——— Sur la fonction de Möbius, *Comptes Rendus Acad. Sci. Paris*, **246** (1958), 863—865. Voir aussi *ibid.*, 2553—2555.

[7] G. BIRKHOFF, *Lattice Theory*, revised edition (New York, 1948).

(Reçu le 4 juillet 1960)

Sums of normal endomorphisms. II

By R. H. BRUCK in Madison (Wisconsin, U. S. A.)[1])

Dedicated to L. Rédei on his sixtieth birthday

1. Introduction. The subject of this paper is (associative) rings of endomorphisms. However, the ring elements are not endomorphisms of groups but of loops, and the reader will need some acquaintance with loop theory — as given, for example, in [1].

Let G be any loop and let $\mathfrak{N}$ be the multiplicative semigroup of all normal endomorphisms of G (for the definition, see [1], [2] or [3]). Also let $\mathfrak{R}$ be the loop additively generated by $\mathfrak{N}$, where the operation is addition of single-valued mappings of G into G. In an earlier paper [3] of like title we found a necessary and sufficient condition (namely, power-associativity of G) in order that $\mathfrak{R}$ should be an associative ring (in the ordinary sense) with respect to addition and multiplication of mappings. However, $\mathfrak{R}$, even when it is a ring, need not consist only of endomorphisms (though see Theorem 6.1 below) and, a fortiori, need not be contained in $\mathfrak{N}$.

In the present paper we are primarily concerned with rings contained wholly within $\mathfrak{N}$. The following result is typical:

The set $\mathfrak{N}$ of all normal endomorphisms of the loop G contains a unique maximal (associative) ring $\mathfrak{S}$, namely the set $\mathfrak{S}$ of all θ in $\mathfrak{N}$ such that $2\theta = \theta + \theta$ is also in $\mathfrak{N}$. (Theorem 5.1.)

Clearly the defining condition for $\mathfrak{N}$ is a necessary condition that the element θ of $\mathfrak{N}$ be contained in a ring of elements of $\mathfrak{N}$. On the way toward Theorem 5.1 we also prove the following (as a special case of Theorem 3.2): *If θ, φ are in $\mathfrak{N}$, a necessary and sufficient condition that $\theta + \varphi$ be in $\mathfrak{N}$ is that $2\theta\varphi$ be in $\mathfrak{N}$* (that is, that $\theta\varphi$ be in $\mathfrak{S}$.)

When G is a group, the ring $\mathfrak{S}$ of Theorem 5.1 is the ring of centralizing endomorphisms of G. When G is a loop, $\mathfrak{S}$ contains the ring of

[1]) The research for this paper was done in Frankfurt am Main, Germany, with the support of grants from the National Science Foundation, U. S. A., and from the Graduate Research Committee of the University of Wisconsin.

centralizing endomorphisms of G but can be much larger. Indeed, in § 4, as an essential part of our investigation, we consider *the loops G for which* $\mathfrak{S} = \mathfrak{N}$. One characterization of such loops (among several given in Theorem 4.1) is in terms of the following two conditions:

(i) *The mapping $x \to x^2x$ is a semi-normal endomorphism of G.*

(ii) *The mapping $x \to x^2$ is a semi-normal endomorphism of G which maps G into $C(G) \cap Z_2(G)$.*

(For the definitions of a *semi-normal* endomorphism, of the *Moufang centre*, $C(G)$, and of the *second centre*, $Z_2(G)$, of a loop G, see [2].)

It may be remarked that conditions (i), (ii) are satisfied, on the one hand, by the commutative Moufang loops which are centrally nilpotent of class at most two — a relatively restricted class, containing, however, all abelian groups — and, on the other hand, by the loops of exponent two — a large and as yet little known class of loops. (In this connection, see the remarks in § 4.) The latter class of loops turns up in another way, which we shall now explain.

Let $\mathfrak{N}'$ be the set of all strongly normal endomorphisms of the loop G. (For the definition and properties of $\mathfrak{N}'$, see [2]; we remark here that $\mathfrak{N}'$ is part, but not always all, of $\mathfrak{N}$, and that every element of N is a sum of two elements of $\mathfrak{N}'$.) Theorem 5.1 (quoted above) has an exact counterpart for $\mathfrak{N}'$:

The set $\mathfrak{N}'$ of all strongly normal endomorphisms of the loop G contains a unique maximal (associative) ring $\mathfrak{S}'$, namely the set $\mathfrak{S}'$ of all θ in $\mathfrak{N}'$ such that $2\theta = \theta + \theta$ is also in $\mathfrak{N}'$. (Theorem 5.2.)

When $\mathfrak{S}' = \mathfrak{N}'$, then $\mathfrak{S}' = \mathfrak{S} = \mathfrak{N}$. A necessary and sufficient condition that $\mathfrak{S}' = \mathfrak{N}'$ for a loop G is (see Theorem 4.2) that

(iii) *the mapping $x \to x^2$ of G is an endomorphism of G into its centre $Z(G)$.*

The condition (iii) implies, in particular, that $G/Z(G)$ is a loop of exponent two. A construction (in terms of central extensions) of the loops G satisfying (iii) is given at the end of § 4.

The methods of the paper take account of other possibilities. For example, if G is a Moufang (and hence power-associative) loop, it is shown in [2] that the ring $\mathfrak{R}$ of our second paragraph has the property that an endomorphism θ of G is in $\mathfrak{R}$ if and only if θ is semi-normal. Thus, in the case of an arbitrary loop G, the question arises as to what endomorphisms of G can be generated by normal endomorphisms of G. As a start on this question, we determine necessary and sufficient conditions that the sum, $\theta + \varphi$, of two normal endomorphisms θ, φ of G should be an endomorphism

of G (Theorem 2.1) and should be semi-normal, weakly normal or normal (Theorem 3.1). In each case, $\theta+\varphi$ has the same "type" as $2\theta\varphi$. Thus, for example, *the loops for which the sum of every two normal endomorphisms is an endomorphism are precisely those satisfying the identical relation*

$$(xy)^2 = x^2y^2. \tag{1.1}$$

And $\theta+\varphi$ is an endomorphism of the loop G (for θ, φ normal endomorphisms of G) precisely when $G\theta\varphi$ satisfies the identical relation (1.1).

Let us mention here a special class of loops satisfying (1.1). If the loop G is *di-associative* (that is, if every two elements of G generate a group) then (1.1) holds precisely when G is commutative. On the other hand, if G is commutative and di-associative, and if $\mathfrak{N}$ is the ring of our second paragraph, then $\mathfrak{N}$ consists entirely of endomorphisms (Theorem 6.1). But, without further hypotheses, we are unable to say much about the nature of the endomorphisms in $\mathfrak{N}$.

At the present time we have no adequate tools for studying the class of all loops satisfying (1.1). Consequently, in § 4, we impose additional hypotheses. In Lemma 4.1 we assume that the mapping $x \to x^2$ of the loop G is a semi-normal endomorphism. Then G is power-associative and the commutator-associator subloop, G', has exponent dividing six. If we assume still further (to give one of several equivalent conditions) that the mapping $x \to x^3$ is a semi-normal endomorphism, then (Lemma 4.3) every power-mapping $(n): x \to x^n$, is a semi-normal endomorphism of G. Moreover, (n) is centralizing if $n \equiv 0 \bmod 6$, (n) is strongly normal if $n \equiv 0$ or $1 \bmod 3$, and (n) has the same "type" as (2) if $n \equiv 2 \bmod 3$. — All of these conclusions are true (in slightly stronger form) for arbitrary commutative Moufang loops but not (I believe) for arbitrary commutative di-associative loops. — The conditions that (2) be normal or strongly normal (given in Lemma 4.3) then lead to the characterizations, given above, of the loops G for which $\mathfrak{S} = \mathfrak{N}$ or $\mathfrak{S}' = \mathfrak{N}'$.

We shall end this introduction with an unsolved problem. It seems likely that if G is a (necessarily) power-associative loop all of whose power-mappings are semi-normal endomorphisms, then the ring $\mathfrak{N}$ generated by the normal endomorphisms consists entirely of endomorphisms, and probably of semi-normal endomorphisms.

2. The word f_4. We define the loop word f_4 as follows:

$$(X_1X_2)(X_3X_4) = [(X_1X_3)(X_2X_4)] \cdot f_4(X_1, X_2, X_3, X_4). \tag{2.1}$$

As pointed out in [2], the word f_4 is important in the study of sums of endomorphisms. Specifically, Lemma 3.1 of [2] can be phrased as follows:

Lemma 2.1. *Let θ, φ, ψ be single-valued mappings of a loop G into itself, such that*

(i) $\theta + \varphi = \psi$;

(ii) *some two of θ, φ, ψ are endomorphisms of G.*

A necessary and sufficient condition that the remaining mapping be an endomorphism of G is that

$$f_4(x\theta, x\varphi, y\theta, y\varphi) = 1 \tag{2.2}$$

for all x, y in G.

The word f_4 is purely non-abelian but not normalized. (For the definition of these terms, see [2].) Our first step here is to express f_4 in terms of normalized, purely non-abelian loop words. In addition to the commutator-word, (X_1, X_2), and the associator-word, (X_1, X_2, X_3), we need a second type of associator-word, A, and three additional words, g_3, h_3, k_4. The definitions are as follows, in terms of an auxiliary word P:

$$X_1X_2 = [X_2X_1]\cdot(X_1, X_2), \tag{2.3}$$

$$(X_1X_2)X_3 = [X_1(X_2X_3)]\cdot(X_1, X_2, X_3), \tag{2.4}$$

$$X_1(X_2X_3) = [(X_1X_2)X_3]\cdot A(X_1, X_2, X_3), \tag{2.5}$$

$$(X_1X_2)X_3 = [(X_1X_3)X_2][(X_2, X_3)\cdot g_3(X_1, X_2, X_3)], \tag{2.6}$$

$$X_1(X_2X_3) = [X_2(X_1X_3)][(X_1, X_2)\cdot h_3(X_1, X_2, X_3)], \tag{2.7}$$

$$f_4(X_1, X_2, X_3, X_4) = \tag{2.8}$$

$$= [(X_2, X_3)\cdot g_3(X_1, X_2, X_3)][(X_1, X_2, X_4)\cdot P(X_1, X_2, X_3, X_4)],$$

$$P(X_1, X_2, X_3, X_4) = A(X_1, X_3, X_4)\cdot[h_3(X_2, X_3, X_4)\cdot k_4(X_1, X_2, X_3, X_4)]. \tag{2.9}$$

Here (2.8), (2.9) together express f_4 in terms of the commutator and associator words and the words A, g_3, h_3, k_4. That the commutator and associator words, together with A, are both purely non-abelian and normalized is evident from (2.3), (2.4), (2.5). From (2.6), (2.7), g_3 and h_3 are certainly purely non-abelian. To see that they are normalized, we need only note that they vanish (i.e., take the value 1) when any one of X_1, X_2, X_3 is replaced by 1. Next we compare (2.1), (2.8). Since f_4, g_3 are purely non-abelian, so is P. Therefore, by (2.9), k_4 is also purely non-abelian. To see that k_4 is normalized, we proceed as follows: In (2.1) we replace X_4, X_3, X_2, X_1 in turn by 1 and compare with (2.6), (2.4), (2.5), (2.7) respectively, getting

$$f_4(X_1, X_2, X_3, 1) = (X_2, X_3)\cdot g_3(X_1, X_2, X_3), \tag{2.10}$$

$$f_4(X_1, X_2, 1, X_4) = (X_1, X_2, X_4), \qquad f_4(X_1, 1, X_3, X_4) = A(X_1, X_3, X_4),$$

$$f_4(1, X_2, X_3, X_4) = (X_2, X_3)\cdot h_3(X_2, X_3, X_4).$$

From (2.10) in (2.8) we get

$$
\begin{aligned}
P(X_1, X_2, X_3, 1) &= 1, \\
P(X_1, X_2, 1, X_4) &= 1, \\
P(X_1, 1, X_3, X_4) &= A(X_1, X_3, X_4), \\
P(1, X_2, X_3, X_4) &= h_3(X_2, X_3, X_4).
\end{aligned} \tag{2.11}
$$

And (2.11), (2.9) show us that k_4 is normalized. To sum up:

Lemma 2.2. *The commutator and associator words, and the words A, g_3, h_3, k_4 are normalized, purely non-abelian loop words, and f_4 is expressible (by (2.8), (2.9)) as a product in these words.*

Remark. The words A, g_3, h_3, k_4 were found from f_4 by applying the method, described in [3], of expressing a purely non-abelian word in terms of essentially normalized purely non-abelian words.

Our first use of the formula just discussed is to prove the following:

Lemma 2.3. *Let θ, φ be normal endomorphisms of the loop G. Then, for all x, y in G,*

$$f_4(x\theta, x\varphi, y\theta, y\varphi) = f_4(x, x, y, y)\theta\varphi, \tag{2.12}$$

$$f_4(x, x, y, y)\theta = f_4(x, x, y, y)\theta^2, \tag{2.13}$$

$$f_4(x, x, y, y)\theta\varphi = f_4(x, x, y, y)\varphi\theta. \tag{2.14}$$

Proof. Since the formula obtained from (2.8), (2.9) by eliminating P is too long to be displayed conveniently, our proof will be given in slightly imprecise terms. These the reader should be able to interpret correctly.

Substituting $x\theta, x\varphi, y\theta, y\varphi$ for X_1, X_2, X_3, X_4 respectively in (2.8), (2.9), we see that the left-hand side of (2.12) is a (precisely defined) product of the following:

$$
\begin{aligned}
(x\varphi, y\theta) &= (x, y)\theta\varphi, \\
g_3(x\theta, x\varphi, y\theta) &= g_3(x, x, y)\theta^2\varphi, \\
(x\theta, x\varphi, y\varphi) &= (x, x, y)\theta\varphi^2, \\
A(x\theta, y\theta, y\varphi) &= A(x, y, y)\theta^2\varphi, \\
h_3(x\varphi, y\theta, y\varphi) &= h_3(x, y, y)\theta\varphi^2, \\
k_4(x\theta, x\varphi, y\theta, y\varphi) &= k_4(x, x, y, y)\theta^2\varphi^2.
\end{aligned} \tag{2.15}
$$

To prove (2.12) we need only show that, on the right-hand sides of the equations in (2.15), each of $\theta^2\varphi$, $\theta\varphi^2$ and $\theta^2\varphi^2$ has the same effect as $\theta\varphi$. The method is the same in each case, and we treat only one example.

The word W_2 defined by

$$W_2(X, Y) = g_3(X, X, Y)$$

is normalized and purely non-abelian. Thus, since θ is a normal endomorphism, we have, for all x, y in G,

$$W_2(x, y)\theta = W_2(x\theta, y\theta) = W_2(x, y)\theta^2.$$

Similarly, since θ and φ are normal endomorphisms,

$$W_2(x, y)\theta\varphi = W_2(x\theta, y\varphi) = W_2(x, y)\varphi\theta.$$

This is enough — since the normal endomorphisms form a multiplicative semigroup — to indicate how to complete the proof of Lemma 2.3.

The next lemma is mainly included as a simple application of Lemma 2.3. We recall that a loop G is *di-associative* if, for every two elements x, y of G, the subloop generated by x and y is a group.

Lemma 2.4. *Let θ, φ be normal endomorphisms of the loop G such that the subloop $G\theta\varphi$ is commutative and di-associative. Then $\theta+\varphi = \varphi+\theta$ is an endomorphism of G.*

Proof. For any x in G, $(x\theta, x\varphi) = (x, x)\theta\varphi = 1$; and this implies that $\theta+\varphi = \varphi+\theta$. By two applications of (2.12),

$$f_4(x\theta, x\varphi, y\theta, y\varphi) = f_4(x\theta\varphi, x\theta\varphi, y\theta\varphi, y\theta\varphi) = 1,$$

the last step following directly from (2.1) and the fact that $x\theta\varphi, y\theta\varphi$ lie in an abelian group. Consequently, by Lemma 2.1, $\theta+\varphi$ is an endomorphism of G.

We shall need two more lemmas concerning f_4.

Lemma 2.5. *If θ is a normal endomorphism of the loop G, then*

$$f_4(x\theta, x\theta, y\theta, z\theta) = f_4(x\theta, x\theta, y, z) \tag{2.16}$$

for all x, y, z in G.

Proof. The proof is very similar to that of Lemma 2.3. To save space, we list below the six terms of which the left-hand side of (2.16) is a product, and transform these into six terms of which the right-hand side of (2.16) is a similar product:

$$\begin{gathered}
(x\theta, y\theta) = (x, y)\theta = (x\theta, y), \\
g_3(x\theta, x\theta, y\theta) = g_3(x, x, y)\theta = g_3(x\theta, x\theta, y), \\
(x\theta, x\theta, z\theta) = (x, x, z)\theta = (x\theta, x\theta, z), \\
A(x\theta, y\theta, z\theta) = A(x, y, z)\theta = A(x\theta, y, z), \\
h_3(x\theta, y\theta, z\theta) = h_3(x, y, z)\theta = h_3(x\theta, y, z), \\
k_4(x\theta, x\theta, y\theta, z\theta) = k_4(x, x, y, z)\theta = k_4(x\theta, x\theta, y, z).
\end{gathered} \tag{2.17}$$

Here we need to make some remarks. In each of the formulas (2.17), the left-hand term is equal to the middle term merely on the ground that θ is an endomorphism of G. In the case of the first, fourth and fifth formulas of (2.17), we get from the middle term to the ringht-hand term by straightforward use of the normality of θ. For the second, third and sixth formulas a slight variation is necessary. If W_2 is defined by

$$W_2(X, Y) = g_3(X, X, Y),$$

then W_2 is normalized and purely non-abelian. Hence

$$g_3(x, x, y)\theta = W_2(x, y)\theta = W_2(x\theta, y) = g_3(x\theta, x\theta, y).$$

Similarly in the remaining cases. This proves Lemma 2.5.

At this point we recall that the *Moufang centre*, $C(G)$, of a loop G, consists of all a in G such that

$$(aa)(yz) = (ay)(az) \tag{2.18}$$

for all y, z in G. It is shown in [2] that $C(G)$ is a (commutative, Moufang) subloop of G and that $C(G)$ has an important rôle in the theory of normal endomorphisms.

Lemma 2.6. *Let θ be a normal endomorphism of the loop G and let a be an element of G. Then each of the following statements implies the other:*

(i) *$a\theta$ lies in the Moufang centre $C(G\theta)$ of $G\theta$.*

(ii) *$a\theta$ lies in the Moufang centre $C(G)$ of G.*

Proof. We note, in view of (2.1), that (2.18) is equivalent to

$$f_4(a, a, y, z) = 1. \tag{2.19}$$

On the other hand, by Lemma 2.5,

$$f_4(a\theta, a\theta, y\theta, z\theta) = f_4(a\theta, a\theta, y, z). \tag{2.20}$$

Thus (i) holds precisely when the left side of (2.20) vanishes for all y, z in G; and (ii) holds precisely when the right side of (2.20) vanishes for all y, z in G. This completes the proof of Lemma 2.6.

Now we are ready for some initial theorems. From Lemma 2.3 we deduce the following:

Theorem 2.1. *Let θ, φ be normal endomorphisms of the loop G. Then each of the following statements implies the other two:*

(i) *$\theta + \varphi$ is an endomorphism of G.*

(ii) *$2\theta\varphi = \theta\varphi + \theta\varphi$ is an endomorphism of G.*

(iii) *If α, β are elements of the multiplicative semigroup generated by θ, φ and the identity mapping of G, and if $\alpha\beta$ contains each of θ and φ as a factor, then $\alpha+\beta$ is an endomorphism of G.*

Proof. The hypotheses on α and β in (iii) ensure that α and β are normal endomorphisms of G. Hence, by Lemma 2.3,

$$f_4(x\alpha, x\beta, y\alpha, y\beta) = f_4(x, x, y, y)\alpha\beta. \tag{2.21}$$

Since $\alpha\beta$ is a product formed from θ and φ, and contains each of θ and φ as a factor, then, by Lemma 2.3 again,

$$f_4(x, x, y, y)\alpha\beta = f_4(x, x, y, y)\theta\varphi.$$

Therefore the left-hand side of (2.21) is independent of the particular choice of α and β. In particular, $\alpha=\theta, \beta=\varphi$ and $\alpha=\beta=\theta\varphi$ are two admissible choices for α, β; another is $\alpha=1, \beta=\varphi\theta$, for example. However, by Lemma 2.1, a necessary and sufficient condition that $\alpha+\beta$ be an endomorphism of G is that

$$f_4(x\alpha, x\beta, y\alpha, y\beta) = 1$$

for all x, y in G. This completes the proof of Theorem 2.1.

As a corollary of Theorem 2.1 we obtain the following:

Theorem 2.2. *Let G be a loop, let $\mathfrak{N}$ be the set of all normal endomorphisms of G, and let $\mathfrak{S}^*$ be the set of all θ in $\mathfrak{N}$ such that $2\theta = \theta+\theta$ is an endomorphism of G. Then each of the following statements implies all the others:*

(i) *θ is in $\mathfrak{S}^*$.*

(ii) *θ is in $\mathfrak{N}$ and $1+\theta$ is an endomorphism of G.*

(iii) $\theta\mathfrak{N} \subset \mathfrak{S}^*$.

(iv) $\mathfrak{N}\theta \subset \mathfrak{S}^*$.

(v) *$\theta \in \mathfrak{N}$, and $\theta+\varphi, \varphi+\theta$ are endomorphisms of G for every θ in $\mathfrak{N}$.*

Proof. Let θ, φ be in $\mathfrak{N}$. By Theorem 2.1, if one of $\theta+\varphi$, $\varphi+\theta$, $2\theta\varphi$, $2\varphi\theta$ is an endomorphism of G, all are. Taking $\varphi=1$, we see the equivalence of (i), (ii). We also see that each of (iii), (iv), (v) implies (i). Keeping φ general, we see that (i) implies (iii), (iv) and (v). This completes the proof of Theorem 2.2.

There is still another corollary of interest:

Theorem 2.3. *Let G be a loop. Then a necessary and sufficient condition that the sum of every two normal endomorphisms of G be an endomorphism of G is that the square-mapping (2), defined by*

$$x(2) = x^2, \qquad \text{all } x \in G, \tag{2.22}$$

be an endomorphism of G; that is, that G satisfy the identical relation

$$(xy)^2 = x^2y^2. \tag{2.23}$$

Proof. In the notation of Theorem 2.2, $\mathfrak{S}^* = \mathfrak{N}$ if and only if the identity mapping 1 is in $\mathfrak{S}^*$. And 1 is in $\mathfrak{S}^*$ if and only if the mapping (2) is an endomorphism of G.

Remark. If θ is an endomorphism of a loop G,

$$\theta(2) = (2)\theta = 2\theta.$$

Hence the study of the $\mathfrak{S}^*$ of Theorem 2.2 is equivalent to the study of those normal endomorphisms θ of G with the property that the sum of every two normal endomorphisms of $G\theta$ is an endomorphism of $G\theta$.

3. Normality of sums. In studying the question of "normality" of a given endomorphism θ of a loop G, we have to consider the validity of equations of the type

$$W_n(x_1\theta, x_2, \ldots, x_n) = W_n(x_1, x_2, \ldots, x_n)\theta, \tag{3.1}$$

required to hold for all $x_1, \ldots, x_n$ in G. Here W_n is a normalized purely non-abelian word. For θ to be normal, (3.1) must hold for all choices of W_n. For θ to be weakly normal or semi-normal, (3.1) must hold for choices of W_n prescribed by the definitions. (See [2].)

In view of Theorems 2.1, 2.2, the next lemma seems natural. We suppose given a normalized, purely non-abelian word W_n. Then the word $F = F_{n+1}$, defined by

$$\begin{aligned} &W_n(XY, Z_2, \ldots, Z_n) = \\ &= [W_n(X, Z_2, \ldots, Z_n)\, W_n(Y, Z_2, \ldots, Z_n)]\, F(X, Y, Z_2, \ldots, Z_n), \end{aligned} \tag{3.2}$$

is also normalized and purely non-abelian.

Lemma 3.1. *Let θ, φ be normal endomorphisms of the loop G. Let α, β be elements of the multiplicative semigroup generated by θ, φ and the identity mapping of G, such that $\alpha\beta$ contains both θ and φ as factors. Then, for all $x, z_2, \ldots, z_n$ in G,*

$$\begin{aligned} &W_n(x(\alpha+\beta), z_2, \ldots, z_n) = \\ &= [W_n(x, z_2, \ldots, z_n)(\alpha+\beta)]\, [F(x, x, z_2, \ldots, z_n)\theta\varphi]. \end{aligned} \tag{3.3}$$

Proof. We recall that if a is any element of the commutator-associator subloop, G', of G, then

$$a\theta = a\theta^3, \quad a\theta\varphi = a\varphi\theta$$

for all normal endomorphisms θ, φ of G. Again, if $x, y, z_2, \ldots, z_n$ are arbitrary

elements of G, the elements

$$a = W_n(x, z_2, \ldots, z_n), \quad b = F(x, y, z_2, \ldots, z_n)$$

are in G'. Since

$$a\theta = W_n(x, z_2, \ldots, z_n)\theta = W_n(x\theta, z_2\theta, \ldots, z_n\theta) = a\theta^n,$$

we see from (3.2) that

$$b\theta = b\theta^n.$$

But, equally, since $F = F_{n+1}$,

$$b\theta = b\theta^{n+1}.$$

Since one of $n, n+1$ is even, and since

$$b\theta^2 = b\theta^4,$$

we deduce that

$$b\theta = b\theta^2$$

for every normal endomorphism θ. Thus also, if α, β are defined as in Lemma 3.1,

$$b\alpha\beta = b\theta\varphi.$$

As a particular case of this we have

$$(3.4) \quad F(x\alpha, x\beta, z_2, \ldots, z_n) = F(x, x, z_2, \ldots, z_n)\alpha\beta = F(x, x, z_2, \ldots, z_n)\theta\varphi.$$

Now we substitute $x\alpha, x\beta, z_2, \ldots, z_n$ for $X, Y, Z_2, \ldots, Z_n$ respectively in (3, 2), note that $(x\alpha)(x\beta) = x(\alpha+\beta)$, and use (3.4). The result is (3.3). This completes the proof of Lemma 3.1.

Combining Lemma 3.1 with Theorem 2.1, we get the following:

Theorem 3.1. *Let θ, φ be normal endomorphisms of the loop G. Let α, β be elements of the multiplicative semigroup generated by θ, φ and the identity mapping of G, such that $\alpha\beta$ contains both θ and φ as factors. If any one of $\theta+\varphi$, $2\theta\varphi$, $\alpha+\beta$ is a semi-normal (or weakly normal, or normal) endomorphism of G, then all are.*

As a special case (cf. the proof of Theorem 2.2):

Theorem 3.2. *Let $\mathfrak{N}$ be the set of all normal endomorphisms of the loop G. Let P be any fixed one of the properties of being a semi-normal, weakly normal or normal endomorphism of G. Let $\mathfrak{S}(P)$ be the set of all θ in $\mathfrak{N}$ such that $2\theta = \theta+\theta$ has property P. Then each of the following statements implies all the others:*

(i) $\theta \in \mathfrak{S}(P)$.

(ii) $\theta \in \mathfrak{N}$, *and* $1+\theta$ *has property* P.

(iii) $\theta\mathfrak{N} \subset \mathfrak{S}(P)$.
(iv) $\mathfrak{N}\theta \subset \mathfrak{S}(P)$.
(v) $\theta \in \mathfrak{N}$, *and* $\theta+\varphi, \varphi+\theta$ *have property* P *for every* $\varphi \in \mathfrak{N}$.

As another special case (cf. the proof of Theorem 2.3):

Theorem 3.3. *Let G be a loop. If the square-mapping,* (2), *of G is a semi-normal, weakly normal or normal endomorphism of G, then (and only then) the sum of every two normal endomorphisms of G has the corresponding property.*

4. The square-mapping. Theorems 2.2, 2.3 suggest that we consider next a loop satisfying the identical relation

$$(xy)^2 = x^2y^2, \tag{4.1}$$

which means that the square-mapping (2): $x \to x^2$ is an endomorphism. However, we shall impose the stronger conditions appropriate to Theorems 3.2, 3.3.

Lemma 4.1. *Let the square-mapping* (2) *be a semi-normal endomorphism of the loop G. Then:*

(i) *G is power-associative;*
(ii) *the commutator-associator subloop G' has exponent dividing six;*
(iii) *G satisfies the identical relations*

$$(x^2, y) = (x, y)^2 = 1, \tag{4.2}$$

$$(x^2, y, x) = (x, y^2, x) = (x, y, x^2) = (x, y, x)^2 = 1, \tag{4.3}$$

$$(x^2, y, z)^3 = (x, y^2, z)^3 = (x, y, z^2)^3 = (x, y, z)^6 = 1. \tag{4.4}$$

Proof. The main difficulty is the proof of (i), and for this we need neither (ii) nor the identity (4.4). Hence we begin by temporarily assuming (i). We recall that a loop is power-associative if each subloop which can be generated by one element is a (cyclic) group.

Assume (i) and set $\theta = (2)$. Then (see [2]) θ and θ^3 coincide on G'. Consequently, $a^2 = a^8$ for each a in G'. Thus $a^6 = 1$, proving (ii). Since (2) is semi-normal and (x, y, z) is in G', formula (4.4) now follows immediately.

Now we are ready to prove (i). For each x in G and for each integer n (positive, negative or zero) we define the *right powers* x^n inductively by

$$x^0 = 1, \quad x^n x = x^{n+1}. \tag{4.5}$$

In particular, $x^1 = x$, $x^2 = xx$. To prove (4.2), we note that

$$(x^2, y) = (x, y)^2 = (x^2, y^2) = (x^2, y)^2 = (x^2, y)(x^2, y)$$

and hence

$$1 = (x^2, y) = (x, y)^2.$$

In view of (4.2),

$$(x^2y)x^2 = x^2(x^2y) = x^2(yx^2)$$

and hence

$$(x^2, y, x^2) = 1.$$

Therefore

$$(x, y, x)^2 = (x^2, y^2, x^2) = (x^2, y, x^2)^2 = 1.$$

From this, (4.3) follows immediately.

Next we need the formula

$$x^n x^2 = x^{n+2} \tag{4.6}$$

for every integer n. Since (4.6) is trivial for $n = 0$, we assume inductively that (4.6) holds for some n. First we choose y so that

$$yx^2 = x^{n+1}.$$

By this with (4.6), (4.5), (4.2), (4.3),

$$x^n x^2 = x^{n+2} = x^{n+1}x = (yx^2)x = (x^2y)x = x^2(yx) = (yx)x^2.$$

Thus

$$yx = x^n, \quad y = x^{n-1}.$$

Hence (4.6) holds for $n-1$. Again, by (4.5), (4.6),

$$(x^n x)x = x^{n+2} = x^n x^2 = x^n(xx),$$

whence

$$(x^n, x, x) = 1$$

and, by (4.3),

$$(x^n, x^2, x) = (x^n, x, x^2) = (x^n, x, x)^2 = 1.$$

The latter formulas, along with (4.6), (4.2), yield

$$x^{n+3} = x^{n+2}x = (x^n x^2)x = x^n(x^2x) = x^n(xx^2) = (x^n x)x^2 = x^{n+1}x^2.$$

Thus (4.6) also holds for $n+1$, and the inductive proof of (4.6) is complete.

We observe that

$$x^{2n} = (x^2)^n \tag{4.7}$$

is true for $n = 0$. Moreover, for every n,

$$x^{2n}x^2 = x^{2(n+1)},$$

$$(x^2)^n x^2 = (x^2)^{n+1},$$

by (4.6) and (4.5) respectively. Therefore (4.7) holds for every n.

Since (2) is an endomorphism, the right-hand side of (4.7) is a square. Thus

$$x^{2n} = (x^n)^2, \quad (x^{2n}, y) = 1 \tag{4.8}$$

for all x, y in G and all integers n. By (4.8),

$$x^n x = x x^n \tag{4.9}$$

when n is an even integer. When $n = 2k+1$, (4.8), (4.3) yield

$$x^n x = x^{2k+1} x = (x^{2k} x)x = (x x^{2k})x = x(x^{2k} x) = x x^n.$$

Therefore (4.9) holds for all n. In particular,

$$x^{-1}x = 1 = x x^{-1}, \quad (x^{-1})^{-1} = x. \tag{4.10}$$

To begin with, we prove the next formula for non-negative n:

$$x^n x^{-1} = x^{n-1}. \tag{4.11}$$

This is trivial for $n = 0$; true for $n = 1$ by (4.10); and true for $n = 2$ by (4.6) (with $n = -1$) and (4.2). We need these special cases for the proof. If (4.11) holds for some $n \geqq 2$, then

$$x^{n-1} = x^n x^{-1} = (x^{n-1} x)x^{-1} = [x^{n-1}(x x^{-1})](x^{n-1}, x, x^{-1}) = x^{n-1}(x^{n-1}, x, x^{-1}).$$

The associator clearly must be 1. Thus

$$(x^{n-1}, x^2, x^{-1}) = (x^{n-1}, x, x^{-1})^2 = 1$$

and hence, by use of (4.6),

$$x^{n+1} x^{-1} = (x^{n-1} x^2)x^{-1} = x^{n-1}(x^2 x^{-1}) = x^{n-1} x = x^n.$$

This proves (4.11) for all $n \geqq 0$. From (4.11) we deduce the formula

$$(x^{-1})^{-n} = x^n \tag{4.12}$$

as follows: Certainly (4.12) holds for $n = 0$. If (4.12) holds for some $n \geqq 0$, then (setting $y = x^{-1}$ for convenience) we use (4.12), (4.11) to get

$$y^{-n-1} y = y^{-n} = x^n = x^{n+1} y,$$

whence we see that (4.12) holds for $n+1$. Hence (4.12) holds for all $n \geqq 0$. However, on replacing x in (4.12) by its inverse, and using (4.10), we get

$$x^{-n} = (x^{-1})^n,$$

which shows that (4.12) also holds for all negative n. — At this point we could go back and prove (4.11) for all negative n, but we do not need to do so.

Now we are ready to prove the main formula:

$$x^m x^n = x^{m+n}. \tag{4.13}$$

When we say that (4.13) holds for $n = k$, we mean that (4.13) holds for $n = k$ when m takes on all integral values. Certainly (4.13) holds for $n = 0$ and $n = 1$. Moreover, (4.13) holds for $n = 2$ by (4.8). Thus we consider

some integer $k \geqq 1$ and assume inductively that (4.13) holds for $0 \leqq n \leqq 2k$. In particular, since $k+1 \leqq 2k$, (4.13) holds for $n = k$, $n = k+1$. Thus, for every integer m,

$$(x^m x^k)x = x^{m+k}x = x^{m+k+1} = x^m x^{k+1} = x^m(x^k x),$$

so that $(x^m, x^k, x) = 1$ and therefore, by (4.8), on successive squaring,

$$(x^m, x^{2k}, x) = 1 = (x^m, x^{2k}, x^2).$$

By the latter formulas and the inductive assumption,

$$x^m x^{2k+1} = x^m(x^{2k}x) = (x^m x^{2k})x = x^{m+2k}x = x^{m+2k+1}$$

and

$$x^m x^{2k+2} = x^m(x^{2k}x^2) = (x^m x^{2k})x^2 = x^{m+2k}x^2 = x^{m+2k+2}.$$

Therefore (4.13) holds for $n = 2k+1$, $n = 2k+2$ and hence for every non-negative n. To obtain (4.13) for negative n, we simply replace x in (4.13) by x^{-1} and use (4.12). This completes the proof of (4.13). Since (4.13) implies (i), the proof of Lemma 4.1 is complete.

In view of Theorem 3.3, it might seem natural to assume next that (2) is weakly normal. However, the following lemma suggests that a weaker hypothesis is more suitable. (We recall that the square of a weakly normal endomorphism is strongly normal; see [2], Corollary to Theorem 3.1.)

Lemma 4.2. *If θ is a semi-normal endomorphism of the loop G, each of the following statements implies the others*:

(i) *θ^2 is a normal endomorphism of G.*

(ii) *The complement, $\lambda = (\theta^2)'$, of θ^2, is a semi-normal endomorphism of G.*

(iii) *θ^2 is a strongly normal endomorphism of G. When* (i), (ii), (iii) *hold, $\theta\lambda$ is a centralizing endomorphism of G.*

Proof. We use the results of [2]. If θ^2 is a normal endomorphism, then λ is a normal (and hence semi-normal) endomorphism. Thus (i) implies (ii). We recall that

$$\theta^2 + \lambda = 1 = \textit{the identity mapping}$$

and hence

$$\theta^3 + \theta\lambda = \theta.$$

If θ is a semi-normal endomorphism, θ^3 and θ coincide on the commutator-associator subloop G'. Therefore $\theta\lambda$ maps G' into 1. If λ is also a semi-normal endomorphism, then $\theta\lambda$ is semi-normal. Since $\theta\lambda$ maps G' into 1, it follows that $\theta\lambda$ is a centralizing endomorphism. Then $\theta^2\lambda$ is also centralizing; and this means that θ^2 is strongly normal. Thus (ii) implies (iii); and, a fortiori, (iii) implies (i). This completes the proof of Lemma 4.2.

Now, if G is power-associative, then for each integer n, we define the power-mapping (n) of G by

$$x(n) = x^n \tag{4.14}$$

for every x in G.

Lemma 4.3. *Let* (2) *be a semi-normal endomorphism of the loop* G, *and impose one of the following conditions:*

(a) (4) *is a normal endomorphism of* G.

(b) (−3) *is a semi-normal endomorphism of* G.

(c) (3) *is a semi-normal endomorphism of* G.

Then all of (a), (b), (c) *are satisfied. Indeed,* (n) *is a semi-normal endomorphism of* G *for every integer* n. *And more is true:*

(i) *If* $n \equiv 0 \bmod 6$, (n) *is centralizing.*

(ii) *If* $n \equiv 0$ *or* $1 \bmod 3$, (n) *is strongly normal.*

(iii) *If* $n \equiv 2 \bmod 3$, (n) *is normal or strongly normal according as* (2) *is normal or strongly normal.*

(iv) *A necessary and sufficient condition that* (2) *be strongly normal is that* $G^2 \subset Z(G)$, *where* $Z(G)$ *is the centre of* G. *When* (2) *is strongly normal,* (n) *is strongly normal for every integer* n.

(v) *A necessary and sufficient condition that* (2) *be normal is that* $G^2 \subset C(G) \cap Z_2(G)$, *where* $C(G)$ *is the Moufang centre and* $Z_2(G)$ *is the second centre of* G. *When* (2) *is normal,* (n) *is normal for every integer* n.

Proof. Since the complement of (4) is (−3), the conditions (a), (b) are equivalent by Lemma 4.2. In addition, if (a) or (b) holds, $(2)(-3) = (-6)$ is a centralizing endomorphism. In this case, (6) is also a centralizing endomorphism. On the other hand, if (c) holds, then, in view of the identities (4.2), (4.4) of Lemma 4.1, $(6) = (2)(3)$ is again a centralizing endomorphism.

From this point on, we assume that (6) is a centralizing endomorphism. The following equations link together pairs of complementary mappings:

$$1 = (1) + (0) = (4) + (-3) = (3) + (-2) = (2) + (-1); \tag{4.15}$$

$$(1)(0) = 0;\ (4)(-3) = (-12);\ (3)(-2) = (-6);\ (2)(-1) = (-2). \tag{4.16}$$

And the next equations show that certain mappings differ by a centralizing endomorphism:

$$(4) = (-2) + (6);\quad (3) = (-3) + (6);\quad (5) = (-1) + (6). \tag{4.17}$$

If we assume (a) or (b), then (4) and (−3) are strongly normal endomorphisms (by Lemma 4.2). Thus, by (4.17), (3) is also a strongly normal endomorphism. If we assume (c), then, by hypotheses, (3) is a semi-normal endomorphism and hence, by (4.17), (−3) is also a semi-normal endomor-

phism; that is, (b) holds. Hence (a), (b), (c) are equivalent and we assume all three henceforth. Then, since (4) is strongly normal, (4.17) shows us that (−2) is also a strongly normal endomorphism.

Since (1) and (4) are (strongly) normal endomorphisms, then, by Theorem 3.3 and the fact that (2) is a semi-normal endomorphism, (5) = = (1) + (4) is a semi-normal endomorphism. By this and (4.17), (−1) is a semi-normal endomorphism.

If n is any integer, there exist unique integers m, k such that

$$n = m + 6k, \quad m = 0, \pm 1, \pm 2, 3. \tag{4.18}$$

We have already seen that (m) is (at least) a semi-normal endomorphism for each admissible choice of m in (4.18). Moreover, $(6k)$ is a centralizing endomorphism, since (6) is. Therefore

$$(n) = (m) + (6k)$$

is semi-normal, and (n) is normal or strongly normal according as (m) is.

If $n \equiv 0 \bmod 6$, then $m = 0$. This proves (i).

If $n \equiv 0$ or $1 \bmod 3$, then $m = 0, 1, -2$ or 3. Since (0), (1), (−2) and (3) are strongly normal endomorphisms, so is (n). This proves (ii).

If $n \equiv 2 \bmod 3$, then $m = -1$ or 2. By (4.15), (2) and (−1) are complementary; thus if one is a normal or strongly normal endomorphism, so is the other. This proves (iii).

Since (2) and (−1) are complementary and since (2)(−1) = (−2), we see that (2) is strongly normal precisely when (−2) is centralizing. However, (−2) is centralizing precisely when (2) is centralizing. This proves (iv). On the other hand, since (−2) is, in any case, strongly normal, the criterion in [2] shows that (2) will be normal precisely when (−2) maps G into

$$C(G) \cap Z_2(G).$$

Since (2) and (−2) have the same image, this proves (v) and completes the proof of Lemma 4.3.

Theorem 4.1. *Let $\mathfrak{N}$ be the set of all normal endomorphisms of the loop G. Then each of the following conditions implies the other two:*

(i) *$\mathfrak{N}$ is an associative ring under addition and multiplication of mappings.*

(ii) *The square-mapping (2) is a normal endomorphism of G.*

(iii) *The power-mappings (2) and (3) = (2) + (1) are semi-normal endomorphisms of G, and (2) maps G into $C(G) \cap Z_2(G)$. (Here $C(G)$ is the Moufang centre and $Z_2(G)$ is the second centre of G.)*

When the conditions are satisfied, G is power-associative and $6\mathfrak{N}$ consists of centralizing endomorphisms of G.

Proof. Clearly (i) implies (ii). If (ii) holds, certainly (2) is semi-normal and $(2)^2=(4)$ is normal. By Lemma 4.3, if (2) is a semi-normal endomorphism, then (4) is a normal endomorphism precisely when (3) is a semi-normal endomorphism. Moreover, when (2) and (3) are semi-normal endomorphisms, a necessary and sufficient condition that (2) be normal is that (2) map G into $C(G)\cap Z_2(G)$. Therefore (ii) and (iii) are equivalent.

Next we assume (ii), (iii). Then, by Lemma 4.1, G is power-associative. However, by the main theorem of [3], power-associativity ensures that the additive loop generated by $\mathfrak{N}$ is a ring $\mathfrak{R}$. We wish to show that $\mathfrak{N}$ coincides with $\mathfrak{R}$. Let θ, φ be in $\mathfrak{N}$. By Lemma 4.3, since (2) is normal, so is (-1). Thus the element $\theta-\varphi=\theta+(-1)\varphi$ of $\mathfrak{R}$ is a sum of two elements θ, $(-1)\varphi$ of $\mathfrak{N}$. Hence, by Theorem 3.3, $\theta-\varphi$ is in $\mathfrak{N}$. This shows that $\mathfrak{N}$ is closed under subtraction. Hence, by the definition of $\mathfrak{R}$, $\mathfrak{N}=\mathfrak{R}$. Thus (i) holds. That is, (i), (ii), (iii) are equivalent. When (i), (ii), (iii) hold, Lemma 4.3 tells us that (6) is a centralizing endomorphism. Hence $6\mathfrak{N}$ consists of centralizing endomorphisms, and the proof of Theorem 4.1 is complete.

Theorem 4.2. *Each of the following statements about the loop G implies the other two:*

(i) *The set $\mathfrak{N}'$ of all strongly normal endomorphisms of G is an associative ring under addition and multiplication of mappings. (Moreover, every normal endomorphism of G is strongly normal.)*

(ii) *The square-mapping* (2) *is a strongly normal endomorphism of G.*

(iii) *The square-mapping* (2) *is a centralizing endomorphism of G.*

Proof. Each of (i), (iii) clearly implies (ii). If (ii) holds, then, a fortiori, (2) is a normal endomorphism. Hence, by Theorem 4.1, the set $\mathfrak{N}$ of normal endomorphisms of G is a ring. Moreover, by Lemma 4.3, (iii) is precisely the condition that (2) be strongly normal. Thus (ii) and (iii) are equivalent. To show that (ii), (iii) imply (i), we proceed as follows: If θ is in $\mathfrak{N}$, with complement θ', then $\theta\theta'=\varphi$ where, according to the criterion of [2], φ is a strongly normal endomorphism which maps G into $C(G)\cap Z_2(G)$. Since $C(G)$ is commutative Moufang, (3) induces a centralizing endomorphism of $C(G)$. Thus $3\varphi=\varphi(3)$ is a centralizing endomorphism of G. However, $2\varphi=\varphi(2)$ is a centralizing endomorphism of G, since (2) is. Thus $\varphi=3\varphi-2\varphi$ is centralizing, and this means that θ is strongly normal. Hence $\mathfrak{N}=\mathfrak{N}'$. Therefore we have (i). This completes the proof of Theorem 4.2.

If (2) is a centralizing endomorphism of a loop G, then $G^2=G(2)$ is a normal subloop of G contained in the centre $Z(G)$; and G/G^2 is a loop, say T, of exponent two. We may remark that, although groups of exponent two are abelian groups, no such statement can be made about loops of

exponent two. Indeed, the class of all loops of exponent two is a very large — and not too well explored — class containing, for example, the totally symmetric loops. The latter are co-extensive with Steiner triple systems. For various contructions of loops of exponent two, see [4] and [5].

The following construction reduces the study of loops whose strongly normal endomorphisms form a ring to the study of a fairly simple type of central extension:

Construction. Let T be any multiplicative loop of exponent two, let A be any additive abelian group, and let f be any function from $T\times T$ to A satisfying the conditions

$$f(t, 1)=0=f(1, t), \tag{4.19}$$

$$f(tt', tt')+2f(t, t')=f(t, t)+f(t', t') \tag{4.20}$$

for all t, t' in T. Then let $G=(T, A; f)$ be the set of all couples (t, a), $t\in T$, $a\in A$, with equality componentwise and with multiplication defined by

$$(t, a)(t', a')=(tt', f(t, t')+a+a'). \tag{4.21}$$

If we omit (4.20), G is the most general loop such that $G^2\subset Z(G)$ and G/G^2 is homomorphic to T (where G^2 denotes the subloop — here normal in G — generated by all squares). The identity (4.20) is necessary and sufficient in order that the square-mapping of G be a (necessarily centralizing) endomorphism of G.

We shall not dwell on the theory of these central extensions; cf., e. g., [6]. In a similar way we could construct all loops G satisfying the conditions of Theorem 4.1. We first observe that, for such a loop G, $G/Z(G)$ is of the type just constructed, and hence may be obtained from a loop $(T, A; f)$ by a central extension. The conditions which must be imposed, however, are rather forbidding, in contrast to the simple condition (4.20).

5. The general case. It will be convenient to begin with two lemmas:

Lemma 5.1. *Let θ be a normal endomorphism of the loop G, and let φ be an endomorphism of $G\theta$. Let P be any one of the properties (of endomorphisms) of being semi-normal, weakly normal, normal or centralizing. Then $\theta\varphi$ has property P relative to G if and only if φ has property P relative to $G\theta$.*

Remark. The conclusion of Lemma 5.1 becomes false (if the normal endomorphism θ of G is not strongly normal) when P is taken to be the property of being strongly normal — as is clear when we choose φ to be the identity mapping of $G\theta$. This choice of P is treated in Lemma 5.2 below.

Proof. First let P be one of the properties of being semi-normal, weakly normal or normal. Then there exists a class $\mathfrak{R}$ (depending on P; see [2]) of normalized, purely non-abelian loop words such that $\theta\varphi$ has property P relative to G if and only if

$$W_n(x_1\theta\varphi, x_2, \ldots, x_n) = W_n(x_1, x_2, \ldots, x_n)\theta\varphi \tag{5.1}$$

for each W_n in $\mathfrak{R}$ and all $x_1, \ldots, x_n$ in G, whereas φ has property P relative to $G\theta$ if and only if

$$W_n(x_1\theta\varphi, x_2\theta, \ldots, x_n\theta) = W_n(x_1\theta, x_2\theta, \ldots, x_n\theta)\varphi \tag{5.2}$$

for each W_n in $\mathfrak{R}$ and all $x_1, \ldots, x_n$ in G.

If (5.1) holds, we replace $x_2, \ldots, x_n$ by $x_2\theta, \ldots, x_n\theta$, respectively, in (5.1). Then the left-hand side of (5.1) becomes the left-hand side of (5.2), whereas the right-hand side of (5.1) becomes

$$W_n(x_1, x_2\theta, \ldots, x_n\theta)\theta\varphi = W_n(x_1\theta, x_2\theta, \ldots, x_n\theta)\varphi.$$

Thus (5.1) implies (5.2). Conversely, if (5.2) holds, we replace $x_2, \ldots, x_n$ by $x_2\theta, \ldots, x_n\theta$, respectively, in (5.2). Using, the facts that

$$W_n(z, x_2, \ldots, x_n)$$

lies in the commutator-associator subloop G' and that the normal endomorphisms θ and θ^3 coincide on G', we deduce this time that

$$W_n(x_1\theta\varphi, x_2, \ldots, x_n)\theta^2 = W_n(x_1, x_2, \ldots, x_n)\theta\varphi. \tag{5.3}$$

Now we must prove that the left-hand sides of (5.3), (5.1) are equal.

We prove this as follows: Since θ is a normal endomorphism of G, then θ^2 and $\lambda = (\theta^2)'$ are strongly normal endomorphisms of G and $\theta\lambda$ is a centralizing endomorphism of G. (Compare the proof of Lemma 4.2.) If x is in G, then, since φ is an endomorphism of $G\theta$, there exists at least one y in G such that $x\theta\varphi = y\theta$. Hence the element $x\theta\varphi\lambda = y\theta\lambda$ is in the centre of G; that is, the endomorphism $\theta\varphi\lambda$ of G is centralizing. Therefore, if

$$a = W_n(x_1\theta\varphi, x_2, \ldots, x_n),$$

then

$$a\lambda = W_n(x_1\theta\varphi\lambda, x_2\lambda, \ldots, x_n\lambda) = 1$$

and

$$a = a(\theta^2 + \lambda) = (a\theta^2)(a\lambda) = a\theta^2.$$

This proves that (5.3) implies (5.1), and completes the proof that (5.1), (5.2) are equivalent identities.

There remains only the case that P is the property of being centralizing. However, an endomorphism of a loop H is centralizing precisely when it is

semi-normal and maps H' into 1. If one of $\theta\varphi$, φ is semi-normal, then both are (by the previous proof). Since, moreover, $G'\theta\varphi = (G\theta)'\varphi$, $\theta\varphi$ maps G' into 1 precisely when φ maps $(G\theta)'$ into 1. This completes the proof of Lemma 5.1.

Lemma 5.2. *If θ is a strongly normal endomorphism of a loop G and if φ is an endomorphism of $G\theta$, then $\theta\varphi$ is a strongly normal endomorphism of G precisely when φ is a strongly normal endomorphism of $G\theta$.*

Proof. Since strongly normal endomorphisms are normal, we may assume, in view of Lemma 5.1, that $\theta\varphi$ and φ are both normal. The element a of G is in G' if and only if $a\theta$ is in $(G\theta)'$. Moreover, since θ is a strongly normal endomorphism of G, $a\theta = a\theta^2$ for every a in G'. Then, for a in G',

$$a(\theta\varphi)\theta = a\theta(\theta\varphi) = a\theta^2\varphi = a\theta\varphi$$

and

$$a(\theta\varphi)^2 = (a\theta)\varphi^2.$$

Hence $(\theta\varphi)^2$ coincides with $\theta\varphi$ on G' precisely when φ^2 coincides with φ on $(G\theta)'$. In view of the properties of normal endomorphisms, this is enough to prove Lemma 5.2.

Theorem 5.1. *Let $\mathfrak{N}$ be the set of all normal endomorphisms of the loop G, and let $\mathfrak{S}$ be the set of all θ in $\mathfrak{N}$ such that $2\theta = \theta+\theta$ is in $\mathfrak{N}$. Then $\mathfrak{S}$ is a ring. Moreover:*

(i) $\mathfrak{N}+\mathfrak{S} = \mathfrak{S}+\mathfrak{N} = \mathfrak{N}$;

(ii) $\mathfrak{N}\mathfrak{S} = \mathfrak{S}\mathfrak{N} = \mathfrak{S}$;

(iii) $G^2\mathfrak{S} \subset C(G) \cap Z_2(G)$, *where $C(G)$ is the Moufang centre and $Z_2(G)$ is the second centre of G.*

Proof. By Lemma 5.1, if θ is in $\mathfrak{N}$, a necessary and sufficient condition that $2\theta = \theta+\theta = \theta(2)$ be in $\mathfrak{N}$ is that the square-mapping (2) of G induce a normal endomorphism of $G\theta$. Thus we are led to consider the class $\mathfrak{K}$ of all normal subloops H of G such that the square-mapping (2) of G induces a normal endomorphism of G/H. By Theorem 4.1, the G-normal subloop H will be in $\mathfrak{K}$ if and only if the mappings (2) and (2)+(1) of G induce semi-normal endomorphisms of G/H and, moreover,

$$G^2H/H \subset C(G/H) \cap Z_2(G/H).$$

Using these conditions, it is not hard to see that there exists a finite class, $\mathfrak{L}$, of loop words W_n such that the G-normal subloop H is in $\mathfrak{K}$ if and only if H contains $W_n(x_1, x_2, \ldots, x_n)$ for each W_n in $\mathfrak{L}$ and all $x_1, \ldots, x_n$ in G. Now it should be clear that $\mathfrak{K}$ contains a minimal element, $K = K(G)$. As a consequence, the element θ of $\mathfrak{N}$ is in $\mathfrak{S}$ if and only if $K\theta = 1$.

Hereafter, let θ be in $\mathfrak{S}$. By Theorem 4.1, applied to $G\theta$:

(a) *$G\theta$ is power-associative;*

(b) *(-1) is a normal endomorphism of $G\theta$.*

If φ, ψ are in $\mathfrak{N}$ and x is in G, then

$$(x\theta, x\varphi) = (x, x)\theta\varphi = 1, \quad (x\theta, x\varphi, x\psi) = (x, x, x)\theta\varphi\psi = 1$$

by (a), and hence

$$\theta + \varphi = \varphi + \theta, \quad (\theta + \varphi) + \psi = \theta + (\varphi + \psi).$$

By Theorem 3.2, if φ is in $\mathfrak{N}$, then $\theta + \varphi = \varphi + \theta$ is in $\mathfrak{N}$ and $\theta\varphi$, $\varphi\theta$ are in $\mathfrak{S}$. This is enough to prove (i), (ii), if we recall that $\mathfrak{N}$ contains the identity mapping of G and note that $\mathfrak{S}$ contains the zero mapping of G. In addition,

$$K(\theta + \varphi) = K\theta \cdot K\varphi = K\varphi,$$

so $\theta + \varphi$ is in $\mathfrak{S}$ precisely when φ is. Hence we see that $\mathfrak{S}$ is closed under an associative and commutative addition. Moreover, by (b) and Lemma 5.1, $\theta^* = \theta(-1)$ is a normal endomorphism of G. Since θ^*, like θ, maps K upon 1, and since $\theta + \theta^*$ is the zero mapping of G, it is now clear that $\mathfrak{S}$ is an additive abelian group. In view of (ii) and the fact that distributive laws are automatic for endomorphisms, we see finally that $\mathfrak{S}$ is a ring.

Again, $G^2\theta = G\theta(2) \subset C(G\theta) \cap Z_2(G\theta)$, by Theorem 4.1 applied to $G\theta$. By Lemma 2.6, for any θ in $\mathfrak{N}$, $G^2\theta \subset C(G\theta)$ is equivalent to $G^2\theta \subset C(G)$. Similarly, by simple calculations using commutators and associators $G^2\theta \subset Z_2(G\theta)$ is equivalent to $G^2\theta \subset Z_2(G)$. This proves (iii) and completes the proof of Theorem 5.1.

Theorem 5.2. *Let $\mathfrak{N}'$ be the set of all strongly normal endomorphisms of the loop G, and let $\mathfrak{S}'$ be the set of all θ in $\mathfrak{N}'$ such that $2\theta = \theta + \theta$ is in $\mathfrak{N}'$. Then $\mathfrak{S}'$ is a ring. Moreover:*

(i) $\mathfrak{N}' + \mathfrak{S}' = \mathfrak{S}' + \mathfrak{N}' = \mathfrak{N}'$.

(ii) $\mathfrak{N}'\mathfrak{S}' = \mathfrak{S}'\mathfrak{N}' = \mathfrak{S}'$.

(iii) *The element θ of $\mathfrak{N}'$ is in $\mathfrak{S}'$ if and only if the following two conditions are satisfied:*

$$f_4(x, x, y, y)\theta = 1 \tag{5.4}$$

for all x, y in G, and

$$G^2\theta \subset Z(G), \tag{5.5}$$

where $Z(G)$ is the centre of G.

Proof. Let θ be in $\mathfrak{N}'$. Then, by Lemma 5.2, $2\theta = \theta(2)$ is a strongly normal endomorphism of G if and only if (2) induces a strongly normal

endomorphism of $G\theta$. By Theorem 4.2 applied to $G\theta$, (2) induces a strongly normal endomorphism of $G\theta$ if and only if (2) induces a centralizing endomorphism of $G\theta$. From the definition of f_4, (2) induces an endomorphism of $G\theta$ if and only if (5.4) holds for all x, y in G. And (2) maps $G\theta$ into its centre, $Z(G\theta)$, if and only if $G^2\theta \subset Z(G\theta)$; but, since θ is (in particular) semi-normal, this latter condition is equivalent to (5.5). Therefore we have proved (iii).

If θ is in $\mathfrak{S}'$ and φ is in $\mathfrak{N}'$ then $\theta\varphi$ and $\varphi\theta$ are in $\mathfrak{N}'$ (see [2]). Also (5.4), (5.5) obviously hold with θ replaced by $\theta\varphi$ or $\varphi\theta$. This is enough to prove (ii).

At this point it will be convenient to note that if θ and 2θ are both in $\mathfrak{N}'$, then both are in $\mathfrak{N}$. Hence $\mathfrak{S}'$ is a subset of $\mathfrak{S}$. As a result, if θ is in $\mathfrak{S}'$ and φ in in $\mathfrak{N}'$, then, by Theorem 5.1, $\theta+\varphi=\varphi+\theta$ is in $\mathfrak{N}$. Also, by the preceding paragraph, $\theta\varphi$ and $\varphi\theta$ are in $\mathfrak{S}'$. Again (see [2]), $\theta\varphi$ and $\varphi\theta$ differ by a centralizing endomorphism of G. Since, in addition, $2\theta\varphi$ is a centralizing endomorphism (inasmuch as $\theta\varphi$ is in $\mathfrak{S}'$), we conclude that

$$\theta\varphi+\varphi\theta=\lambda \tag{5.6}$$

where λ is a centralizing endomorphism of G. Again (see [2]), since θ, φ are in $\mathfrak{N}'$,

$$\theta^2=\theta+\mu, \quad \varphi^2=\varphi+\nu \tag{5.7}$$

where μ, ν are centralizing endomorphisms of G. Combining (5.6), (5.7) with the fact that $\theta^2, \theta\varphi, \varphi\theta$ are in $\mathfrak{S}' \subset \mathfrak{S}$, we get

$$(\theta+\varphi)^2=(\theta+\varphi)\theta+(\theta+\varphi)\varphi=$$
$$=\theta^2+\varphi\theta+\theta\varphi+\varphi^2=\theta+\varphi+\varrho$$

where $\varrho=\lambda+\mu+\nu$ is a centralizing endomorphism of G. Now it is clear that the element $\theta+\varphi$ of $\mathfrak{N}$ is in fact in $\mathfrak{N}'$. And this is enough to prove (i).

Again let θ be in $\mathfrak{S}'$. Then $G\theta$ is power-associative and $\mathfrak{N}'(G\theta)$ is a ring. In particular, (-1) induces a strongly normal endomorphism of $G\theta$. Consequently, by Lemma 5.2, $\theta^*=\theta(-1)$ is in $\mathfrak{N}'$. Since θ^* clearly satisfies the same conditions (5.4), (5.5) as θ, we see that θ^* is in $\mathfrak{S}'$. Hence $\mathfrak{S}'$ contains the negatives of its elements.

If θ, φ are in $\mathfrak{S}'$ then $\theta+\varphi$ is in $\mathfrak{N}'$ (as shown above). Moreover, since θ and φ satisfy (5.4), (5.5), so does $\theta+\varphi$. Hence $\mathfrak{S}'$ is closed under addition. Now we have that $\mathfrak{S}'$ is an additive subgroup of $\mathfrak{S}$. By this and (ii), $\mathfrak{S}'$ is a subring of $\mathfrak{S}$. And now the proof of Theorem 5.2 is complete.

It will be noted that, in Theorem 5.2, we gave explicit necessary and sufficient conditions that θ be in $\mathfrak{S}'$. It would have been easy, in Theorem

5.1, to give explicit necessary and sufficient conditions that θ be in $\mathfrak{S}$. We refrained from doing so merely because the conditions seemed too space-consuming.

6. Rings generated by normal endomorphisms. Up until this point we have been concerned mainly with rings consisting of normal endomorphisms. Here we indicate some other possibilities by proving the following theorems:

Theorem 6.1. *Let G be a commutative, di-associative loop, let $\mathfrak{N}$ be the set of all normal endomorphisms of G, and let $\mathfrak{R}$ be the additive loop generated by $\mathfrak{N}$ under addition of mappings. Then $\mathfrak{R}$ is a ring of endomorphisms of G.*

Theorem 6.2. *Let G be an arbitrary loop, let $\mathfrak{N}$ be the set of all normal endomorphisms of G, let $\mathfrak{N}^*$ be the set of all θ in $\mathfrak{N}$ such that $G\theta$ is commutative and di-associative, and let $\mathfrak{R}^*$ be the additive loop generated by $\mathfrak{N}^*$ under addition of mappings. Then $\mathfrak{R}^*$ is a ring of endomorphisms of G. Moreover, $\mathfrak{N}\mathfrak{R}^* = \mathfrak{R}^*\mathfrak{N} = \mathfrak{R}^*$.*

Proof. Clearly Theorem 6.1 is a corollary of Theorem 6.2. Hence we need only prove Theorem 6.2. If φ is in $\mathfrak{R}^*$, there exists at least one loop word

$$F_n = F_n(X_1, X_2, \ldots, X_n)$$

and elements $\theta_1, \theta_2, \ldots, \theta_n$ of $\mathfrak{N}^*$ such that

$$\varphi = F_n(\theta_1, \theta_2, \ldots, \theta_n). \tag{6.1}$$

Moreover (compare [3]),

$$x\varphi = F_n(x\theta_1, x\theta_2, \ldots, x\theta_n) \tag{6.2}$$

for each x in G.

From F_n we define a loop word L_{2n} by

$$\begin{aligned} &F_n(X_1Y_1, X_2Y_2, \ldots, X_nY_n) = \\ &= [F_n(X_1, \ldots, X_n)\, F_n(Y_1, \ldots, Y_n)]\, L_{2n}(X_1, \ldots, X_n, Y_1, \ldots, Y_n). \end{aligned} \tag{6.3}$$

Thus L_{2n} is a member of the free multiplicative group on the $2n$ free generators $X_1, \ldots, X_n, Y_1, \ldots, Y_n$. Since L_{2n} obviously vanishes on every abelian group, L_{2n} is purely non-abelian. As a consequence, by the method in [3], L_{2n} can be built up from normalized, purely non-abelian words of form

$$W_{s+t}(X_{i_1}, \ldots, X_{i_s}, Y_{j_1}, \ldots, Y_{j_t}) \tag{6.4}$$

on some but perhaps not all of the $2n$ generators. (Here one of s, t can be

zero.) Now let x, y be arbitrary elements of G, and substitute $x\theta_k$ for X_k, $y\theta_k$ for Y_k, $k=1, 2, \ldots, n$. From the fact that each θ_k is in $\mathfrak{N}^*$ and hence in $\mathfrak{N}$, we deduce that (6.4) becomes

$$W_{s+t}(x, \ldots, x, y, \ldots, y)\theta_{i_1} \cdots \theta_{i_s}\theta_{j_1} \cdots \theta_{j_t}. \tag{6.5}$$

If θ is the product of endomorphisms appearing in (6.5), then θ is also in $\mathfrak{N}^*$. Hence, since the subloop generated by $x\theta$ and $y\theta$ is an abelian group, (6.5) must be equal to the identity. As a consequence,

$$L_{2n}(x\theta_1, \ldots, x\theta_n, y\theta_1, \ldots, y\theta_n) = 1 \tag{6.6}$$

for all x, y in G. In view of (6.2), (6.3), (6.6), we have

$$(xy)\varphi = (x\varphi)(y\varphi)$$

for all x, y in G. This proves that each element φ of $\mathfrak{N}^*$ is an endomorphism of G.

Now let us assume temporarily that G is commutative and di-associative, so that $\mathfrak{N}^* = \mathfrak{N}$ and $\mathfrak{N}^* = \mathfrak{N}$. Since di-associativity implies power-associativity, it follows from the main theorem of [3] that $\mathfrak{N}^* = \mathfrak{N}$ is a ring. This completes the proof of Theorem 6.1.

In the general case of Theorem 6.2, we still have to prove that $\mathfrak{N}^*$ is a ring. As a first step, we must show that the additive loop $A = (\mathfrak{N}^*, +)$ of $\mathfrak{N}^*$ is an abelian group. For this it is enough to show that if φ, given by (6.1), is in the commutator-associator subloop A' of A, then $\varphi = 0$. However, if φ is in A', we can always suppose that F_n is in the commutator-associator subloop of the free loop on $X_1, \ldots, X_n$. This means that F_n is purely non-abelian. But then, by a simplication of the proof of (6.6) — this time using only power-associativity — we get (cf. [3])

$$x\varphi = F_n(x\theta_1, \ldots, x\theta_n) = 1$$

for all x in G. This means that A is an abelian group.

Next let $\theta_1, \ldots, \theta_n$ be arbitrary elements of $\mathfrak{N}^*$, let φ be any element of $\mathfrak{N}^*$, given by (6.1), and let θ be any element of $\mathfrak{N}$. Then, using (6.2), we see that

$$\theta\varphi = F_n(\theta\theta_1, \ldots, \theta\theta_n), \quad \varphi\theta = F_n(\theta_1\theta, \ldots, \theta_n\theta).$$

In addition, all of the products $\theta\theta_i$, $\theta_i\theta$ are easily seen to be in $\mathfrak{N}^*$. This is enough to prove that $\mathfrak{N}\mathfrak{N}^* = \mathfrak{N}^*\mathfrak{N} = \mathfrak{N}^*$. In particular, $\mathfrak{N}^*\mathfrak{N}^* \subset \mathfrak{N}^*$. Next, for any fixed φ in $\mathfrak{N}^*$, let $\mathfrak{M}$ be the set of all ψ in $\mathfrak{N}^*$ such that $\psi\varphi$ is in $\mathfrak{N}^*$. We see readily that $\mathfrak{M}$ is an additive subgroup of $\mathfrak{N}^*$; hence $\mathfrak{M} = \mathfrak{N}^*$. Therefore $\mathfrak{N}^*$ is closed under multiplication. Since $\mathfrak{N}^*$ consists wholly of endomorphisms, the distributive laws are automatic. Hence $\mathfrak{N}^*$ is a ring, and the proof of Theorem 6.2 is complete.

Bibliography

[1] R. H. Bruck, A Survey of Binary Systems, *Ergebnisse der Math. und ihrer Grenzgebiete*, Neue Folge, Heft **20** (Berlin—Göttingen—Heidelberg, 1958).

[2] ——— Normal endomorphisms, *Illinois Journal of Math.*, **4** (1960), 38—87.

[3] ——— Sums of normal endomorphisms, *Proc. Amer. Math. Soc.*, **10** (1959), 674—678.

[4] ——— Some results in the theory of quasigroups, *Transaction Amer. Math. Soc.*, **55** (1944), 19—52.

[5] ——— What is a loop? (In press; to appear in a volume published by the *Math. Assoc. of America.*)

[6] ——— An extension theory for a certain class of loops, *Bull. Amer. Math. Soc.*, **57** (1951), 11—26.

UNIVERSITY OF WISCONSIN,
MADISON, WISCONSIN, U. S. A.

(Received March 22, 1960)

Notwendige und hinreichende Bedingungen für die Existenz von nichtkonstanten Lösungen linearer Funktionalgleichungen

Von ZOLTÁN DARÓCZY in Debrecen

Herrn Professor Ladislaus Rédei zum 60. Geburtstag gewidmet

In gewissen Funktionalgleichungen treten außer den unbekannten Funktionen und den Veränderlichen auch konstante Größen auf. A priori sind diese Konstanten beliebig wählbar, aber nicht jedem möglichen Wert derselben entsprechen nichttriviale Lösungen der Funktionalgleichung. Ziel der vorliegenden Arbeit ist es, für einige Funktionalgleichungen von solchem Typus notwendige und hinreichende Bedingungen für die Existenz nichtkonstanter Lösungen zu bestimmen.

Herr Professor J. ACZÉL hat mich auf das folgende Ergebnis von I. BERSTEIN aufmerksam gemacht (s. S. MARCUS [3]):

Die Funktionalgleichung

$$f\left(\frac{x+y}{2}\right)=\lambda f(x)+(1-\lambda)f(y) \qquad (0<\lambda<1)$$

besitzt für $\lambda \neq \frac{1}{2}$ keine nichtkonstante Lösung.

Auffallend ist es dabei, daß bezüglich der Funktion $f(x)$ keinerlei Voraussetzungen gemacht wurden, so daß das Ergebnis auch für nichtstetige Lösungen gilt. J. ACZÉL [1] hat bezüglich der allgemeineren Funktionalgleichung

$$f(ax+by)=pf(x)+qf(y) \tag{1}$$

bewiesen, daß diese nur im Falle $a=p$, $b=q$ stetige nichtkonstante Lösungen besitzt, wobei dieses Ergebnis mitsamt dem Beweis auch dann gültig bleibt, falls wir statt der Stetigkeit eine schwächere Voraussetzung, wie z. B. die der Meßbarkeit, Beschränkheit usw. machen.

In derselben Arbeit hat J. ACZÉL auch die Funktionalgleichung

$$f(ax+by+c)=pf(x)+qf(y)+r \tag{1'}$$

behandelt.

In Hinblick auf die obigen Resultate läßt sich nun die Frage aufwerfen: was kann man über die nichtkonstanten Lösungen von (1) und (1′) im allgemeinen Falle aussagen, d. h. dann, falls über die Funktion nichts vorausgesetzt wird? Die vorliegende Arbeit soll einen Beitrag zur Lösung dieses Problems leisten.

In § 1 beweisen wir eine leichte Verallgemeinerung der Tatsache, daß aus $a=b$ das Bestehen von $p=q$ folgt und umgekehrt. In § 2 zeigen wir, daß aus der Existenz nichtkonstanter Lösungen und aus der Rationalität einer der Konstanten a, p das Bestehen von $a=p$ folgt und ebenso für b, q. Wir untersuchen in diesem § auch den Fall algebraischer Koeffizienten. In § 3 geben wir notwendige und hinreichende Bedingungen für die Existenz der nicht-trivialen Lösungen der Funktionalgleichung $f(ax+y)=pf(x)+f(y)$ im Falle beliebiger reeller a und p.

Für die Problemstellung sowie für wertvolle Ratschläge möchte ich Herrn Prof. J. ACZÉL aufrichtig danken.

§ 1. Die kommutativen Fälle

Bevor wir unser eigentliches Problem in Angriff nehmen, geben wir eine Verallgemeinerung des Ergebnisses von I. BERSTEIN. Es sei $\circ$ eine kommutative Operation, d. h. für zwei beliebige reelle (oder komplexe) Zahlen x, y soll

$$x \circ y = y \circ x$$

gelten. Dann haben wir den folgenden

Satz 1. *Die Funktionalgleichung*

$$f(x \circ y) = af(x) + bf(y) + c \tag{2}$$

kann nur im Falle $a=b$ eine nichtkonstante Lösung haben.

Beweis. Wegen der Kommutativität der Operation $\circ$ gilt $f(x \circ y) = f(y \circ x)$, und dementsprechend folgt aus (2)

$$af(x) + bf(y) + c = af(y) + bf(x) + c$$

d. h.

$$(a-b)[f(x)-f(y)] = 0.$$

Da $f(x)$ keine Konstante ist, muß $a-b=0$, d. h. $a=b$ gelten. Im Falle

$$x \circ y = \frac{x+y}{2}, \quad a+b=1 \quad a>0, \quad b>0$$

erhalten wir das von I. BERSTEIN [3] auf einem längeren Wege gewonnene Ergebnis.

Weiterhin gilt der folgende, dem vorangehenden Satz analoge

Satz 2. *Die Funktionalgleichung*

$$f(ax+by+c)=f(x)\circ f(y) \tag{3}$$

kann nur im Falle $a=b$ für jedes reelle (komplexe) x eine nichtkonstante Lösung $f(x)$ haben.

Beweis. Wegen der Kommutativität der Operation $\circ$ gilt

$$f(ax+by+c)=f(ay+bx+c). \tag{4}$$

Wir nehmen an, daß (3) für $a\neq b$ eine nichtkonstante Lösung hat. Dann gibt es Werte x_1 und x_2, für welche $f(x_1)\neq f(x_2)$ ist. Wir betrachten nunmehr das Gleichungssystem

$$ax+by+c=x_1,\quad bx+ay+c=x_2. \tag{5}$$

Dieses ist immer lösbar, falls nur $a^2-b^2\neq 0$ ist. Da $a\neq b$ ist, haben wir also nur im Falle $a=-b\neq 0$ nicht immer eine Lösung. Diesen Fall werden wir einstweilen unbeachtet lassen. Es sei $x=\xi$, $y=\eta$ die eindeutig bestimmte Lösung von (5). Unter Anwendung von (4) erhalten wir dann

$$f(x_1)=f(a\xi+b\eta+c)=f(b\xi+a\eta+c)=f(x_2),$$

was offenbar einen Widerspruch bedeutet, da wir ja $f(x_1)\neq f(x_2)$ angenommen haben.

Nun bleibt nur noch die Untersuchung des Falles $a=-b\neq 0$ übrig. In diesem Falle nimmt unsere Funktionalgleichung die Gestalt

$$f[a(x-y)+c]=f(x)\circ f(y) \tag{6}$$

an. Setzen wir $x=y$, so ergibt sich

$$f(c)=f(x)\circ f(x). \tag{7}$$

Wegen der Kommutativität folgt aus (6)

$$f[a(x-y)+c]=f[a(y-x)+c].$$

Indem wir davon und von (7) Gebrauch machen, erhalten wir

$$f[a(x-y)+c]\circ f[a(y-x)+c]=f[a(x-y)+c]\circ f[a(x-y)+c]=f(c).$$

Hier läßt sich die linke Seite auf Grund von (6) in der Form

$$f[a(ax-ay+c-ay+ax-c)+c]$$

schreiben. Da $2a^2(x-y)+c=z$ beliebig ist ($a\neq 0$), erhalten wir $f(z)=$ $=f(c)$, d. h. falls es eine Lösung gibt, so kann diese nur konstant sein.

Damit haben wir unseren Satz vollständig bewiesen.

§ 2. Die Funktionalgleichung $f(ax+by+c)=pf(x)+qf(y)+r$

In diesem Paragraphen werden wir die Funktionalgleichung

$$f(ax+by+c)=pf(x)+qf(y)+r \tag{8}$$

untersuchen, wobei keine der Konstanten a, b, p und q gleich Null ist, und x sowie y die Gesamtheit der reellen (komplexen) Zahlen durchläuft. Zuerst beweisen wir einen Hilfssatz, den wir im folgenden benötigen werden.

Hilfssatz 1. *Genügt die nichtkonstante Funktion $f(x)$ der Gleichung (8), so genügt die Funktion $g(x)\equiv f(x)-f(0)$ der Cauchyschen Grundgleichung*

$$g(x+y)=g(x)+g(y). \tag{9}$$

Beweis. Zuerst setzen wir $a+b\neq 0$ voraus. Dann folgt aus (8), indem wir $x=y$ setzen, mit Rücksicht auf die Tatsache, daß $f(x)$ nicht konstant ist, $p+q\neq 0$. Mit der Substitution

$$x=y=\frac{ax^*+by^*}{a+b}$$

ergibt sich aus (8)

$$f(ax^*+by^*+c)=(p+q)f\left(\frac{ax^*+by^*}{a+b}\right)+r.$$

Falls wir hier die linke Seite gemäß (8) aufschreiben und die Bezeichnungen

$$\alpha=\frac{a}{a+b},\quad \beta=\frac{b}{a+b},\quad \gamma=\frac{p}{p+q},\quad \delta=\frac{q}{p+q}$$

einführen, erhalten wir die Gleichung

$$\gamma f(x^*)+\delta f(y^*)=f(\alpha x^*+\beta y^*), \tag{10}$$

wobei $\alpha+\beta=\gamma+\delta=1$ ist. Indem wir in (10) $x^*=0$ bzw. $y^*=0$ setzen, erhalten wir die beiden folgenden Gleichungen:

$$f(\beta y^*)=\gamma f(0)+\delta f(y^*),\quad f(\alpha x^*)=\gamma f(x^*)+\delta f(0).$$

Mit Hilfe dieser Relationen nehmen wir nun die folgende Umformung von (10) vor:

$$\begin{aligned} f(\alpha x^*+\beta y^*)&=\gamma f(x^*)+\delta f(y^*)=f(\alpha x^*)-\delta f(0)+\\ &+f(\beta y^*)-\gamma f(0)=f(\alpha x^*)+f(\beta y^*)-f(0).\end{aligned}$$

Führen wir jetzt die Bezeichnungen $\alpha x^*=u$ und $\beta y^*=v$ ein ($\alpha\neq 0$, $\beta\neq 0$), so ergibt sich aus der obigen Gleichung

$$f(u+v)-f(0)=f(u)-f(0)+f(v)-f(0),$$

d. h. $g(t)\equiv f(t)-f(0)$ genügt tatsächlich der Gleichung (9).

Ist $a+b=0$, so folgt aus (8), da $f(x)$ nichtkonstant ist, $p+q=0$. Dann müssen wir die Gleichung

$$f[a(x-y)+c]=p[f(x)-f(y)]+r \tag{11}$$

untersuchen. Es sei $y=0$. In diesem Falle ergibt sich

$$f(ax+c)=p[f(x)-f(0)]+r,$$

woraus

$$p[f(x-y)-f(0)]=f[a(x-y)+c]-r=p[f(x)-f(y)]$$

und wegen $p\neq 0$

$$f(x-y)=f(x)-f(y)+f(0)$$

folgt. Durch die Substitution $x-y=z$ $(x=y+z)$ gewinnen wir jetzt

$$f(y+z)=f(y)+f(z)-f(0)$$

und daraus folgt, daß $g(t)\equiv f(t)-f(0)$ der Gleichung (9) genügt.

Damit haben wir unseren Hilfssatz bewiesen.

Satz 3. *Sind von den Zahlen a, b, p, q die Zahlen a, b, oder a, q, oder b, p, oder p, q rational, so ist zur Existenz einer nichtkonstanten Lösung der Funktionalgleichung* (8) *notwendig und hinreichend, daß $a=p$, $b=q$ und (im Falle $a+b=1$, $c=0$) $r=0$ ist.*

Beweis. Setzen wir a rational voraus. Auf Grund von Hilfssatz 1 genügt $g(x)\equiv f(x)-f(0)$ der Cauchyschen Grundgleichung, und somit gilt

$$g(ax)=ag(x). \tag{12}$$

Anderseits folgt aus (8), indem man $y=0$ setzt,

$$f(ax+c)=pf(x)+qf(0)+r.$$

Durch eine Umformung und unter Anwendung von (12) erhält man

$$pf(x)+qf(0)+r-f(0)=f(ax+c)-f(0)=f(ax)-f(0)+$$
$$+f(c)-f(0)=af(x)-af(0)+f(c)-f(0),$$

woraus sich $(a-p)f(x)=$ Konstante ergibt, und da die Funktion $f(x)$ nicht konstant ist, muß notwendigerweise $a=p$ sein.

Im Falle wo b rational ist, verläuft der Beweis ähnlich.

Ist p eine rationale Zahl, so gilt

$$f(ax-px)=f(ax-px)-f(0)+f(0)=g(ax-px)+f(0)=$$
$$=g(ax)-g(px)+f(0)=g(ax+c)-g(c)-g(px)+f(0)=$$
$$=pf(x)+qf(0)+r-f(c)-pf(x)+pf(0)+f(0)=f(0),$$

d. h. $f[(a-p)x]=$ Konstante, und da die Funktion $f(x)$ nichtkonstant ist, muß $a=p$ sein.

Im Falle wo q rational ist, verläuft der Beweis ähnlich.

Ist $a+b=1$ und $c=0$, so nimmt unsere Funktionalgleichung die Gestalt

$$f[ax+(1-a)y]=af(x)+(1-a)f(y)+r$$

an. Setzt man $x=y$, so ergibt sich $f(x)=f(x)+r$, d. h. in diesem Falle muß $r=0$ sein.

Damit haben wir die Notwendigkeit der Bedingungen bewiesen.

Der Beweis der Hinlänglichkeit geschieht durch Angabe von Lösungsfunktionen. Wir unterscheiden die folgenden Fälle:

I. Ist $c=0$ und $r=0$, so ist $f(x)=Ax$ eine Lösung, wobei A eine von Null verschiedene Konstante bedeutet.

II. Ist $c\neq 0$ und $r\neq 0$, so ist $f(x)=\frac{r}{c}x$ eine, offenbar nichtkonstante, Lösung.

III. Ist $c=0$, $r\neq 0$ und $a+b\neq 1$, so ist

$$f(x)=Ax+\frac{r}{1-a-b}$$

eine Lösung, wobei A eine von Null verschiedene Konstante bedeutet.

IV. Ist $c\neq 0$ und $r=0$, so unterscheiden wir die folgenden beiden Fälle:

1. $a+b\neq 1$. Dann ist

$$f(x)=Ax+\frac{Ac}{a+b-1}$$

eine Lösung, wobei A eine von Null verschiedene Konstante ist.

2. $a+b=1$. In diesem Falle nimmt unsere Funktionalgleichung die Gestalt

$$f[ax+(1-a)y+c]=af(x)+(1-a)f(y) \tag{13}$$

an. Durch die Substitution $x=y$ ergibt sich $f(x+c)=f(x)$, d. h. die Funktion ist periodisch mit der Periode c.

Mit Hilfe der Hamelschen Basis [2] geben wir nunmehr eine solche nirgends stetige additive Funktion $f(x)$ an, welche periodisch ist und der Gleichung (13) genügt.

Die Elemente der Hamelschen Basis seien die reellen Zahlen $\{c, \ldots, r_\nu, \ldots\}$. Dann entsteht eine beliebige reelle Zahl x in der Form

$$x=\alpha c+\sum_j \beta_j r_{\nu_j},$$

wobei α und die β_j rationale Zahlen sind. Wir definieren die Funktion $f(x)$ durch die Formel

$$f(x) = \alpha f(c) + \sum_j \beta_j f(r_{\nu_j})$$

und den Basiselementen entsprechend wählen wir die Funktionswerte

$$f(c) = 0, \quad f(r_\nu) \neq 0.$$

Da die Zahl a rational und die Funktion $f(x)$ additiv ist, gilt nunmehr

$$f[ax + (1-a)y + c] = f(ax) + f[(1-a)y] + f(c) = af(x) + (1-a)f(y),$$

d. h. die nichtkonstante Funktion $f(x)$ genügt (13).

Damit haben wir unseren Satz vollständig bewiesen.

Im Falle rationaler Konstanten ist es uns verhältnismäßig leicht gelungen, die früher unter Voraussetzung der Stetigkeit gewonnenen notwendigen Bedingungen zu beweisen, der Fall irrationaler Koeffizienten ist aber noch underledigt geblieben. Im folgenden erörtern wir die Ergebnisse unserer diesbezüglichen Untersuchungen.

Hilfssatz 2. *Befriedigt die nichtkonstante Funktion $f(x)$ die Gleichung (8), so gelten für die Funktion $g(x) \equiv f(x) - f(0)$ die Relationen*

$$g(a^k x) = p^k g(x), \quad g(b^k x) = q^k g(x),$$

wo k eine beliebige natürliche Zahl ist.

Beweis. Aus (8) folgt durch die Substitution $y = 0$

$$f(ax + c) = pf(x) + qf(0) + r.$$

Durch eine Umformung und unter Verwendung von Hilfssatz 1 erhalten wir

$$f(ax) - f(0) + f(c) - f(0) = f(ax + c) - f(0) =$$
$$= pf(x) - pf(0) + (p + q)f(0) - f(0) + r$$

und hieraus folgt

$$g(ax) = f(ax) - f(0) = p[f(x) - f(0)] + (p + q)f(0) + r - f(c) = pg(x).$$

Nunmehr verwenden wir vollständige Induktion. Wir nehmen an, daß unsere Behauptung für k richtig ist, d. h. daß $g(a^k x) = p^k g(x)$ gilt. Dann ergibt sich $g[a(a^k x)] = pg(a^k x) = pp^k g(x)$, d. h. $g(a^{k+1} x) = p^{k+1} g(x)$.

Damit ist unser Hilfssatz bereits bewiesen, da der Beweis für b und q analog verläuft.

Nun gilt der folgende

Satz 4. *Es seien a und b, oder a und q, oder b und p, oder p und q algebraische Zahlen, und $P_a(x)$, $P_b(x)$, $P_p(x)$ bzw. $P_q(x)$ sei das den Zahlen a, b, p bzw. q eindeutig zugeordnete irreduzible Hauptpolynom. Dann ist zur*

Existenz einer nichtkonstanten Lösung der Gleichung (8) *notwendig, daß auch die übrigen Koeffizienten algebraisch sind, und daß die Identitäten*

$$P_a(x) \equiv P_p(x), \quad P_b(x) \equiv P_q(x)$$

bestehen.

Beweis. Es sei

$$P_a(x) = x^n + \sum_{i=0}^{n-1} \alpha_i x^i$$

(α_i rational für jedes i). Auf Grund der Hilfssätze 1 und 2 ergibt sich

$$(14) \quad g\left[\left(a^n + \sum_{i=0}^{n-1} \alpha_i a^i\right)x\right] = g(a^n x) + \sum_{i=0}^{n-1} \alpha_i g(a^i x) = \left(p^n + \sum_{i=0}^{n-1} \alpha_i p^i\right) g(x)$$

und dementsprechend muß im Falle $P_a(a) = a^n + \sum_{i=0}^{n-1} \alpha_i a^i = 0$, da $g(x)$ nicht konstant ist,

$$(15) \qquad p^n + \sum_{i=0}^{n-1} \alpha_i p^i = 0$$

sein, so daß auch die Zahl p algebraisch ist. Dann gehört auch zu p ein eindeutig bestimmtes irreduzibles Hauptpolynom $P_p(x)$. Da $P_a(p) = 0$ ist, gilt $P_a(x) | P_p(x)$, so daß mit Rücksicht auf die Irreduzibilität $P_a(x) \equiv P_p(x)$ sein muß.

Ähnlich verläuft der Beweis im Falle, daß b algebraisch ist.

Falls p algebraisch ist und z. B. (15) befriedigt, dann erhalten wir, indem wir (14) in umgekehrter Richtung lesen, da $g(x)$ nicht konstant ist, die Relation $a^n + \sum_{i=0}^{n-1} \alpha_i a^i = 0$, und so ist $P_p(a) = 0$; folglich gilt $P_p(x) | P_a(x)$ und wegen der Irreduzibilität

$$P_a(x) \equiv P_p(x).$$

Ein ähnlicher Schluß gilt im Falle, daß q algebraisch ist.

Obwohl dieser Satz keine vollständige Lösung des Problems bedeutet, lassen sich mit seiner Hilfe zahlreiche konkrete Fälle erledigen. Betrachten wir z. B. die Funktionalgleichung

$$f(\sqrt[3]{2}x + y) = pf(x) + f(y),$$

wo p reell ist. Das zu $\sqrt[3]{2}$ gehörige Hauptpolynom ist $x^3 - 2$. Da nun dieses außer $\sqrt[3]{2}$ keine reelle Wurzel hat, muß $\sqrt[3]{2} = p$ sein. Auf Grund einer analogen Überlegung gilt auch im allgemeinen das folgende

Korollar. *Sind a und b, oder a und q, oder b und p, oder p und q reelle algebraische Zahlen, für welche die entsprechenden eindeutig zugeordneten irreduziblen Hauptpolynome keine anderen reellen Wurzeln haben, so ist zur Existenz einer nichtkonstanten Lösung der Gleichung* (8) *notwendig, daß $a=p$ und $b=q$ ist.*

Dieses Korollar enthält offenbar die Notwendigkeitsaussage von Satz 3, da ja die rationalen Zahlen die eindeutig bestimmten Wurzeln von Polynomen ersten Grades sind.

Alle unsere Schlußweisen bleiben auch für komplexe Funktionen komplexer Veränderlichen gültig, der Beweis von Satz 3 läßt sich aber auf den Fall „komplexer rationaler" Koeffizienten nicht übertragen, da (12) für komplexe rationale Zahlen $a=\alpha+\beta i$ (α, β rational) seine Gültigkeit verliert. Hingegen bleibt Satz 4 samt seinem Beweis auch für komplexe algebraische Zahlen a, b bzw. p bzw. q gültig.

§ 3. Notwendige und hinreichende Bedingungen im Falle irrationaler Koeffizienten

Man könnte daran denken, daß die Beschränkung auf rationale bzw. algebraische Koeffizienten nur eine Mangelhaftigkeit unserer Beweismethode ist, und der dritte Satz auch im Falle beliebiger Koeffizienten besteht. Im weiteren zeigen wir nun, daß unsere Ergebnisse keiner wesentlichen Verbesserung fähig sind.

Es bezeichne R den Körper der rationalen Zahlen, V den Körper der reellen Zahlen und K einen beliebigen Teilkörper der reellen Zahlen. Wir betrachten K als einen Vektorraum über R, mit der Basis $\{\ldots, s_\nu, \ldots\}$ und V als einen Vektorraum über K mit der Basis $\{\ldots, r_\mu, \ldots\}$.

Wir brauchen den folgenden Hilfssatz[1]).

Hilfssatz 3. *Die Zahlenmenge*

$$\{\ldots, s_\nu r_\mu, \ldots\}$$

ist eine Basis der reellen Zahlen über R.

Nunmehr betrachten wir die Funktionalgleichung

$$f(ax+y)=pf(x)+f(y), \tag{16}$$

wo a und p nichtrationale reelle Zahlen sind. Im folgenden wird für uns die folgende Definition von Nutzen sein:

[1]) Für den Fall einer endlichen Basis siehe z. B. Rédei [4], § 413. Für unendliche Basen verläuft der Beweis analog.

Zwei reelle Zahlen, r und s nennen wir *entsprechend*, falls

a) r und s Wurzel desselben irreduziblen Hauptpolynoms über R sind, oder aber

b) r und s beide transzendent über R sind.

Es gilt der folgende

Satz 5. *Zur Existenz einer nichtkonstanten Lösung der Funktionalgleichung* (16) *ist es notwendig und hinreichend, daß a und p entsprechende Zahlen sind.*

Beweis. Die Notwendigkeit der Bedingungen folgt aus Satz 4. Um zu beweisen, daß die Bedingungen auch hinreichend sind, nehmen wir an, daß a und p entsprechende Zahlen sind. Bekanntlich gibt es dann einen solchen Isomorphismus φ zwischen $R(a)$ und $R(p)$, für welchen die Relationen $\varphi(a)=p$ und $\varphi(r)=r$ bei beliebigem $r\in R$ gelten[2]).

Es sei $\{\ldots, s_\nu, \ldots\}$ eine Basis von $R(a)$ über R, und $\{1, \ldots, r_\mu, \ldots\}$ eine Basis von V über $R(a)$. Dann ist auf Grund des Hilfssatzes 3 die Zahlenmenge

$$\{\ldots, s_\nu, \ldots, s_\nu r_\mu, \ldots\}$$

eine Basis von V über R. Es sei nunmehr x eine beliebige reelle Zahl. Nach dem obigen läßt x eine Darstellung von der Form

$$x=\sum_i \alpha_i s_{\nu_i}+\sum_{j,k}\beta_j^k s_{\nu_j} r_{\mu_k}$$

zu, wobei $\alpha_i, \beta_j^k \in R$ ist.

Wir definieren die Funktion $f(x)$ durch

$$f(x)=\sum_i \alpha_i f(s_{\nu_i})+\sum_{j,k}\beta_j^k f(s_{\nu_j} r_{\mu_k})$$

und wir wählen die den Basiselementen entsprechenden Funktionswerte auf folgende Weise:

$$f(s_\nu)=\varphi(s_\nu), \quad f(s_\nu r_\mu)=0.$$

Dann gilt

$$f(x)=\sum_i \alpha_i \varphi(s_{\nu_i}).$$

Bekanntlich ist die so definierte Funktion additiv, d. h. sie befriedigt die Funktionalgleichung

$$f(x+y)=f(x)+f(y).$$

---

[2]) $R(a)$ bedeutet die Erweiterung von R durch das Element a. Da R gemeinsamer Primkörper der Körper $R(a)$ und $R(p)$ ist, gilt $\varphi(r)=r$ für jedes Element $r\in R$. (S. Rédei [4].)

Es genügt jetzt noch zu zeigen, daß auch $f(ax)=pf(x)$ gilt. Um den Nachweis der letzten Behauptung zu erbringen, berechnen wir den Wert von ax:

$$ax=\sum_i \alpha_i a s_{\nu_i}+\sum_{j,k}\beta_j^k a s_{\nu_j} r_{\mu_k}.$$

Da $as_{\nu}\in R(a)$ ist, kann man

$$as_{\nu_i}=\sum_k \gamma_k^i s_{\nu_k}, \qquad \gamma_k^i \in R$$

schreiben. Indem wir davon Gebrauch machen, erhalten wir

$$ax=\sum_i \alpha_i\Big(\sum_k \gamma_k^i s_{\nu_k}\Big)+\sum_{j,k}\beta_j^k\Big(\sum_l \gamma_l^j s_{\nu_l}\Big) r_{\mu_k}.$$

Nunmehr berechnen wir den Wert von $f(ax)$:

$$f(ax)=\sum_i \alpha_i \sum_k \gamma_k^i \varphi(s_{\nu_k})=\sum_i \alpha_i \sum_k \varphi(\gamma_k^i)\varphi(s_{\nu_k})=\sum_i \alpha_i \varphi\Big(\sum_k \gamma_k^i s_{\nu_k}\Big)=$$
$$=\sum_i \alpha_i \varphi(as_{\nu_i})=\sum_i \alpha_i \varphi(a)\varphi(s_{\nu_i})=\varphi(a)\sum_i \alpha_i \varphi(s_{\nu_i})=pf(x).$$

Damit haben wir den Satz 5 bewiesen.

Aus dem Satz 5 folgt, daß sich die Behauptung von Satz 3 nicht auf den Fall beliebiger reeller Koeffizienten übertragen läßt. Z. B. haben die Funktionalgleichungen

$$f(\sqrt{2}x+y)=-\sqrt{2}f(x)+f(y),$$
$$f(\pi x+y)=ef(x)+f(y)$$

nichttriviale Lösungen.

Literatur

[1] J. Aczél, Über eine Klasse von Funktionalgleichungen, *Commentarii Math. Helvetici*, **21** (1948), 247—256.

[2] G. Hamel, Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung $f(x+y)=f(x)+f(y)$, *Math. Annalen*, **60** (1905), 459—462.

[3] S. Marcus, Sur une classe de fonctions définies par des inégalités, introduite par M. Á. Császár, *Acta Sci. Math.*, **19** (1958), 192—217.

[4] L. Rédei, *Algebra* I (Budapest, 1954).

(Eingegangen am 4. Dezember 1959)

On the ordering of quotient rings and quotient semigroups

By L. FUCHS in Budapest

Dedicated to L. Rédei on his 60th birthday

It is a rather familiar problem how to extend the ordering relation of a fully ordered ring R to a full order of a larger ring S, in particular, those cases are of great interest in which such an extension is uniquely possible. The most important special case of this problem is when R is a domain of integrity and S is its quotient field; this case is dealt with in most textbooks on algebra. Other important special cases have been considered by several authors. ALBERT [1] and NEUMANN [6] discussed the case in which S was the Ore quotient skewfield of R. Recently, Prof. RÉDEI has been interested in this problem [7] when R was supposed to be a ring without divisors of zero and S its ring extension with identity containing no divisors of zero. GRÄTZER and SCHMIDT [4] considered the more general problem when R was an ideal of S and S was supposed to be free of divisors of zero. Here we wish to give a common generalization of these results. Our starting point is a rather general definition of quotient ring, one which includes the relationship of R and S in all above-mentioned cases.

Our main result can be carried over to semigroups. Because of the failure of a positive cone in semigroups by means of which it is easy to handle the ordering relation in rings, a certain amount of complication arises, but this is merely of technical character. Its effect appears in that the proof is somewhat longer. As corollaries we obtain well-known results of TAMARI —ALIMOV—NAKADA and CONRAD, respectively.

By a *fully ordered ring* R we mean an associative (but not necessarily commutative) ring which is at the same time a fully ordered set satisfying: $a \leqq b$ implies $a \pm c \leqq b \pm c$, $ac \leqq bc$ and $ca \leqq cb$ for all $c > 0$ in the ring. By the *positive cone* P of R we mean the set of all $x \in R$ with $x \geqq 0$. P has the characterizing properties: it is closed with respect to addition and multiplication, it contains 0 and for any $x \in R$, $x \neq 0$, exactly one of $x, -x$.

The positive cone P uniquely determines the ordering relation of R, since $a \leqq b$ if and only if $b-a \in P$.

Let R be an arbitrary ring and S an overring of R. Assume that to each $\alpha \in S \setminus R$ there exist elements $a, b \in R$ such that (i) a is not a left divisor of zero in S, (ii) b is not a right divisor of zero in S, (iii) $a\alpha = c$ and $\alpha b = d$ belong to R. In this case S will be called *a quotient ring of* R.

Our main result is the following theorem.

Theorem 1. *A full order of an (associative) ring R can be uniquely extended to a full order of an arbitrary quotient ring S of R.*

Let R be a fully ordered ring with the positive cone P and S a quotient ring of R. There is no loss of generality in assuming that in (i) and (ii) the elements a, b are >0. Then in (iii) the elements c and d have the same sign, for $cb = a\alpha b = ad$, and so the sign of $a\alpha$ and αb does not depend on the special choice of a or b. We define the positive cone Q of S to consist of P and of all $\alpha \in S \setminus R$ such that $a\alpha$ (and so αb) lies in P. Then we see immediately that for any $\alpha \neq 0$ in S, either α or $-\alpha$ belongs to Q, but not both. If $\alpha, \beta \in Q$, then there exist elements $a, b \in P$ with (i) and (ii) or $=1$ such that $a\alpha, \beta b \in P$. Hence $a(\alpha+\beta)b = (a\alpha)b + a(\beta b) \in P$, and so[1]) $\alpha+\beta \in Q$. Again, $a(\alpha\beta)b = (a\alpha)(\beta b) \in P$ whence $\alpha\beta \in Q$. Consequently, Q defines a full order in S. The uniqueness is evident. Q. e. d.

We mention the following consequences of our theorem.[2])

1. If R is a fully ordered ring having an Ore left quotient skewfield S, then S can be fully ordered uniquely so as to continue the ordering of R. (ALBERT [1], NEUMANN [6].)

2. Any full order of a domain of integrity can be uniquely extended to a full order of its quotient field.

3. Let R be an ideal of a ring S containing at least one element which is not a divisor of zero. Then any full order of R can be extended in a unique way to a full order of S. (Cp. GRÄTZER—SCHMIDT [4].)

4. Let R be a ring containing a non-divisor of zero and S a minimal ring with identity[3]) containing R. Every full order of R can be extended uniquely to a full order of S. (Cp. RÉDEI [7].)

Let us turn to semigroups. By a *fully ordered semigroup* S is meant a

---

[1]) Here we make use of the fact that if $a, b > 0$ and $c = a\alpha b \in R$, then α and c have the same sign. In fact, if $d > 0$ is chosen so that $d(a\alpha) = f \in R$, then the elements $\alpha, f, fb = dc, c$ are simultaneously positive or negative.

[2]) The proofs are immediate and therefore may be left to the reader.

[3]) If the ring contains elements which are not divisors of zero, then it has a ring extension with identity in which they remain non-divisors of zero. We understand this by "minimal".

semigroup which is at the same time a fully ordered set satisfying: $a \leqq b$ implies $ac \leqq bc$ and $ca \leqq cb$ for all $c \in S$.

Let T be a semigroup containing the semigroup S. Assume that to any $\alpha \in T \setminus S$ there exist elements $a, b \in S$ such that (i) a is left-cancellable[4]) in T, (ii) b is right-cancellable in T and (iii) $a\alpha$, αb belong to S. Then we shall say that T is *a quotient semigroup of* S.

We have the following analogue of Theorem 1:

Theorem 2. *A full order of a semigroup S can be extended, in one and only one way, to a full order of an arbitrary quotient semigroup T of S.*

If T properly contains S, then there exist surely elements $a, b \in S$ which are left- resp. right-cancellable in T, and therefore in the above definition the case $\alpha \in S$ need not be excluded. Now if $\alpha, \beta \in T$ $(\alpha \neq \beta)$ and if a, b are left- resp. right-cancellable elements such that $a\alpha$, $\beta b \in S$, then $a\alpha b$ and $a\beta b$ are different elements of S, and we define $\alpha \gtrless \beta$ according as $a\alpha b \gtrless a\beta b$ in S. It is a trivial fact that for the elements of S this definition coincides with that originally given in S. The definition does not depend on the special choice of a, b. For, if a', b' are again left- resp. right-cancellable elements with $a'\alpha$, $\beta b' \in S$, then — taking a left- and a right-cancellable element $a'', b'' \in S$ such that $a''(a'\beta), (\alpha b)b'' \in S$ — we obtain e. g. from $a\alpha b < a\beta b$ in turn $a\alpha bb'' < a\beta bb''$, $\alpha bb'' < \beta bb''$, $a''a'\alpha bb'' < a''a'\beta bb''$, $a''a'\alpha < a''a'\beta$, $a''a'\alpha b' < a''a'\beta b'$, $a'\alpha b' < a'\beta b'$. A similar reasoning applies if a', b' are determined so as to have $a'\beta, \alpha b' \in S$. The transitivity of $<$ follows by a straightforward computation of similar kind. Finally, we show that $\alpha \leqq \beta$ implies $\gamma\alpha \leqq \gamma\beta$ for all $\gamma \in T$. If a, b, b'' are defined as before and $c \in S$ is left-cancellable such that $c\gamma \in S$, then we get successively $a\alpha b \leqq a\beta b$, $a\alpha bb'' \leqq a\beta bb''$, $\alpha bb'' \leqq \beta bb''$, $c\gamma\alpha bb'' \leqq c\gamma\beta bb''$. Hence, by multiplying by suitable elements we arrive at $\gamma\alpha \leqq \gamma\beta$. The uniqueness of the extension is evident.

We obtain the following corollaries.

1. Let S be a cancellative fully ordered semigroup satisfying:[5]) for each pair $a, b \in S$ there is a pair $x, y \in S$ such that $ax = by$. Then there exists a fully ordered group G containing S in such a way that every $g \in G$ has the form $g = ab^{-1} (a, b \in S)$ and $g > e$ if and only if $a > b$ in S. This G is unique within to order-isomorphism. (CONRAD [3].)

2. A cancellative commutative fully ordered semigroup S has a quotient group which can be fully ordered in a unique manner. (TAMARI [8], ALIMOV [2], NAKADA [5].)

---

[4]) An element a is left-cancellable if $ax = ay$ implies $x = y$.

[5]) This is just the Ore condition and ensures the existence of a quotient group of S.

References

[1] A. A. Albert, A property of ordered rings, *Proc. Amer. Math. Soc.*, **8** (1957), 128—129.
[2] Н. Г. Алимов, Об упорядоченных полугруппах, Изв. Акад. Наук СССР, **14** (1950), 569—576.
[3] P. F. Conrad, Ordered semigroups, *Nagoya Math. Journ.*, **16** (1960), 51—64.
[4] G. Grätzer—E. T. Schmidt, Über die Anordnung von Ringen, *Acta Math. Acad. Sci. Hung.*, **8** (1957), 259—260.
[5] O. Nakada, Partially ordered abelian semigroups. I—II, *Journ. Fac. Sci. Hokkaido Univ.*, **11** (1951), 181—189; **12** (1952), 73—86.
[6] B. H. Neumann, On ordered groups, *Amer. Journ. Math.*, **71** (1949), 1—18.
[7] L. Rédei, *Algebra*, vol. I (Budapest, 1954).
[8] D. Tamari, Groupoïdes reliés et demi-groupes ordonnés, *C. R. Acad. Sci. Paris*, **228** (1949), 1184—1186.

(Received December 15, 1960.)

Subnormale Untergruppen und p-Sylowgruppen

Von BERTRAM HUPPERT in Tübingen (Deutschland)

Herrn Professor L. Rédei zum 60. Geburtstag gewidmet

Diese Note schließt sich an die Arbeit [11] von WIELANDT an. Wir bezeichnen mit $s\mathfrak{G}$ den Verband der subnormalen (nachinvarianten) Untergruppen der endlichen Gruppe $\mathfrak{G}$, d. h. derjenigen Untergruppen von $\mathfrak{G}$, welche Mitglied einer Kompositionsreihe von $\mathfrak{G}$ sind. Stets sei $\mathfrak{P}$ eine p-Sylowgruppe von $\mathfrak{G}$; in unseren Betrachtungen wird $\mathfrak{P}$ immer festgehalten werden. Nach WIELANDT [11] ist für jedes $\mathfrak{N} \in s\mathfrak{G}$ die Gruppe $\mathfrak{N} \cap \mathfrak{P}$ eine p-Sylowgruppe von $\mathfrak{N}$, und die Abbildung von $\mathfrak{N}$ auf $\mathfrak{N} \cap \mathfrak{P}$ ist ein Verbandshomomorphismus von $s\mathfrak{G}$ in den Verband $s\mathfrak{P}$ aller Untergruppen von $\mathfrak{P}$ (in der p-Gruppe $\mathfrak{P}$ ist jede Untergruppe subnormal, sodaß die Bezeichnung $s\mathfrak{P}$ für den Verband aller Untergruppen von $\mathfrak{P}$ gerechtfertigt ist). Das Bild von $s\mathfrak{G}$ in $s\mathfrak{P}$ bezeichnen wir mit $s_{\mathfrak{G}}\mathfrak{P}$. Unsere Betrachtungen knüpfen insbesondere an die folgenden beiden Sätze von WIELANDT an ([11], 3. 8 und 4. 2):

(A) Ist $p^2 \| |\mathfrak{G}|$, so sind die folgenden beiden Aussagen gleichwertig: 1. $s\mathfrak{P} = s_{\mathfrak{G}}\mathfrak{P}$, 2. $\mathfrak{G}$ ist p-auflösbar von der p-Länge 1, d. h. es gibt eine Normalkette $\mathfrak{E} \trianglelefteq \mathfrak{N} \trianglelefteq \mathfrak{M} \trianglelefteq \mathfrak{G}$ derart, daß die Ordnungen von $\mathfrak{N}$ und $\mathfrak{G}/\mathfrak{M}$ zu p teilerfremd sind und $\mathfrak{M}/\mathfrak{N}$ eine p-Gruppe ist (zum Begriff der p-Länge siehe HALL—HIGMAN [5]).

(B) Ist $\mathfrak{P}$ zyklisch, so ist entweder $s_{\mathfrak{G}}\mathfrak{P} = s\mathfrak{P}$ oder $s_{\mathfrak{G}}\mathfrak{P}$ ist der triviale Verband $s_0\mathfrak{P} = \{\mathfrak{E}, \mathfrak{P}\}$.

Wir werden für ungerade Primzahlen p eine Verschärfung von (A) beweisen, ferner einige Sätze für den Fall einer abelschen p-Sylowgruppe $\mathfrak{P}$, die bei zyklischem $\mathfrak{P}$ alle mit (B) übereinstimmen.

Bezeichnungen. $|\mathfrak{G}|$ sei die Ordnung der Gruppe $\mathfrak{G}$ (es werden nur endliche Gruppen betrachtet). $\mathbf{Z}(\mathfrak{G})$ bezeichne das Zentrum, $\Phi(\mathfrak{G})$ die Frattinigruppe und $\mathfrak{G}'$ die Kommutatorgruppe von $\mathfrak{G}$. Es sei $A^G = G^{-1}AG$ und $(A, G) = A^{-1}G^{-1}AG$. Den Normalisator bzw. Zentralisator der Untergruppe $\mathfrak{A}$ von $\mathfrak{G}$ bezeichnen wir mit $\mathbf{N}(\mathfrak{A})$ bzw. $\mathbf{C}(\mathfrak{A})$. Ist $\mathfrak{A}$ Untergruppe (echte Untergruppe) von $\mathfrak{G}$, so schreiben wir $\mathfrak{A} \leqq \mathfrak{G}$ ($\mathfrak{A} < \mathfrak{G}$); ist $\mathfrak{A}$ subnormale oder nor-

male Untergruppe von $\mathfrak{G}$, so sei dies durch $\mathfrak{A} \lhd\lhd \mathfrak{G}$ bzw. $\mathfrak{A} \lhd \mathfrak{G}$ hervorgehoben. Mit $\langle \mathfrak{A}, \mathfrak{B} \rangle$ bezeichnen wir die von $\mathfrak{A}$ und $\mathfrak{B}$ erzeugte Untergruppe von $\mathfrak{G}$; $\mathfrak{A}$ und $\mathfrak{B}$ sind dabei irgendwelche Teilmengen von $\mathfrak{G}$, nicht notwendig Untergruppen. Ist $\mathfrak{P}$ eine p-Gruppe, so schreiben wir $\Omega_1(\mathfrak{P})$ für das Erzeugnis aller Elemente der Ordnung p von $\mathfrak{P}$.

§ 1. Hilfssätze

1.1. Definition. *Die endliche Gruppe $\mathfrak{G}$ heißt p-nilpotent, wenn sie einen Normalteiler besitzt, dessen Ordnung zu p teilerfremd ist und dessen Index eine p-Potenz ist.* (Offenbar ist dieser Normalteiler dann eine charakteristische Untergruppe von $\mathfrak{G}$.)

1.2. Definition. *Die Gruppe $\mathfrak{G}$ heißt p-reduziert, wenn sie keine nichttrivialen Normalteiler oder Faktorgruppen von zu p teilerfremder Ordnung besitzt.*

1.3. Hilfssatz. *Sei $\mathfrak{N}$ subnormal in $\mathfrak{G}$. Für mindestens eine p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ gelte $\mathfrak{N} \cap \mathfrak{P} \leqq \Phi(\mathfrak{P})$. Ferner sei $p > 2$ oder $\Phi(\mathfrak{P})$ abelsch. Dann ist $\mathfrak{N}$ p-nilpotent.*

Beweis. a) Wir beweisen den Satz zunächst für den Fall $\mathfrak{N} \trianglelefteq \mathfrak{G}$. Sei $\mathfrak{G}$ ein Gegenbeispiel minimaler Ordnung gegen Hilfssatz 1.3. Ferner sei $\mathfrak{N}$ ein kleinster Normalteiler von $\mathfrak{G}$, welcher die Voraussetzungen von 1.3 erfüllt, aber nicht p-nilpotent ist.

Sei $\mathfrak{M} \lhd \mathfrak{G}$, ferner $\mathfrak{M} < \mathfrak{N}$ und $\mathfrak{M}$ maximal mit diesen Eigenschaften. Dann haben wir $\mathfrak{M} \cap \mathfrak{P} \leqq \mathfrak{N} \cap \mathfrak{P} \leqq \Phi(\mathfrak{P})$. Die Voraussetzungen von 1.3 sind somit für $\mathfrak{M}$ erfüllt, nach unserer Annahme ist also $\mathfrak{M}$ p-nilpotent. Das p-Komplement $\mathfrak{K}$ von $\mathfrak{M}$ ist dann charakteristisch in $\mathfrak{M}$, daher normal in $\mathfrak{G}$. Ist $\mathfrak{K} \neq \mathfrak{E}$, so erfüllt $\mathfrak{G}/\mathfrak{K}$ wegen $\Phi(\mathfrak{P})\mathfrak{K}/\mathfrak{K} = \Phi(\mathfrak{P}\mathfrak{K}/\mathfrak{K})$ unsere Voraussetzungen. Also ist $\mathfrak{N}/\mathfrak{K}$ p-nilpotent, wegen $p \nmid |\mathfrak{K}|$ dann aber auch $\mathfrak{N}$. Somit gilt $\mathfrak{K} = \mathfrak{E}$ und daher $|\mathfrak{M}| = p^a$. Nun sind zwei Fälle zu unterscheiden:

Fall 1: Sei p kein Teiler von $|\mathfrak{N}/\mathfrak{M}|$. Nach einem bekannten Satz gibt es eine Untergruppe $\mathfrak{S}$ von $\mathfrak{N}$ mit $\mathfrak{N} = \mathfrak{M}\mathfrak{S}$ und $\mathfrak{M} \cap \mathfrak{S} = \mathfrak{E}$ (siehe Zassenhaus [13], S. 125). Wegen der Auflösbarkeit von $\mathfrak{M}$ sind alle solchen Gruppen $\mathfrak{S}$ unter $\mathfrak{N}$ konjugiert. Dies hat $\mathfrak{G} = \mathbf{N}(\mathfrak{S})\mathfrak{N} = \mathbf{N}(\mathfrak{S})\mathfrak{M}$ zur Folge. Aus $\mathfrak{M} \lhd \mathfrak{G}$ und $\mathfrak{M} = \mathfrak{M} \cap \mathfrak{P} \leqq \Phi(\mathfrak{P})$ ergibt sich $\mathfrak{M} \leqq \Phi(\mathfrak{G})$ (Gaschütz [3], S. 162, Satz 5), damit aber $\mathfrak{G} = \mathbf{N}(\mathfrak{S})$, also $\mathfrak{S} \lhd \mathfrak{G}$. Nun ist $\mathfrak{S}$ das gewünschte invariante p-Komplement für $\mathfrak{N}$.

Fall 2: Sei p ein Teiler von $|\mathfrak{N}/\mathfrak{M}|$. Ist $|\mathfrak{N}/\mathfrak{M}| = p^b$, so ist $|\mathfrak{N}| = p^{a+b}$ und wir sind fertig. Andernfalls ist $\mathfrak{N}/\mathfrak{M}$ nicht p-auflösbar, denn wegen der maximalen Wahl von $\mathfrak{M}$ ist $\mathfrak{N}/\mathfrak{M}$ eine charakteristisch einfache Gruppe. Ist

$\mathfrak{M} > \mathfrak{E}$, so erfüllt $\mathfrak{G}/\mathfrak{M}$ alle unsere Voraussetzungen; denn es gilt ja $\Phi(\mathfrak{P}\mathfrak{M}/\mathfrak{M}) = \Phi(\mathfrak{P})\mathfrak{M}/\mathfrak{M}$. Dann ist $\mathfrak{N}/\mathfrak{M}$ p-nilpotent, entgegen der eben getroffenen Feststellung. Also haben wir $\mathfrak{M} = \mathfrak{E}$ und $\mathfrak{N}$ ist charakteristisch einfach.

Da $\mathfrak{G}$ ein minimales Gegenbeispiel ist, gilt $\mathfrak{G} = \mathfrak{N}\mathfrak{P}$. Sei $\mathfrak{L}$ irgendeine Untergruppe von $\mathfrak{P}$ mit $\mathfrak{E} < \mathfrak{L} \triangleleft \mathbf{N}(\mathfrak{P})$. Wir setzen $\mathbf{N}(\mathfrak{L}) = \mathfrak{G}^*$. Ist $\mathfrak{G}^* = \mathfrak{G}$, so folgt $\mathfrak{L} \triangleleft \mathfrak{G}$. Dann erfüllen $\mathfrak{G}/\mathfrak{L}$ und $\mathfrak{N}\mathfrak{L}/\mathfrak{L}$ unsere Voraussetzungen, daher ist $\mathfrak{N}\mathfrak{L}/\mathfrak{L}$ p-nilpotent, somit $\mathfrak{N}$ p-auflösbar, entgegen der oben gemachten Feststellung. Also haben wir $\mathfrak{G}^* < \mathfrak{G}$. Wegen $\mathfrak{L} \triangleleft \mathfrak{P}$ gilt $\mathfrak{P} \leqq \mathbf{N}(\mathfrak{L}) = \mathfrak{G}^*$. Nun können wir auf die Gruppe $\mathfrak{G}^*$ und ihren Normalteiler $\mathfrak{N}^* = \mathbf{N}(\mathfrak{L}) \cap \mathfrak{N}$ unseren Satz anwenden, denn es ist ja $\mathfrak{N}^* \cap \mathfrak{P} \leqq \mathfrak{N} \cap \mathfrak{P} \leqq \Phi(\mathfrak{P})$. Wir gewinnen so die p-Nilpotenz von $\mathfrak{N}^*$, damit wegen $|\mathfrak{G}^*/\mathfrak{N}^*| = |\mathfrak{N}\mathbf{N}(\mathfrak{L})/\mathfrak{N}| = p^a$ auch die p-Nilpotenz von $\mathfrak{G}^*$. Somit bewirkt $\mathfrak{G}^* = \mathbf{N}(\mathfrak{L})$ auf $\mathfrak{L}$ nur Automorphismen von p-Potenzordnung. Dies gilt für alle $\mathfrak{L}$ mit $\mathfrak{L} \leqq \mathfrak{P}$ und $\mathfrak{L} \triangleleft \mathbf{N}(\mathfrak{P})$. Nehmen wir nun noch $p > 2$ an, so sind die Voraussetzungen des Satzes von J. THOMPSON [9] erfüllt und wir erhalten die p-Nilpotenz von $\mathfrak{G}$, damit auch die p-Nilpotenz von $\mathfrak{N}$.

Für $p = 2$ schließen wir so: Sei $\mathfrak{N} \cap \mathfrak{P} = \mathfrak{Q}$. Da $\mathfrak{N}$ nicht p-auflösbar ist, ist sicher $\mathbf{N}(\mathfrak{Q}) < \mathfrak{G}$. Außerdem haben wir $\mathfrak{N} \cap \mathfrak{P} = \mathfrak{Q} \triangleleft \mathfrak{P}$, also $\mathfrak{P} \leqq \mathbf{N}(\mathfrak{Q})$. Auf $\mathbf{N}(\mathfrak{Q})$ und $\mathbf{N}(\mathfrak{Q}) \cap \mathfrak{N}$ können wir nun unseren Satz anwenden. Demnach ist $\mathbf{N}(\mathfrak{Q}) \cap \mathfrak{N}$ 2-nilpotent. Da $\mathfrak{Q}$ als Untergruppe von $\Phi(\mathfrak{P})$ abelsch ist, liegt dann $\mathfrak{Q}$ im Zentrum von $\mathbf{N}(\mathfrak{Q}) \cap \mathfrak{N}$. Nach dem Satz von BURNSIDE (ZASSENHAUS [13], S. 133) ist dann $\mathfrak{N}$ selbst 2-nilpotent.

b) Beweis für $\mathfrak{N} \triangleleft\triangleleft \mathfrak{G}$:[1]) Sei wieder $\mathfrak{G}$ ein minimales Gegenbeispiel. Dann ist $\mathfrak{G}$ das Erzeugnis $\langle \mathfrak{N}, \mathfrak{P} \rangle$ von $\mathfrak{N}$ und $\mathfrak{P}$. Für jedes Element $P \in \mathfrak{P}$ gilt

$$(\mathfrak{N} \cap \mathfrak{P})^P \leqq \Phi(\mathfrak{P})^P = \Phi(\mathfrak{P}).$$

Nun folgt aus dem Wielandtschen Hauptsatz ([11], S. 218)

$$\langle \mathfrak{N}^P | P \in \mathfrak{P} \rangle \cap \mathfrak{P} = \langle (\mathfrak{N} \cap \mathfrak{P})^P | P \in \mathfrak{P} \rangle \leqq \Phi(\mathfrak{P}).$$

Ferner ist $\langle \mathfrak{N}^P | P \in \mathfrak{P} \rangle \trianglelefteq \langle \mathfrak{N}, \mathfrak{P} \rangle = \mathfrak{G}$. Nach a) ist nun $\langle \mathfrak{N}^P | P \in \mathfrak{P} \rangle$ p-nilpotent, also erst recht die Untergruppe $\mathfrak{N}$.

1.4. Zusatz.[2]) Im Falle 2. bei a) sei r eine von p verschiedene Primzahl, welche die Ordnung von $\mathfrak{N}$ teilt, $\mathfrak{R}$ eine r-Sylowgruppe von $\mathfrak{N}$. Da alle r-Sylowgruppen von $\mathfrak{N}$ schon unter $\mathfrak{N}$ konjugiert sind, gilt $\mathfrak{G} = \mathbf{N}(\mathfrak{R})\mathfrak{N}$. Indem wir nötigenfalls zu einer Konjugierten von $\mathfrak{R}$ übergehen, wählen wir nun $\mathfrak{R}$ so, daß $\mathbf{N}(\mathfrak{R}) \cap \mathfrak{P}$ eine p-Sylowgruppe von $\mathbf{N}(\mathfrak{R})$ ist. Wegen $\mathfrak{R} \triangleleft \mathfrak{G}$

[1]) Diesen Beweis verdanke ich Herrn WIELANDT.

[2]) Auf das Folgende hat mich Herr N. Itô hingewiesen.

und der Wahl von $\mathfrak{G}$ als kleinstes Gegenbeispiel ist $\mathfrak{G} = \mathfrak{N}\mathfrak{P}$. Dann ist auch $\mathfrak{G} = (\mathfrak{P} \cap \mathbf{N}(\mathfrak{N}))\mathfrak{N}$, daher

$$\mathfrak{P} = (\mathfrak{P} \cap \mathfrak{N})(\mathfrak{P} \cap \mathbf{N}(\mathfrak{N})) = \mathfrak{Q}(\mathfrak{P} \cap \mathbf{N}(\mathfrak{N})).$$

Wegen $\mathfrak{Q} = \mathfrak{N} \cap \mathfrak{P} \leqq \Phi(\mathfrak{P})$ liefert dies $\mathfrak{P} = \mathfrak{P} \cap \mathbf{N}(\mathfrak{N}) \leqq \mathbf{N}(\mathfrak{N})$. Da $\mathfrak{N}$ nicht in $\mathfrak{N}$ normal ist, denn $\mathfrak{N}$ ist charakteristisch einfach von zusammengesetzter Ordnung, haben wir $\mathbf{N}(\mathfrak{N}) < \mathfrak{G}$. Alle Voraussetzungen sind nun für die Gruppen $\mathbf{N}(\mathfrak{N})$ und $\mathbf{N}(\mathfrak{N}) \cap \mathfrak{N}$ erfüllt, also ist $\mathbf{N}(\mathfrak{N}) \cap \mathfrak{N}$ p-nilpotent.

Hilfssatz 1.3 ließe sich also ohne die Einschränkung für $p = 2$ und ohne die Hilfe des tiefliegenden Thompsonschen Satzes beweisen, wenn man zeigen könnte: Es gibt keine einfache nichtabelsche Gruppe $\mathfrak{N}$ mit den folgenden Eigenschaften: Es gibt einen Primteiler p der Ordnung von $\mathfrak{N}$ derart, daß für jeden Primteiler r von $|\mathfrak{N}|$ (auch $r = p$ ist zugelassen!) der Normalisator $\mathbf{N}(\mathfrak{R})$ einer r-Sylowgruppe $\mathfrak{R}$ von $\mathfrak{N}$ stets eine volle p-Sylowgruppe von $\mathfrak{N}$ enthält und p-nilpotent ist.

Die üblichen Verlagerungsmethoden lassen sich auf diese Frage nicht direkt anwenden, da sie nur die Sylownormalisatoren zu einer festen Primzahl betrachten, aber nicht die Beziehungen zwischen den Sylownormalisatoren zu verschiedenen Primzahlen berücksichtigen.

Hilfssatz 1.5 ist eine Dualisierung des folgenden bekannten Satzes: Bewirkt der Automorphismus A der p-Gruppe $\mathfrak{P}$ auf $\mathfrak{P}/\Phi(\mathfrak{P})$ den identischen Automorphismus, so hat A p-Potenzordnung.

1.5. Hilfssatz. *Sei $\mathfrak{P}$ eine p-Gruppe, $\mathfrak{P}$ abelsch für $p = 2$, beliebig für $p > 2$. Sei $\mathfrak{A}$ eine Gruppe von Automorphismen von $\mathfrak{P}$, welche jedes Element der Ordnung p von $\mathfrak{P}$ fest läßt. Dann ist $|\mathfrak{A}| = p^{\alpha}$.*

Beweis. Sei $A \in \mathfrak{A}$ und p kein Teiler der Ordnung von A. Wir haben zu zeigen, daß dann A der identische Automorphismus ist. Dies geschieht durch Induktion nach der Ordnung von $\mathfrak{P}$. Unsere Voraussetzung überträgt sich offenbar auf charakteristische Untergruppen von $\mathfrak{P}$. Also können wir annehmen, daß A auf der Frattini-Gruppe $\Phi(\mathfrak{P})$ von $\mathfrak{P}$ den identischen Automorphismus bewirkt. Nach dem Satz von MASCHKE zerfällt $\mathfrak{P}/\Phi(\mathfrak{P})$ in ein direktes Produkt von unter A invarianten Gruppen. Wir können offenbar annehmen, daß diese Zerlegung nur einen Faktor enthält. Nun betrachten wir die Untergruppe $\mathfrak{U} = \Phi(\mathfrak{P})\langle P^A P^{-1} | P \in \mathfrak{P}\rangle$ von $\mathfrak{P}$. Wegen $\mathfrak{U} \geqq \Phi(\mathfrak{P})$ ist $\mathfrak{U}$ invariant unter $\mathfrak{P}$. Aber $\mathfrak{U}$ ist auch invariant unter A, denn es gilt

$$(P^A P^{-1})^A = (P^A)^A (P^A)^{-1} \quad \text{mit} \quad P^A \in \mathfrak{P}.$$

Ist $\mathfrak{U} = \Phi(\mathfrak{P})$, so bewirkt A auf $\mathfrak{P}/\Phi(\mathfrak{P})$ den identischen Automorphismus. Dann ist A nach dem oben erwähnten Satz auch der identische Automorphis-

mus von $\mathfrak{P}$. Also können wir $\mathfrak{U} = \mathfrak{P}$ annehmen, sodaß die Elemente $P^A P^{-1}$ ganz $\mathfrak{P}$ erzeugen.

Wir zeigen nun, daß $\Phi(\mathfrak{P})$ im Zentrum $Z(\mathfrak{P})$ von $\mathfrak{P}$ liegt: Sei $Y \in \Phi(\mathfrak{P})$ und $P \in \mathfrak{P}$. Dann ist $Y^A = Y$, daher $P^{-1}YP \in \Phi(\mathfrak{P})$ und $(P^{-1}YP)^A = P^{-A}YP^A = P^{-1}YP$. Somit ist $P^A P^{-1}$ vertauschbar mit Y. Da die $P^A P^{-1}$ ganz $\mathfrak{P}$ erzeugten, folgt $Y \in Z(\mathfrak{P})$.

Also hat $\mathfrak{P}$ höchstens die Klasse 2. In $\mathfrak{P}$ gelten dann bekanntlich die Relationen

$$(X, Y)^p = (X^p, Y) \quad \text{und} \quad (XY)^p = X^p Y^p (X, Y)^{\binom{p}{2}}.$$

Aus $X^p \in \Phi(\mathfrak{P}) \leqq Z(\mathfrak{P})$ folgt jetzt $(X, Y)^p = E$ für alle X, Y aus $\mathfrak{P}$. Für $p > 2$ liefert dies $(XY)^p = X^p Y^p$, für $p = 2$ ist diese Relation trivial, da dann $\mathfrak{P}$ nach unserer Voraussetzung abelsch ist. Da $\mathfrak{P}/\Phi(\mathfrak{P})$ unter A irreduzibel ist, können wir annehmen, daß $\Phi(\mathfrak{P})$ die genaue Fixpunktmenge von A ist. Nun erhalten wir für $X \in \mathfrak{P}$ die Gleichung $(X^p)^A = (X^A)^p = X^p$, also $(X^A X^{-1})^p = (X^A)^p X^{-p} = E$, somit $X^A \equiv X \bmod \Phi(\mathfrak{P})$. Also bewirkt A auf $\mathfrak{P}/\Phi(\mathfrak{P})$ den identischen Automorphismus, dann nach dem eingangs erwähnten Satz aber auch auf $\mathfrak{P}$.

Den Hinweis darauf, daß Hilfssatz 1.5 ohne die Voraussetzung der Regularität von $\mathfrak{P}$ (im Sinne von P. HALL) gilt, verdanke ich Herrn N. ITÔ. Der vorliegende Beweis verwendet die wohlbekannte Schlußweise, mit welcher die Struktur der nichtnilpotenten Gruppen mit lauter nilpotenten Untergruppen bestimmt werden kann.

Die beiden folgenden Hilfssätze sind bekannt (siehe etwa N. ITÔ [6] und K. IWASAWA [7]).

1.6. Hilfssatz. *Ist jede eigentliche Untergruppe von $\mathfrak{G}$ p-nilpotent, aber die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ nicht invariant in $\mathfrak{G}$, so ist $\mathfrak{G}$ selbst p-nilpotent.*

Beweis. Durch Induktion nach $|\mathfrak{G}|$.

a) $\mathfrak{G}$ ist p-normal im Sinne von GRÜN: Sonst gäbe es nach einem Satz von BURNSIDE (siehe [1], S. 156) eine p-Untergruppe $\mathfrak{P}_1$ von $\mathfrak{P}$, auf welcher ein Element Q von zu p teilerfremder Ordnung einen nichttrivialen Automorphismus bewirkt. $\mathfrak{P}_1\langle Q\rangle$ ist echte Untergruppe von $\mathfrak{G}$, da in $\mathfrak{G}$ nach der Voraussetzung die p-Sylowgruppe nicht invariant ist. Dann ist nach unserer Annahme $\mathfrak{P}_1\langle Q\rangle$ p-nilpotent, also wirkt Q trivial auf $\mathfrak{P}_1$, entgegen der obigen Annahme. Somit ist $\mathfrak{G}$ p-normal.

b) Nun betrachten wir $\mathbf{N}(Z(\mathfrak{P}))$. Ist $\mathbf{N}(Z(\mathfrak{P})) < \mathfrak{G}$, so ist $\mathbf{N}(Z(\mathfrak{P}))$ p-nilpotent, hat also nichttriviale p-Faktorgruppen. Nach dem Satz von GRÜN (siehe [13], S. 135) hat dann auch $\mathfrak{G}$ eine nichttriviale p-Faktorgruppe. Also

existiert ein Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ mit $|\mathfrak{G}/\mathfrak{N}| = p^a > 1$. Nach unserer Annahme ist $\mathfrak{N}$ p-nilpotent, dann aber $\mathfrak{G}$ ebenso.

Es bleibt der Fall $\mathbf{N}(Z(\mathfrak{P})) = \mathfrak{G}$, also $Z(\mathfrak{P}) \lhd \mathfrak{G}$. Dann können wir den Satz auf $\mathfrak{G}/Z(\mathfrak{P})$ anwenden und erhalten ein $\mathfrak{N} \lhd \mathfrak{G}$ mit $p \nmid |\mathfrak{N}/Z(\mathfrak{P})|$ und $|\mathfrak{G}/\mathfrak{N}| = p^b$. Wegen $Z(\mathfrak{P}) \neq \mathfrak{P}$ — denn $\mathfrak{P}$ ist nicht invariant in $\mathfrak{G}$ — haben wir $\mathfrak{N} < \mathfrak{G}$. Also ist $\mathfrak{N}$ p-nilpotent, dann aber auch $\mathfrak{G}$.

1.7. Hilfssatz. *Liegt jedes Element der Ordnung p von $\mathfrak{G}$ im Zentrum von $\mathfrak{G}$, ist $p > 2$ oder die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ abelsch, so ist $\mathfrak{G}$ p-nilpotent.*

Beweis. Durch Induktion nach $|\mathfrak{G}|$. Wir können annehmen, daß jede echte Untergruppe von $\mathfrak{G}$ p-nilpotent ist. Ist $\mathfrak{G}$ selbst nicht p-nilpotent, so erhalten wir $\mathfrak{P} \lhd \mathfrak{G}$ nach 1.6. Aber nach 1.5 erleidet $\mathfrak{P}$ durch $\mathfrak{G}$ keine Automorphismen von zu p teilerfremder Ordnung. Also ist $\mathfrak{G} = \mathfrak{P} \times \mathfrak{S}$ (mit einem p-Komplement $\mathfrak{S}$), somit $\mathfrak{G}$ p-nilpotent.

Auf die zusätzliche Voraussetzung für $p = 2$ kann nicht verzichtet werden; dies zeigt das Beispiel der Quaternionengruppe der Ordnung 8, welche einen Automorphismus der Ordnung 3 besitzt, der auf der einzigen Untergruppe der Ordnung 2 trivial wirkt.

Nun folgt die Dualisierung von Hilfssatz 1.3:

1.8. Hilfssatz. *Die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ sei abelsch für $p = 2$, sonst beliebig und es sei $\Omega_1(\mathfrak{P}) \leqq Z(\mathfrak{P})$. Es sei $\mathfrak{N}$ eine subnormale Untergruppe von $\mathfrak{G}$ mit $\Omega_1(\mathfrak{P}) \leqq \mathfrak{N}$. Dann liegen zwischen $\mathfrak{N}$ und $\mathfrak{G}$ nur p-auflösbare Kompositionsfaktoren von $\mathfrak{G}$.*

Beweis. a) Zunächst sei $\mathfrak{N} \trianglelefteq \mathfrak{G}$. Dann ist $\mathfrak{N} \cap \mathfrak{P} = \mathfrak{Q}$ eine p-Sylowgruppe von $\mathfrak{N}$. Da nach dem Sylowschen Satz alle unter $\mathfrak{G}$ Konjugierten von $\mathfrak{Q}$ schon unter $\mathfrak{N}$ konjugiert sind, erhalten wir $\mathfrak{G} = \mathbf{N}(\mathfrak{Q})\mathfrak{N}$ und daraus

$$\mathfrak{G}/\mathfrak{N} \cong \mathbf{N}(\mathfrak{Q})/\mathbf{N}(\mathfrak{Q}) \cap \mathfrak{N}.$$

Es genügt daher der Nachweis, daß $\mathbf{N}(\mathfrak{Q})$ p-auflösbar ist. Wir können uns also weiterhin auf die Betrachtung von $\mathbf{N}(\mathfrak{Q})$ beschränken, d. h. wir können $\mathfrak{N} = \mathfrak{Q} \trianglelefteq \mathfrak{G}$ annehmen.

Wegen $\Omega_1(\mathfrak{P}) \leqq \mathbf{Z}(\mathfrak{P})$ gilt nun $\mathfrak{P} \leqq \mathbf{C}(\Omega_1(\mathfrak{P}))$, und wegen $\Omega_1(\mathfrak{P}) \leqq \mathfrak{Q}$ ist $\Omega_1(\mathfrak{P}) = \Omega_1(\mathfrak{Q}) \trianglelefteq \mathfrak{G}$. Mithin ist p kein Teiler der Ordnung von $\mathfrak{G}/\mathbf{C}(\Omega_1(\mathfrak{P}))$, und wir können $\mathfrak{G} = \mathbf{C}(\Omega_1(\mathfrak{P}))$ annehmen. Dies gilt für alle p-Sylowgruppen $\mathfrak{P}$ von $\mathfrak{G}$. Also sind die Voraussetzungen von Hilfssatz 1.7 erfüllt und $\mathfrak{G}$ ist p-nilpotent.

b) Nun sei nur $\mathfrak{N} \lhd\lhd \mathfrak{G}$. Dann gibt es subnormale Untergruppen $\mathfrak{N}_i$ von $\mathfrak{G}$ mit $\mathfrak{N} = \mathfrak{N}_0 \lhd \mathfrak{N}_1 \lhd \cdots \lhd \mathfrak{N}_s = \mathfrak{G}$. Wenden wir a) auf die Paare $\mathfrak{N}_{i+1}, \mathfrak{N}_i$ an, so erhalten wir, daß $\mathfrak{N}_{i+1}/\mathfrak{N}_i$ p-auflösbar ist. Dies ergibt die Behauptung.

Die volle Dualisierung von 1.3 für $\mathfrak{N} \triangleleft \mathfrak{G}$ würde besagen, daß $\mathfrak{G}/\mathfrak{N}$ eine invariante p-Sylowgruppe hat; einfachste Beispiele zeigen, daß dies selbst bei zyklischem $\mathfrak{P}$ nicht immer zutrifft.

1.9. Beispiele. a) Die Einschränkung für $p=2$ in 1.8 kann nicht gestrichen werden; dies zeigt die Gruppe der Ordnung 120, welche nichtzerfallende Erweiterung einer Gruppe der Ordnung 2 mit der alternierenden Gruppe $\mathfrak{A}_5$ ist; die 2-Sylowgruppe ist in diesem Falle eine Quaternionengruppe der Ordnung 8.

b) Auch die Voraussetzung $\Omega_1(\mathfrak{P}) \leqq \mathbf{Z}(\mathfrak{P})$ kann nicht gestrichen werden, wie folgendes Beispiel beweist:

Wir betrachten die Gruppe $\mathfrak{G}$ aller Matrizen vom Grade 2, deren Matrixelemente dem Restklassenring mod p^2 entnommen sind und deren Determinante zu p teilerfremd ist. Die Abbildung dieser Matrizen auf ihre Reste mod p ist ein Homomorphismus von $\mathfrak{G}$ auf die volle lineare Gruppe $GL(2,p)$. Der Kern $\mathfrak{K}$ dieses Homomorphismus besteht genau aus den Matrizen der Gestalt $E+pA$, ist also elementar abelsch von der Ordnung p^4. Dann hat die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ die Ordnung p^5, ist daher für $p>3$ regulär (HALL [4], S. 73). Das Element $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ hat die Ordnung p^2. Somit hat $\mathfrak{P}$ den Exponenten p^2, woraus mit $\mathfrak{K} \leqq \Omega_1(\mathfrak{P}) < \mathfrak{P}$ und $|\mathfrak{P}/\mathfrak{K}| = p$ folgt, daß $\mathfrak{K} = \Omega_1(\mathfrak{P})$ ist. Die Voraussetzungen von Hilfssatz 1.8 sind nun bis auf $\Omega_1(\mathfrak{P}) \leqq \mathbf{Z}(\mathfrak{P})$ erfüllt, aber $\mathfrak{G}/\mathfrak{K} \cong GL(2,p)$ ist bekanntlich für $p>3$ nicht p-auflösbar.

§ 2. Untersuchung von $s_{\mathfrak{G}}\mathfrak{P}$

2.1. Satz. *Sei p^2 ein Teiler der Ordnung von $\mathfrak{G}$.*

a) *Ist $p>2$ oder $\Phi(\mathfrak{P})$ abelsch, liegen ferner alle maximalen Untergruppen von $\mathfrak{P}$ in $s_{\mathfrak{G}}\mathfrak{P}$, so ist $\mathfrak{G}$ p-auflösbar von der p-Länge 1; nach Satz* (A) *von Wielandt ist dann $s_{\mathfrak{G}}\mathfrak{P} = s\mathfrak{P}$, d. h. jede Untergruppe von $\mathfrak{P}$ liegt $s_{\mathfrak{G}}\mathfrak{P}$.*

b) *Ist $\Omega_1(\mathfrak{P}) \leqq \mathbf{Z}(\mathfrak{P})$, ferner $\mathfrak{P}$ abelsch für $p=2$ und liegen alle minimalen Untergruppen von $\mathfrak{P}$ in $s_{\mathfrak{G}}\mathfrak{P}$, so ist $\mathfrak{G}$ p-auflösbar.*

Beweis. a) Wir können annehmen, daß $\mathfrak{G}$ p-reduziert ist. Seien die $\mathfrak{A}_i$ die sämtlichen maximalen Untergruppen von $\mathfrak{P}$, also $\Phi(\mathfrak{P}) = \cap \mathfrak{A}_i$. Nach unserer Voraussetzung gibt es zu jedem $\mathfrak{A}_i$ mindestens ein $\mathfrak{N} \triangleleft\triangleleft \mathfrak{G}$ mit $\mathfrak{N} \cap \mathfrak{P} = \mathfrak{A}_i$. Wir betrachten die Menge M aller subnormalen Untergruppen $\mathfrak{N}$ von $\mathfrak{G}$ mit der Eigenschaft, daß $\mathfrak{N} \cap \mathfrak{P}$ eines der $\mathfrak{A}_i$ ist. Diese Menge enthält mit einem $\mathfrak{N}$ alle seine Konjugierten. Daher ist $\mathfrak{K} = \bigcap_M \mathfrak{N}$ ein Normaltei-

ler von $\mathfrak{G}$ mit $\mathfrak{K} \cap \mathfrak{P} = \cap \mathfrak{A}_i = \Phi(\mathfrak{P})$. Nach Hilfssatz 1.3 ist $\mathfrak{K}$ p-nilpotent. Da $\mathfrak{G}$ p-reduziert ist, also keine nichttrivialen Normalteiler von zu p teilerfremder Ordnung hat, folgt $|\mathfrak{K}| = p^\alpha$.

$\mathfrak{G}/\mathfrak{K}$ hat elementar abelsche p-Sylowgruppe $\mathfrak{P}/\Phi(\mathfrak{P})$. Jede Untergruppe von $\mathfrak{P}/\Phi(\mathfrak{P})$ ist Durchschnitt von einigen maximalen Untergruppen $\mathfrak{A}_i/\Phi(\mathfrak{P})$ von $\mathfrak{P}/\Phi(\mathfrak{P})$. Wegen $\mathfrak{A}_i \in s_\mathfrak{G}\mathfrak{P}$ ist auch $\mathfrak{A}_i/\Phi(\mathfrak{P}) \in s_{\mathfrak{G}/\mathfrak{K}}\mathfrak{P}/\Phi(\mathfrak{P})$. Da $s_{\mathfrak{G}/\mathfrak{K}}\mathfrak{P}/\Phi(\mathfrak{P})$ ein Verband ist, liegt also auch jede Untergruppe von $\mathfrak{P}/\Phi(\mathfrak{P})$ in $s_{\mathfrak{G}/\mathfrak{K}}\mathfrak{P}/\Phi(\mathfrak{P})$. Ist nun $|\mathfrak{P}/\Phi(\mathfrak{P})| = p$, so ist $\mathfrak{P}$ nach dem Burnsideschen Basissatz zyklisch (ZASSENHAUS [13], S. 105), wegen $p^2 \| \mathfrak{P}|$ und $\Phi(\mathfrak{P}) \in s_\mathfrak{G}\mathfrak{P}$ ist dann sicher $s_\mathfrak{G}\mathfrak{P} \neq s_0\mathfrak{P}$, daher $\mathfrak{G}$ p-auflösbar von der p-Länge 1 nach Satz (B) von WIELANDT. Ist aber $|\mathfrak{P}/\Phi(\mathfrak{P})| \geqq p^2$, so können wir Satz (A) auf $\mathfrak{G}/\mathfrak{K}$ anwenden und erhalten, daß $\mathfrak{G}/\mathfrak{K}$ die p-Länge 1 hat. Da $\mathfrak{G}$ p-reduziert ist, gibt es dann einen Normalteiler $\mathfrak{M}$ von $\mathfrak{G}$ mit $p \nmid |\mathfrak{M}/\mathfrak{K}|$ und $|\mathfrak{G}/\mathfrak{M}| = p^b$. Wie beim Beweis von 1.3 gibt es nun ein $\mathfrak{S}$ mit $\mathfrak{M} = \mathfrak{K}\mathfrak{S}$ und $\mathfrak{K} \cap \mathfrak{S} = \mathfrak{E}$, und wieder gilt $\mathfrak{G} = \mathfrak{K}\mathbf{N}(\mathfrak{S})$. Aus $\mathfrak{K} = \Phi(\mathfrak{P})$ und $\mathfrak{K} \lhd \mathfrak{G}$ ergibt sich $\mathfrak{K} \leqq \Phi(\mathfrak{G})$ und dann $\mathfrak{G} = \mathbf{N}(\mathfrak{S})$, also $\mathfrak{S} \trianglelefteq \mathfrak{G}$. Da $\mathfrak{G}$ p-reduziert ist, folgt nun $\mathfrak{S} = \mathfrak{E}$. Also hat $\mathfrak{G}$ die p-Länge 1.

b) Seien die $\mathfrak{B}_i$ die sämtlichen minimalen Untergruppen von $\mathfrak{P}$, also $\langle \mathfrak{B}_i \rangle = \Omega_1(\mathfrak{P}) \in s_\mathfrak{G}\mathfrak{P}$. Somit gibt es ein $\mathfrak{N} \lhd\lhd \mathfrak{G}$ mit $\mathfrak{N} \cap \mathfrak{P} = \Omega_1(\mathfrak{P})$. Nach Hilfssatz 1.8 befinden sich zwischen $\mathfrak{G}$ und $\mathfrak{N}$ nur p-auflösbare Kompositionsfaktoren von $\mathfrak{G}$.

Wir betracten nun $\mathfrak{N}$ mit der elementar abelschen p-Sylowgruppe $\Omega_1(\mathfrak{P})$. Jede Untergruppe $\mathfrak{A}$ von $\Omega_1(\mathfrak{P})$ ist Vereinigung einiger minimaler Untergruppen $\mathfrak{B}_i$, liegt also in $s_\mathfrak{N}\Omega_1(\mathfrak{P})$. Ist $|\Omega_1(\mathfrak{P})| > p$, so folgt mit Satz (A) sofort $l_p(\mathfrak{N}) = 1$. Ist aber $|\Omega_1(\mathfrak{P})| = p$, so ist $\mathfrak{P}$ zyklisch, und wegen $p^2 \| \mathfrak{P}|$ liefert nun Satz (B) die Aussage $l_p(\mathfrak{G}) = 1$.

Wir wissen nun, daß $\mathfrak{N}$ und auch alle Kompositionsfaktoren oberhalb $\mathfrak{N}$ p-auflösbar sind. Daher ist $\mathfrak{G}$ selbst p-auflösbar.

2.2. Hilfssatz. *Es sei $\mathfrak{G}$ p-reduziert und die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ sei regulär. Dann ist jeder nichtabelsche Hauptfaktor von $\mathfrak{G}$ mit durch p teilbarer Ordnung einfach.*

Beweis. Durch Übergang zu einer Faktorgruppe von $\mathfrak{G}$ können wir erreichen, daß der vorgegebene Hauptfaktor ein minimaler Normalteiler von $\mathfrak{G}$ wird. Dieser ist direktes Produkt von einfachen nichtabelschen, isomorphen Gruppen $\mathfrak{N}_i$. Diese Zerlegung in nichtabelsche Faktoren ist eindeutig, die $\mathfrak{N}_i$ werden daher bei inneren Automorphismen von $\mathfrak{G}$ nur permutiert. Sei $\mathfrak{K}$ derjenige Normalteiler von $\mathfrak{G}$, welcher auf den $\mathfrak{N}_i$ die identische Permutation hervorruft. Angenommen, es sei $\mathfrak{P} \not\leqq \mathfrak{K}$. Dann gibt es ein $P \in \mathfrak{P}$, welches auf den $\mathfrak{N}_i$ einen p-Zyklus hervorruft, d. h. es gibt $\mathfrak{N}_1, \ldots, \mathfrak{N}_p$

mit $\mathfrak{N}_i^P = \mathfrak{N}_{i+1}$ und $\mathfrak{N}_p^P = \mathfrak{N}_1$. Sei nun $E \neq N_1 \in \mathfrak{N}_1$ mit $N_1^p = E$. Wir setzen

$$N_i = N_{i-1}^P = N_1^{P^{i-1}} \qquad (1 < i \leqq p)$$

und betrachten die Untergruppe $\mathfrak{A} = \langle P, N_1, \ldots, N_p \rangle$ von $\mathfrak{P}$. Die Kommutatorgruppe $\mathfrak{A}'$ von $\mathfrak{A}$ liegt in der elementar abelschen Gruppe $\langle N_1, \ldots, N_p \rangle$, hat daher nur Elemente der Ordnung p. Als Untergruppe der regulären Gruppe $\mathfrak{P}$ ist auch $\mathfrak{A}$ regulär. Dies erfordert $(N_1 P^{-1})^p = N_1^p P^{-p} = P^{-p}$. Andererseits gilt aber

$$(N_1 P^{-1})^p = N_1^{E+P+\cdots+P^{p-1}} P^{-p} = N_1 N_2 \cdots N_p P^{-p} \neq P^{-p}.$$

Also ist doch $\mathfrak{P} \leqq \mathfrak{R}$ und dann $\mathfrak{G} = \mathfrak{R}$ wegen der p-Reduziertheit von $\mathfrak{G}$. Da $\mathfrak{N}$ minimaler Normalteiler von $\mathfrak{G}$ war, ist dann $\mathfrak{N}$ einfach.

2.3. Satz. *Es sei d die minimale Erzeugendenanzahl von $\mathfrak{P}$ (also $|\mathfrak{P}/\Phi(\mathfrak{P})| = p^d$). Bezeichnen wir als p-Kompositionsfaktoren von $\mathfrak{G}$ die Kompositionsfaktoren von durch p teilbarer Ordnung, so gilt:*

a) *Ist $p \neq 2$, so hat $\mathfrak{G}$ höchstens d paarweise nichtisomorphe, nichtauflösbare p-Kompositionsfaktoren; genauer: die Anzahl der nichtauflösbaren Hauptfaktoren von durch p teilbarer Ordnung ist höchstens d.*

b) *Ist $\mathfrak{P}$ regulär, so hat $\mathfrak{G}$ höchstens d nichtauflösbare p-Kompositionsfaktoren.*

Beweis. a) Wir beweisen den Satz durch Induktion nach der Ordnung von $\mathfrak{G}$. Die Voraussetzungen übertragen sich offenbar auf alle Faktorgruppen von $\mathfrak{G}$. Sei $\mathfrak{N}$ ein minimaler Normalteiler von $\mathfrak{G}$. Ist $\mathfrak{N} \cap \mathfrak{P} \leqq \Phi(\mathfrak{P})$, so ist $\mathfrak{N}$ nach Hilfssatz 1.3 p-nilpotent, enthält daher nur p-auflösbare Kompositionsfaktoren von $\mathfrak{G}$. Da für $\mathfrak{G}/\mathfrak{N}$ der Satz nach unserer Induktionsannahme gilt, sind wir in diesem Falle schon fertig.

Ist aber $\mathfrak{N} \cap \mathfrak{P} \not\leqq \Phi(\mathfrak{P})$, so enthält $\mathfrak{N} \cap \mathfrak{P}$ ein Element aus einem geeigneten minimalen Erzeugendensystem von $\mathfrak{P}$; denn jedes nicht in $\Phi(\mathfrak{P})$ liegende Element von $\mathfrak{P}$ ist Mitglied eines minimalen Erzeugendensystems von $\mathfrak{P}$. Dann haben wir $d(\mathfrak{P}\mathfrak{N}/\mathfrak{N}) \leqq d-1$. Nach unserer Induktionsannahme hat nun $\mathfrak{G}/\mathfrak{N}$ höchstens $d-1$ nichtisomorphe, nichtauflösbare p-Hauptfaktoren. Die charakteristisch einfach Gruppe $\mathfrak{N}$ trägt höchstens einen weiteren solchen Hauptfaktor bei.

b) Der Beweis verläuft zunächst wie in Teil a). Die Bedingung $p \neq 2$ ist nun überflüssig, da eine reguläre 2-Gruppe stets abelsch ist und für abelsche p-Sylowgruppen der Hilfssatz 1.3 ohne Einschränkung zur Verfügung steht. Da man beim Beweis annehmen kann, dass $\mathfrak{G}$ p-reduziert ist, ist der minimale Normalteiler $\mathfrak{N}$ (sofern er überhaupt nichtabelsch ist und zu unserer Zählung etwas beiträgt) nach 2.2 einfach, liefert daher genau einen nichtabelschen p-Kompositionsfaktor.

2.4. Beispiele. a) Wir konstruieren eine p-auflösbare Gruppe der p-Länge 2 derart, daß alle minimalen Untergruppen von $\mathfrak{P}$ in $s_{\mathfrak{G}}\mathfrak{P}$ liegen. Sei $p = 2^n + 1$ eine Fermatsche Primzahl und $\mathfrak{H}$ die von HALL—HIGMAN konstruierte Gruppe der Ordnung $p^{p-1}2^{2n+1}$, welche eine invariante, elementar abelsche Untergruppe $\mathfrak{L}$ der Ordnung p^{p-1} und einen Automorphismus σ der Ordnung p hat ([5], S. 32). Wir bilden $\mathfrak{R} = \mathfrak{H} \times \mathfrak{Z}$ mit $|\mathfrak{Z}| = p$ und dann die folgende nichtzerfallende Erweiterung von $\mathfrak{R}$ mit einer zyklischen Gruppe der Ordnung p:

$$H^P = H^\sigma \quad \text{für} \quad H \in \mathfrak{H}, \quad Z^P = Z \quad \text{für} \quad \mathfrak{Z} = \langle Z \rangle \quad \text{und} \quad P^p = Z.$$

Die entstehende Gruppe $\mathfrak{G}$ hat sicher die p-Länge 2, denn $\mathfrak{G}/\langle Z \rangle$ ist isomorph zu der von HALL—HIGMAN angegebenen Gruppe der p-Länge 2 ([5], S. 32). Die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ hat die Ordnung p^{p+1} und mindestens ein Zentrum der Ordnung p^2, ist daher sicher regulär (siehe [4], S. 73). Da $\mathfrak{P}$ den Exponenten p^2 hat, ist $\Omega_1(\mathfrak{P}) = \mathfrak{R}$. Also sind alle minimalen Untergruppen von $\mathfrak{P}$ subnormal in $\mathfrak{G}$.

b) Wir bilden das direkte Produkt von 7 alternierenden Gruppen vom Grad 7 und erweitern dies zerfallend mit der einfachen Gruppe der Ordnung 168, welche die Faktoren transitiv vertauscht. Die entstehende Gruppe zeigt, daß die Regularitätsvoraussetzung in 2.3 b) nicht überflüssig ist.

§ 3. Gruppen mit abelscher p-Sylowgruppe

3.1. Satz. *Sei $\mathfrak{P}$ abelsch und $\mathfrak{H} \in s_{\mathfrak{G}}\mathfrak{P}$. Dann gilt:* a) *Ist $\mathfrak{H} \leqq \Phi(\mathfrak{P})$, so liegen alle Untergruppen von $\mathfrak{H}$ in $s_{\mathfrak{G}}\mathfrak{P}$.* b) *Ist $\Omega_1(\mathfrak{P}) \leqq \mathfrak{H}$, so liegen alle Obergruppen von $\mathfrak{H}$ in $s_{\mathfrak{G}}\mathfrak{P}$.* c) *Ist schließlich $\Omega_1(\mathfrak{P}) \leqq \mathfrak{H} \leqq \Phi(\mathfrak{P})$, so liegen alle Untergruppen von $\mathfrak{P}$ in $s_{\mathfrak{G}}\mathfrak{P}$ (und $\mathfrak{G}$ ist daher p-auflösbar von der p-Länge 1).*

Beweis. a) Nach Voraussetzung gibt es ein $\mathfrak{N} \lhd\lhd \mathfrak{G}$ mit $\mathfrak{N} \cap \mathfrak{P} = \mathfrak{H} \leqq \Phi(\mathfrak{P})$. Nach Hilfssatz 1.3 ist dann $\mathfrak{N}$ p-nilpotent, hat also insbesondere p-Länge 1. Nach Satz (A) liegen dann alle Untergruppen von $\mathfrak{H}$ in $s_{\mathfrak{N}}\mathfrak{H}$, wegen der Transitivität der Subnormalität dann aber auch in $s_{\mathfrak{G}}\mathfrak{P}$.

b) Nun gibt es ein $\mathfrak{N} \lhd\lhd \mathfrak{G}$ mit $\mathfrak{P} \cap \mathfrak{N} = \mathfrak{H} \geqq \Omega_1(\mathfrak{P})$. Nach Hilfssatz 1.8 liegen oberhalb von $\mathfrak{N}$ nur p-auflösbare Kompositionsfaktoren von $\mathfrak{G}$. Ist $\mathfrak{K}$ der Durchschnitt aller Konjugierten von $\mathfrak{N}$ in $\mathfrak{G}$, so liegen auch oberhalb von $\mathfrak{K}$ nur p-auflösbare Kompositionsfaktoren von $\mathfrak{G}$ (WIELANDT [10], S. 214), d. h. $\mathfrak{G}/\mathfrak{K}$ ist p-auflösbar. Da $\mathfrak{G}/\mathfrak{K}$ abelsche p-Sylowgruppe hat, hat $\mathfrak{G}/\mathfrak{K}$ die p-Länge 1 (HALL—HIGMAN [5], S. 7) und nach Satz (A) von WIELANDT liegt jede Obergruppe von $\mathfrak{K} \cap \mathfrak{P}$ in $s_{\mathfrak{G}}\mathfrak{P}$. Wegen $\mathfrak{K} \cap \mathfrak{P} \leqq \mathfrak{H}$ folgt daraus die Behauptung.

c) Aus a) und b) zusammen folgt die p-Auflösbarkeit von $\mathfrak{G}$. Dann hat $\mathfrak{G}$ die p-Länge 1 und Satz (A) ergibt die Behauptung.

Die Voraussetzung von Satz 3. 1 c) ist offensichtlich nur dann erfüllbar, wenn $\Omega_1(\mathfrak{S}) \leqq \Phi(\mathfrak{P})$ gilt, d. h. wenn die abelsche Gruppe $\mathfrak{P}$ keine Invariante p hat. Wir werden auch weiterhin sehen, daß die Invarianten p besondere Schwierigkeiten bereiten. Schon in WIELANDT [11] blieb ja bei der Betrachtung elementar abelscher Sylowgruppen vom Typ (p, p) die Frage offen, ob der Verband $s_{\mathfrak{G}}\mathfrak{P}$ eine Kette der Länge 2 sein kann.

Satz 3. 1 umfaßt offenbar den Satz (B) von WIELANDT: Ist nämlich $\mathfrak{P}$ zyklisch von einer Ordnung $\geqq p^2$, so folgt aus $\mathfrak{E} < \mathfrak{H} < \mathfrak{P}$ auch $\Omega_1(\mathfrak{P}) \leqq \mathfrak{H} \leqq \Phi(\mathfrak{P})$.

3. 2. Hilfssatz. *Hat $\mathfrak{G}$ abelsche p-Sylowgruppe $\mathfrak{P}$, so gilt*

$$\mathfrak{G}' \cap \mathbf{Z}(\mathfrak{G}) \cap \mathfrak{P} = \mathfrak{E}.$$

Beweis. Sei $\mathfrak{G} = \sum_1^n G_i\mathfrak{P}$ eine Zerlegung von $\mathfrak{G}$ in Linksnebenklassen nach $\mathfrak{P}$; dabei ist $p \nmid n$. Ist G ein Element aus $\mathfrak{G}$, so seien die $P_i(G) \in \mathfrak{P}$ eindeutig bestimmt durch $GG_i = G_iP_i(G)$. Dann ist die Abbildung $G \to V(G) = \prod_{i=1}^n P_i(G)$ bekanntlich ein Homomorphismus von $\mathfrak{G}$ in $\mathfrak{P}$, die Verlagerung von $\mathfrak{G}$ in $\mathfrak{P}$.

Ist nun $G \in \mathfrak{G}'$, so ist $V(G) = E$, denn es handelt sich um einen Homomorphismus in die abelsche Gruppe $\mathfrak{P}$. Ist $G \in \mathbf{Z}(\mathfrak{G}) \cap \mathfrak{P}$, so haben wir $GG_i = G_iG$, daher $P_i(G) = G$ für alle i und dann $V(G) = G^n$. Gilt schließlich $G \in \mathfrak{G}' \cap \mathbf{Z}(\mathfrak{G}) \cap \mathfrak{P}$, so folgt $V(G) = G^n = E$, also $G = E$.

Dieser Hilfssatz wurde von D. TAUNT auf anderem Wege für auflösbare Gruppen $\mathfrak{G}$ bewiesen (TAUNT [8]); wie ich erfuhr, ist der obenstehende Beweis auch den Herren P. HALL und D. TAUNT bekannt.

3. 3. Satz. *Hat $\mathfrak{G}$ abelsche p-Sylowgruppe $\mathfrak{P}$, so gibt es einen Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ mit den folgenden Eigenschaften: $\mathfrak{G}/\mathfrak{N}$ ist p-auflösbar und jeder abelsche Kompositionsfaktor von $\mathfrak{N}$ hat zu p teilerfremde Ordnung. Es gibt also stets eine Kompositionsreihe von $\mathfrak{G}$, in der alle Kompositionsfaktoren der Ordnung p höher stehen als alle nichtabelschen Kompositionsfaktoren mit durch p teilbarer Ordnung. (Über die Position der Kompositionsfaktoren von zu p teilerfremder Ordnung kann natürlich nichts ausgesagt werden.)*

Beweis. Wir führen den Beweis durch Induktion nach der Ordnung von $\mathfrak{G}$. Ist $\mathfrak{G}' = \mathfrak{E}$, so ist $\mathfrak{G}$ abelsch und der Satz trivial. Andernfalls sei $\mathfrak{R}$ ein in $\mathfrak{G}'$ liegender minimaler Normalteiler von $\mathfrak{G}$. Nach unserer Induktionsannahme ist der Satz für $\mathfrak{G}/\mathfrak{R}$ erfüllt. Hat $\mathfrak{R}$ eine zu p teilerfremde Ordnung

oder ist $\mathfrak{R}$ direktes Produkt von einfachen nichtabelschen Gruppen mit durch p teilbarer Ordnung, so ist der Satz offensichtlich auch für $\mathfrak{G}$ richtig. Es bleibt der Fall zu untersuchen, daß $\mathfrak{R}$ elementar abelsch vom Exponenten p ist.

Sei $\mathfrak{C}$ der Zentralisator von $\mathfrak{R}$ in $\mathfrak{G}$. Wegen $\mathfrak{R} \lhd \mathfrak{G}$ ist auch $\mathfrak{C} \trianglelefteq \mathfrak{G}$. Da $\mathfrak{P}$ abelsch ist, haben wir $\mathfrak{P} \leqq \mathfrak{C}$, also $p \nmid |\mathfrak{G}/\mathfrak{C}|$. Ist nun $\mathfrak{C} < \mathfrak{G}$, so gilt nach unserer Induktionsannahme der Satz für $\mathfrak{C}$, dann aber auch für $\mathfrak{G}$, da die oberhalb von $\mathfrak{C}$ noch auftretenden Kompositionsfaktoren von zu p teilerfremder Ordnung nicht stören. Wir können also $\mathfrak{G} = \mathfrak{C}$ annehmen. Dann folgt aber $\mathfrak{R} \leqq \mathfrak{P} \cap \mathbf{Z}(\mathfrak{G}) \cap \mathfrak{G}'$, also mit Hilfssatz 3.2 $\mathfrak{R} = \mathfrak{E}$, entgegen unserer Wahl von $\mathfrak{R}$.

Das Holomorph der abelschen Gruppe vom Typ (p, p) zeigt sofort, daß Satz 3.3 schon bei p-Sylowgruppen der Klasse 2 nicht mehr allgemein gilt.

3.4. Satz. *$\mathfrak{G}$ habe abelsche p-Sylowgruppe $\mathfrak{P}$. Es sei $\mathfrak{N}$ der kleinste Normalteiler von $\mathfrak{G}$ mit p-auflösbarer Faktorgruppe. Dann gilt:*

$$\mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_s \times \mathfrak{Q}; \quad \textit{dabei ist} \quad \mathfrak{N} \cap \mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_s$$

und jedes $\mathfrak{P}_i$ ist isomorph zur p-Sylowgruppe eines Kompositionsfaktors von $\mathfrak{G}$.

Beweis. a) Es sei $\mathfrak{P} \cap \mathfrak{N} = \mathfrak{S}$; wir zeigen zunächst, dass $\mathfrak{S}$ ein direkter Faktor von $\mathfrak{P}$ ist. Dies folgt sofort aus dem folgenden Satz von GASCHÜTZ ([2], S. 105, Satz 7): $\mathfrak{N}$ sei eine Gruppe mit abelscher p-Sylowgruppe und ohne nichttriviale p-Faktorgruppen. Dann zerfällt jede Erweiterung von $\mathfrak{N}$ mit einer p-Gruppe über $\mathfrak{N}$.

b) Sei $\mathfrak{E} = \mathfrak{N}_0 \lhd \mathfrak{N}_1 \lhd \cdots \lhd \mathfrak{N}_s = \mathfrak{N}$ eine Normalkette derart, daß $\mathfrak{N}_{i+1}/\mathfrak{N}_i$ genau einen Kompositionsfaktor von durch p teilbarer Ordnung enthält. Wir setzen $\mathfrak{P} \cap \mathfrak{N}_1 = \mathfrak{P}_1$. Angenommen, es sei schon $\mathfrak{P} \cap \mathfrak{N}_i = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_i$ gezeigt. Wir setzen $\mathfrak{P} \cap \mathfrak{N}_{i+1} = \mathfrak{L}_i$. Dann ist $\mathfrak{L}_i \mathfrak{N}_i/\mathfrak{N}_i$ p-auflösbar, aber $\mathfrak{N}_i$ hat keinen Kompositionsfaktor der Ordnung p. Nach a) folgt nun $\mathfrak{L}_i = (\mathfrak{N}_i \cap \mathfrak{P}) \times \mathfrak{P}_{i+1}$ für ein geeignetes $\mathfrak{P}_{i+1}$.

Wir vermerken zwei direkte Folgerungen aus Satz 3.4:

3.5. Satz. *$\mathfrak{G}$ habe abelsche p-Sylowgruppe $\mathfrak{P}$.* a) *Ist d die minimale Erzeugendenzahl von $\mathfrak{P}$, so hat $\mathfrak{G}$ höchstens d nichtauflösbare Kompositionsfaktoren von durch p teilbarer Ordnung; hat $\mathfrak{G}$ mindestens einen Kompositionsfaktor der Ordnung p, so hat es höchstens $d-1$ nichtauflösbare Kompositionsfaktoren von durch p teilbarer Ordnung.* b) *Es sei p^n die kleinste Invariante von $\mathfrak{P}$. Haben die p-Sylowgruppen jedes Kompositionsfaktors von $\mathfrak{G}$ einen Exponenten kleiner als p^n, so ist $\mathfrak{G}$ p-auflösbar.*

Offenbar liefern 3.5 a) und 3.5 b) für zyklisches $\mathfrak{P}$ wieder den Satz (B) von Wielandt.

Wir wollen den Normalteiler $\mathfrak{N}$ aus Satz 3.4 noch etwas genauer studieren:

3.6. Satz. *$\mathfrak{G}$ habe abelsche p-Sylowgruppe $\mathfrak{P}$ und keinen Kompositionsfaktor der Ordnung p. Zu jeder Kompositionsreihe $\mathfrak{E} = \mathfrak{N}_0 \lhd \mathfrak{N}_1 \lhd \cdots \lhd \mathfrak{N}_r = \mathfrak{G}$ von $\mathfrak{G}$ gibt es dann eine direkte Zerlegung $\mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_s$ mit den folgenden Eigenschaften:*

a) $\mathfrak{P}_1 \times \cdots \times \mathfrak{P}_i = \mathfrak{P} \cap \mathfrak{N}_{j(i)} \in s_{\mathfrak{G}}\mathfrak{P}$ $(i = 1, \ldots, s)$,

b) *jede Gruppe $\mathfrak{Q} \in s_{\mathfrak{G}}\mathfrak{P}$ ist Produkt einiger der $\mathfrak{P}_i$.*

Beweis. Offenbar können wir annehmen, dass $\mathfrak{G}$ p-reduziert ist.

1. Zu einer vorgegebenen Kompositionsreihe $\mathfrak{E} = \mathfrak{N}_0 \lhd \mathfrak{N}_1 \lhd \cdots \lhd \mathfrak{N}_r = \mathfrak{G}$ konstruieren wir zuerst eine Reihe $\mathfrak{E} = \mathfrak{K}_0 \lhd \mathfrak{K}_1 \lhd \cdots \lhd \mathfrak{K}_s = \mathfrak{G}$ mit $\mathfrak{K}_i \lhd \mathfrak{G}$ derart, daß (i) alle $\mathfrak{K}_i$ p-reduziert sind, (ii) die $\mathfrak{K}_i \cap \mathfrak{P}$ und die $\mathfrak{N}_i \cap \mathfrak{P}$ abgesehen von der Numerierung die gleichen Gruppen sind.

Die Konstruktion verläuft so:
Sei $\mathfrak{M}_i$ die normale Hülle von $\mathfrak{N}_i$ in $\mathfrak{G}$, $\mathfrak{L}_i$ der kleinste Normalteiler von $\mathfrak{M}_i$ mit p-freier Faktorgruppe. Die $\mathfrak{K}_i$ seien die verschiedenen unter den $\mathfrak{L}_i$. Dann ist (i) offenbar erfüllt, ferner sind die $\mathfrak{M}_i \cap \mathfrak{P}$ und die $\mathfrak{K}_i \cap \mathfrak{P}$ abgesehen von der Numerierung gleich. Zum Beweis von (ii) genügt es nun, $\mathfrak{M}_i \cap \mathfrak{P} = \mathfrak{N}_i \cap \mathfrak{P}$ zu zeigen.

Sei schon $\mathfrak{M}_i \cap \mathfrak{P} = \mathfrak{N}_i \cap \mathfrak{P}$. Ist p kein Teiler von $|\mathfrak{N}_{i+1}/\mathfrak{N}_i|$, so ist p auch kein Teiler von $|\mathfrak{M}_{i+1}/\mathfrak{M}_i|$ und daher $\mathfrak{M}_{i+1} \cap \mathfrak{P} = \mathfrak{M}_i \cap \mathfrak{P} = \mathfrak{N}_i \cap \mathfrak{P} = \mathfrak{N}_{i+1} \cap \mathfrak{P}$. Ist p ein Teiler von $|\mathfrak{N}_{i+1}/\mathfrak{N}_i|$, so gilt $\mathfrak{N}_{i+1} \cap \mathfrak{P} > \mathfrak{N}_i \cap \mathfrak{P} = \mathfrak{M}_i \cap \mathfrak{P}$, also ist $\mathfrak{N}_{i+1} \not\leqq \mathfrak{M}_i$. Nun ist $\mathfrak{N}_{i+1}\mathfrak{M}_i/\mathfrak{M}_i$ eine einfache nichtabelsche subnormale Untergruppe von $\mathfrak{G}/\mathfrak{M}_i$. Nach WIELANDT ([12], S. 464, Satz (5)) ist dann die normale Hülle $\mathfrak{M}_{i+1}/\mathfrak{M}_i$ direktes Produkt einiger Konjugierter von $\mathfrak{N}_{i+1}\mathfrak{M}_i/\mathfrak{M}_i$. Da aber $\mathfrak{G}/\mathfrak{M}_i$ keine nichttrivialen Faktorgruppen von zu p teilerfremder Ordnung besitzt, ist $\mathfrak{M}_{i+1}/\mathfrak{M}_i$ nach Hilfssatz 2.2 einfach, also ist $\mathfrak{M}_{i+1} = \mathfrak{N}_{i+1}\mathfrak{M}_i$. Daraus folgt $\mathfrak{M}_{i+1} \cap \mathfrak{P} = \mathfrak{N}_{i+1} \cap \mathfrak{P}$.

In allen folgenden Überlegungen betrachten wir statt der Kompositionsreihe $\mathfrak{N}_i$ die Normalreihe $\mathfrak{K}_i$.

2. Nun konstruieren wir die $\mathfrak{P}_i$: Wir setzen $\mathfrak{K}_1 \cap \mathfrak{P} = \mathfrak{P}_1$. Es sei $\mathfrak{N}_1$ der kleinste Normalteiler von $\mathbf{N}_{\mathfrak{G}}(\mathfrak{P}_1)$ mit p-auflösbarer Faktorgruppe; nach Satz 3.3 enthält $\mathfrak{N}_1$ keinen Kompositionsfaktor der Ordnung p. Andererseits gilt $\mathfrak{G} = \mathbf{N}_{\mathfrak{G}}(\mathfrak{P}_1)\mathfrak{K}_1$, daher $\mathbf{N}_{\mathfrak{G}}(\mathfrak{P}_1)/\mathbf{N}_{\mathfrak{N}_1}(\mathfrak{P}_1) \cong \mathfrak{G}/\mathfrak{K}_1$ und dies ist eine Gruppe ohne Kompositionsfaktoren der Ordnung p und ohne nichttriviale Faktorgruppen von zu p teilerfremder Ordnung. Dies zusammen liefert $\mathbf{N}_{\mathfrak{G}}(\mathfrak{P}_1) = \mathbf{N}_{\mathfrak{N}_1}(\mathfrak{P}_1)\mathfrak{N}_1$. Jetzt folgt $\mathfrak{G} = \mathfrak{K}_1\mathbf{N}_{\mathfrak{G}}(\mathfrak{P}_1) = \mathfrak{K}_1\mathfrak{N}_1$, und $\mathfrak{K}_1 \cap \mathfrak{N}_1 = \mathbf{N}_{\mathfrak{G}}(\mathfrak{P}_1) \cap \mathfrak{K}_1 \cap \mathfrak{N}_1 = \mathbf{N}_{\mathfrak{N}_1}(\mathfrak{P}_1) \cap \mathfrak{N}_1$ hat zu p teilerfremde Ordnung, da $\mathbf{N}_{\mathfrak{N}_1}(\mathfrak{P}_1)$ und $\mathfrak{N}_1$ Normalteiler von $\mathbf{N}_{\mathfrak{G}}(\mathfrak{P}_1)$ sind, $\mathbf{N}_{\mathfrak{N}_1}(\mathfrak{P}_1)$ p-auflösbar ist und $\mathfrak{N}_1$ keinen Kompositionsfaktor der Ordnung

p besitzt. Mit $\mathfrak{R}_1 \cap \mathfrak{P} = \mathfrak{Q}_1$ erhalten wir also $\mathfrak{P} = \mathfrak{P}_1 \times \mathfrak{Q}_1$. Wenn wir nun annehmen, daß für $\mathfrak{R}_1$ mit der p-Sylowgruppe $\mathfrak{Q}_1$ und der Normalkette $\mathfrak{E} \lhd \mathfrak{K}_2 \cap \mathfrak{R}_1 \lhd \cdots \lhd \mathfrak{R}_1$ die entsprechende Zerlegung $\mathfrak{Q}_1 = \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_s$ mit $\mathfrak{K}_i \cap \mathfrak{R}_1 \cap \mathfrak{Q}_1 = \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_i$ und der Eigenschaft b) schon durchgeführt ist, so erhalten wir die gewünschte Zerlegung von $\mathfrak{P}$.

3. Sei $\mathfrak{M}$ ein von $\mathfrak{K}_1$ verschiedener minimaler Normalteiler von $\mathfrak{G}$. Da $\mathfrak{G}$ p-reduziert ist, hat $\mathfrak{M}$ durch p teilbare Ordnung, ist also nach Hilfssatz 2.2 einfach. Dies ergibt $\mathfrak{M} \cap \mathfrak{K}_1 = \mathfrak{E}$, somit $\mathfrak{M} \leqq \mathbf{C}(\mathfrak{K}_1) \leqq \mathbf{N}_{\mathfrak{G}}(\mathfrak{P}_1)$. Da $\mathfrak{M}$ nicht p-auflösbar ist, erhalten wir $\mathfrak{M} \leqq \mathfrak{R}_1$. Angenommen, es sei $\mathfrak{M} \not\leqq \mathfrak{K}_j$, aber $\mathfrak{M} \leqq \mathfrak{K}_{j+1}$. Da $\mathfrak{K}_{j+1}$ p-reduziert ist, ergibt sich $\mathfrak{K}_{j+1} = \mathfrak{M} \times \mathfrak{K}_j$. Nehmen wir an, daß der Satz für $\mathfrak{R}_1$ schon gilt, so ist $\mathfrak{P} \cap \mathfrak{M} = \mathfrak{Q}_1 \cap \mathfrak{M}$ ein $\mathfrak{P}_i$; wegen $\mathfrak{K}_j \cap \mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_j \not\geqq \mathfrak{P}_i$ und $\mathfrak{K}_{j+1} \cap \mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_{j+1} \geqq \mathfrak{P}_i$ folgt notwendig $i = j+1$.

Nun vergleichen wir die beiden Normalreihen

$$\mathfrak{E} = \mathfrak{K}_0 \lhd \mathfrak{K}_1 \lhd \cdots \lhd \mathfrak{K}_s = \mathfrak{G} \quad \text{und} \quad \mathfrak{E} = \mathfrak{K}_0^* \lhd \mathfrak{K}_1^* \lhd \cdots \lhd \mathfrak{K}_s^* = \mathfrak{G}$$

mit $\mathfrak{K}_i^* = \mathfrak{M} \times \mathfrak{K}_{i-1}$ für $1 \leqq i \leqq j$ und $\mathfrak{K}_i^* = \mathfrak{K}_i$ für $i \geqq j+1$.

Es ist $\mathfrak{K}_i^* \cap \mathfrak{P} = \mathfrak{P}_{j+1} \times \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_{i-1}$ für $1 \leqq i \leqq j$ und $\mathfrak{K}_i^* \cap \mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_i$ für $i \geqq j+1$. Also erhalten wir bis auf die Anordnung der Faktoren aus beiden Normalreihen wieder die gleiche Zerlegung $\mathfrak{P} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_s$.

4. Nun beweisen wir die Aussage b) durch Induktion nach s. Seien

(I) $$\mathfrak{E} = \mathfrak{K}_0 \lhd \mathfrak{K}_1 \lhd \cdots \lhd \mathfrak{K}_s = \mathfrak{G} \quad \text{und}$$

(II) $$\mathfrak{E} = \mathfrak{M}_0 \lhd \mathfrak{M}_1 \lhd \cdots \lhd \mathfrak{M}_s = \mathfrak{G}$$

Normalreihen, welche gemäß 1. zu vorgegebenen Kompositionsreihen konstruiert sind. $\mathfrak{K}_1$ und $\mathfrak{M}_1$ sind minimale Normalteiler von $\mathfrak{G}$. Ist $\mathfrak{K}_1 \neq \mathfrak{M}_1$, so ersetzen wir die Reihe (I) gemäß 3. durch eine Reihe, welche mit $\mathfrak{M}_1$ beginnt, und dabei werden die $\mathfrak{P}_i$ nicht geändert. Also können wir $\mathfrak{K}_1 = \mathfrak{M}_1$ annehmen. Dann vergleichen wir in $\mathfrak{R}_1$ die Ketten $\mathfrak{E} \lhd \mathfrak{R}_1 \cap \mathfrak{K}_2 \lhd \cdots \lhd \mathfrak{R}_1$ und $\mathfrak{E} \lhd \mathfrak{R}_1 \cap \mathfrak{M}_2 \lhd \cdots \lhd \mathfrak{R}_1 \cap \mathfrak{M}_s = \mathfrak{R}_1$. Die erste liefert die Zerlegung $\mathfrak{Q}_1 = \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_s$, die zweite liefert gemäß unserer Induktionsannahme die gleichen $\mathfrak{P}_i$. Damit ist der Satz bewiesen.

Satz 3.6 gibt einen ziemlich genauen Einblick in die Struktur von $s_{\mathfrak{G}}\mathfrak{P}$:

3.7. Satz. *$\mathfrak{G}$ habe abelsche p-Sylowgruppe $\mathfrak{P}$ und keinen Kompositionsfaktor der Ordnung p. Dann gilt:*

a) *$s_{\mathfrak{G}}\mathfrak{P}$ ist isomorph zu einem Teilverband eines Mengenverbandes $\{1, \ldots, s\}$, ist also distributiv.*

b) *Trifft für die Kompositionsfaktoren von $\mathfrak{G}$ von durch p teilbarer Ordnung die Schreiersche Vermutung zu, so ist $s_{\mathfrak{G}}\mathfrak{P}$ der volle Mengenverband $\{1, \ldots, s\}$, ist also komplementär.*

Beweis. a) folgt direkt aus Satz 3.6.

b) Wir können annehmen, daß $\mathfrak{G}$ p-reduziert ist. Sei $\mathfrak{N}$ ein minimaler Normalteiler von $\mathfrak{G}$. Dann ist p ein Teiler von $|\mathfrak{N}|$, also nach unserer Voraussetzung $\mathfrak{N}$ nichtabelsch. Nach 2.2 ist $\mathfrak{N}$ einfach. Die Richtigkeit der Schreierschen Vermutung liefert die Auflösbarkeit von $\mathfrak{G}/\mathbf{C}(\mathfrak{N})\mathfrak{N}$, also unter unserer Voraussetzung $\mathfrak{G} = \mathbf{C}(\mathfrak{N})\mathfrak{N}$. Aber andererseits ist $\mathbf{C}(\mathfrak{N}) \cap \mathfrak{N} = \mathfrak{E}$, also $\mathfrak{G} = \mathbf{C}(\mathfrak{N}) \times \mathfrak{N}$. Die Fortsetzung dieses Verfahrens liefert eine Darstellung von $\mathfrak{G}$ als direktes Produkt von einfachen nichtabelschen Gruppen mit durch p teilbarer Ordnung. Daraus folgt offensichtlich die Behauptung b).

3.8. Beispiel. Wir wollen noch durch Angabe eines Beispiels zeigen, daß sich Satz 3.5 b) nicht auf alle regulären p-Sylowgruppen $\mathfrak{P}$ ausdehnen läßt, obwohl in einer regulären p-Gruppe Invarianten definiert sind, daher Satz 3.5 b) für reguläres $\mathfrak{P}$ in der vorliegenden Formulierung durchaus Sinn hat. Wir gehen ganz ähnlich vor wie bei 1.9 b) und betrachten die Gruppe $\mathfrak{G}$ aller Matrizen vom Grade 2, deren Matrixelemente dem Restklassenring $\bmod p^3$ entnommen sind und deren Determinante zu p teilerfremd ist. Die Abbildung dieser Matrizen auf ihre Reste $\bmod p$ ist wieder ein Homomorphismus von $\mathfrak{G}$ auf die lineare Gruppe $GL(2, p)$. Der Kern $\mathfrak{K}$ besteht diesmal aus den Matrizen $E + pA$, wobei $A \bmod p^2$ zu lesen ist. Also ist $|\mathfrak{K}| = p^8$, daher $|\mathfrak{P}| = p^9$ und $\mathfrak{P}$ ist für $p \geqq 11$ sicher regulär. $\mathfrak{K}$ hat offenbar den Exponenten p^2, und da $\mathfrak{P}$ Elemente der genauen Ordnung p^3 besitzt, z. B. $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, ist $\mathfrak{K}$ gleich dem Erzeugnis aller p^3-ten Potenzen von Elementen aus $\mathfrak{P}$. Eine kurze Rechnung zeigt, daß die Elemente der Ordnung p in $\mathfrak{K}$ die Gestalt $E + p^2A$ besitzen, daher stets p-te Potenzen von Elementen aus $\mathfrak{K}$ sind. Somit hat $\mathfrak{K}$ lauter Invarianten p^2 und $\mathfrak{P}$ hat die Invarianten p^3, p^2, p^2, p^2, also keine Invariante p. Alle Kompositionsfaktoren von $\mathfrak{G}$ enthalten p nur in der ersten Potenz, aber $\mathfrak{G}$ hat dennicht p-auflösbaren Kompositionsfaktor $GL(2, p)$.

Durch Übergang zu der Faktorgruppe von $\mathfrak{G}$ nach dem zentralen Normalteiler, welcher von $(1 + p)E$ erzeugt wird, läßt sich dieses Beispiel noch so abändern, daß $\mathfrak{P}$ genau 3 Invarianten hat. Besitzt dagegen $\mathfrak{P}$ nur 2 Invarianten, so gilt Satz 3.5 b) und auch alle übrigen Ergebnisse von § 3. Darauf soll in einer späteren Arbeit eingegangen werden.

Literatur

[1] W. Burnside, *Theory of groups of finite order*, second edition (Cambridge, 1911).
[2] W. Gaschütz, Zur Erweiterungstheorie der endlichen Gruppen, *Journal für Math.*, **190** (1952), 93–107.
[3] W. Gaschütz, Über die Φ-Untergruppe endlicher Gruppen, *Math. Zeitschrift*, **58** (1953), 160—170.
[4] P. Hall, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.*, (2) **36** (1933), 29—95.
[5] P. Hall—G. Higman, On the p-length of p-soluble groups and reduction theorems for Burnside's problem, *Proc. London Math. Soc.*, (3) **6** (1956), 1—42.
[6] N. Itô, Über eine zur Frattini-Gruppe duale Bildung, *Nagoya Journ. of Math.*, **9** (1955), 123—127.
[7] K. Iwasawa, Über die Struktur der endlichen Gruppen, deren echte Untergruppen sämtlich nilpotent sind, *Proc. Phys.-Math. Soc. Japan*, (III) **23** (1941), 1—4.
[8] D. Taunt, On A-groups, *Proc. Cambridge Phil. Soc.*, **45** (1949), 24—42.
[9] J. Thompson, Normal p-complements for finite groups, *Math. Zeitschrift*, **72** (1960), 332—354.
[10] H. Wielandt, Eine Verallgemeinerung der invarianten Untergruppen, *Math. Zeitschrift*, **45** (1939), 209—244.
[11] H. Wielandt, Sylowgruppen und Kompositionsstruktur, *Abh. Math. Seminar Hamburg*, **22** (1958), 215—228.
[12] H. Wielandt, Über den Normalisator der subnormalen Untergruppen, *Math. Zeitschrift*, **69** (1958), 463—465.
[13] H. Zassenhaus, *Lehrbuch der Gruppentheorie*. I (Leipzig—Berlin, 1937).

(Eingegangen am 28. März 1960,
in durchgearbeiteter Form am 3. Oktober 1960)

Über die Struktur kommutativer Hauptidealringe

Von G. POLLÁK in Szeged

Herrn Professor László Rédei zum 60. Geburtstag gewidmet

In der vorliegenden Arbeit wird der Begriff „Hauptidealring" im weitesten Sinne benutzt, d. h. es wird weder Nullteilerfreiheit, noch Existenz eines Einselements erfordert. Wir wollen zuerst die Struktur der kommutativen Hauptidealringe mit Einselement (kurz: k. H. E.) untersuchen und dann das bekommene Resultat zur Betrachtung kommutativer Hauptidealringe im allgemeinen zu Hilfe nehmen.

1. Wir nennen π ein *schwaches Primelement*, falls aus $\pi = \alpha\beta$, $\alpha \notin (\pi)$ folgt: $\beta \in (\pi)$. Wir zeigen vor allem:

Hilfssatz 1. *Es sei R ein k. H. E., $\pi \in R$ ein schwaches Primelement und $\mathfrak{v}_{\pi^m}$ der Annihilator*[1]) *von π^m. Ist $\pi^m \neq 0$, $\mathfrak{v}_{\pi^m} \subseteq (\pi)$, so ist (π^m) ein direkter Summand in R.*

Es genügt zu zeigen, daß (π^m) durch einen von 0 verschiedenen Idempotenten erzeugt ist. Zu diesem Zwecke sei $\mathfrak{v}_{\pi^m} = (\alpha)$, $\alpha \notin (\pi)$ und

$$(\alpha, \pi) = (\beta), \quad \beta = \alpha\xi + \pi\eta \quad (\notin (\pi)).$$

Hieraus erhalten wir $\pi = \beta\gamma$. Wegen $\beta \notin (\pi)$ muß $\gamma \in (\pi)$, $\gamma = \pi\gamma'$ sein und

$$\pi^m = \pi^{m-1}\beta\gamma = \pi^m\beta\gamma' = (\alpha\xi + \pi\eta)\pi^m\gamma' = \pi^{m+1}\eta\gamma'.$$

Dann ist aber $\varepsilon = (\pi\eta\gamma')^m$ ein Idempotent und wegen $\pi^m = \pi^m\varepsilon$ ist $(\pi^m) = (\varepsilon)$, $\varepsilon \neq 0$ falls $\pi^m \neq 0$, was zu beweisen war.

Das Hauptresultat in der angedeuteten Richtung ist im folgenden Satz enthalten:

Satz 1. *Jeder k. H. E. R läßt sich in die direkte Summe von endlich vielen solchen unzerlegbaren k. H. E. zerlegen, in denen die eindeutige Primzerlegung gilt.*

---

[1]) Wir wollen statt Annullatorenideal diesen kürzeren Ausdruck benutzen.

Beweis. Wir nehmen an, daß in R die eindeutige Primzerlegung nicht gilt und zeigen, daß R dann in eine direkte Summe von zwei Komponenten zerfällt.

In der Tat, wenn es in R ein schwaches Primelement $\pi \neq 0$ gibt, das nicht prim ist, so sei α ein Nullteiler mod π. Wir können voraussetzen, daß $(\alpha) \supset (\pi)$, denn wir dürfen α durch das Erzeugende α' des Ideals (α, π) ersetzen. In der Tat, wenn $\alpha\beta \in (\pi)$ ist, so gilt auch $\alpha'\beta \in (\alpha\beta, \pi\beta) \subseteq (\pi)$. Dann ist $\pi = \alpha\gamma$, wobei wegen der schwachen Primeigenschaft von π die Gleichung $\gamma = \delta\pi$ mit passendem δ bestehen muß. Hieraus erhalten wir $(1-\alpha\delta)\pi = 0$. Da α offenbar keine Einheit sein kann, ist $1-\alpha\delta \notin (\alpha)$, also wegen $(\alpha) \supset (\pi)$ um so mehr $1-\alpha\delta \notin (\pi)$. Nach Hilfssatz 1 zerfällt dann R in eine direkte Summe, d. h. ist unsere Behauptung in diesem Falle richtig.

Es sei jetzt in R jedes schwache Primelement prim. Ist dann $\alpha \in R$ nicht prim, so gilt mit passenden β, γ

$$\alpha = \beta\gamma, \quad (\beta) \supset (\alpha), \quad (\gamma) \supset (\alpha).$$

Ist einer der Faktoren noch immer nicht prim, so kann man ihn wieder ähnlicherweise zerlegen usw. Da ein Hauptidealring immer die Maximumbedingung (für Ideale) erfüllt, führt dieser Zerlegungsprozeß in endlich vielen Schritten zu einer Primzerlegung. Damit gibt es für jedes Element von R wenigstens eine Primzerlegung, und nach unserer Annahme gibt es für irgendwelches $\alpha \neq 0$ zwei wesentlich (d. h. nicht nur in Ordnung und Einheitsfaktoren) verschiedene Zerlegungen:

$$\alpha = \pi_1^{i_1} \dots \pi_n^{i_n} = \varepsilon \pi_1^{j_1} \dots \pi_n^{j_n}, \tag{1}$$

wobei ε eine Einheit ist; aus $\varepsilon' \pi_s = \pi_t$ mit irgendwelcher Einheit ε' folgt $s = t$; $i_s, j_s \geqq 0$, $i_s + j_s > 0$ für alle $1 \leqq s \leqq n$; für irgendwelches s gilt $i_s \neq j_s$. Wir unterscheiden zwei Fälle.

a) Nicht alle i und j sind von 0 verschieden. Sei z. B. $j_1 = 0$. Da π_1 ein Primelement ist, muß einer der Faktoren auf der rechten Seite von (1) (z. B. π_2) in (π_1) enthalten sein, d. h.

$$\pi_2 = \pi_1 \varrho. \tag{2}$$

Wir haben erhalten, daß das Primelement π_2 reduzibel ist, d. h. es läßt sich in zwei Faktoren zerlegen, aus denen keiner eine Einheit ist (von der Primeigenschaft von π_1 werden wir im Folgenden schon keinen Nutzen machen). Aus (2) folgt, daß entweder $\pi_1 \in (\pi_2)$ oder $\varrho \in (\pi_2)$. Sei z. B. $\varrho = \sigma\pi_2$. Daraus und aus (2) ergibt sich

$$(1-\pi_1\sigma)\pi_2 = 0.$$

Da wegen (2) $(\pi_2) \subset (\pi_1) \neq (1)$, ist $1-\pi_1\sigma \notin (\pi_2)$, der Annihilator von π_2

ist also nicht in (π_2) enthalten. Damit ist (π_2) nach Hilfssatz 1 ein direkter Summand in R.

b) Alle i und j sind in (1) von 0 verschieden. Es gibt ein s, für welches $i_s \neq j_s$ ist; bestimmtheitshalber sei $0 < i_1 < j_1$. Wir setzen $\pi_2^{i_2} \dots \pi_n^{i_n} = \beta$, $\varepsilon \pi_1^{j_1 - i_1} \pi_2^{i_2} \dots \pi_n^{i_n} = \gamma$. Dann haben wir

$$(\beta - \gamma)\pi_1^{i_1} = 0.$$

Wäre hier $\beta - \gamma \in (\pi_1)$, so wäre auch $\beta \in (\pi_1)$ und wir hätten

$$\beta = \pi_2^{i_2} \dots \pi_n^{i_n} = \pi_1 \beta',$$

d. h. wieder Fall a). Ist dagegen $\beta - \gamma \notin (\pi_1)$, so ist der Annihilator von $\pi_1^{i_1}$ nicht in (π_1) enthalten, also ist in diesem Falle wieder $(\pi_1^{i_1})$ ein direkter Summand in R.

Es gilt also $R = R_{11} \dotplus R_{12}$. Als direkte Summanden eines Ringes mit Einselement, sind R_{11} und R_{12} auch solche Ringe. Ferner sind R_{11} und R_{12} Hauptidealringe, denn wenn $\mathfrak{a}$ ein Ideal z. B. in R_{11} ist, so ist es auch in R ein Ideal, und wenn $\mathfrak{a} = (\alpha)$ in R, so besteht dasselbe auch in R_{11}. Endlich, wenn wir diesen Zerlegungsprozeß fortsetzen, muß dieser nach endlich vielen Schritten abbrechen. Um das zu zeigen, betrachten wir einen Ring R der unbegrenzt zerlegbar ist, d. h. für welchen die unendlich vielen Zerlegungen

$$\begin{aligned} &R = R_{11} \dotplus R_{12}, \\ &R = R_{21} \dotplus R_{22} \dotplus R_{23}, \\ &\dots\dots\dots\dots\dots\dots \\ &R = R_{n1} \dotplus \dots \dotplus R_{n,n+1}, \\ &\dots\dots\dots\dots\dots\dots \end{aligned} \qquad (R_{ij} \neq 0 \text{ für } i = 1, 2, \dots; \; j = 1, \dots, i+1) \tag{3}$$

gelten, wo die n-te Zerlegung aus der $(n-1)$-ten so entsteht, daß eine der Komponenten in zwei nichttriviale Summanden zerlegt wird. Es ist klar, daß in jeder Zerlegung wenigstens eine Komponente auch selbst unbegrenzt zerlegbar ist; darum können wir ohne Beschränkung der Allgemeinheit annehmen, daß in jeder Zerlegung in (3) immer die letzte Komponente zerlegbar ist und

$$R_{n-1,1} = R_{n1}, \dots, R_{n-1,n-1} = R_{nn-1}; \quad R_{n-1,n} = R_{nn} \dotplus R_{nn+1}$$

gilt. Dann ist aber

$$R_{11} \subset R_{11} \dotplus R_{22} \subset \dots \subset R_{11} \dotplus R_{nn} \subset \dots$$

eine unendliche aufsteigende Idealkette. Das ist aber wegen der Maximumbedingung unmöglich. Damit ist Satz 1 bewiesen.

Es ist leicht zu sehen, daß die direkte Summe R von endlich vielen Hauptidealringen mit Einselement $R_1, \dots, R_k$ wieder ein Hauptidealring mit

Einselement ist. In der Tat, ein Ideal $\mathfrak{a}$ in R ist eine direkte Summe von gewissen Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ in $R_1, \ldots, R_k$. Ist dabei $\mathfrak{a}_i = (a_i)$ in R_i für jedes $1 \leqq i \leqq k$, so haben wir

$$\mathfrak{a} = \mathfrak{a}_1 \dotplus \cdots \dotplus \mathfrak{a}_k = (a_1) \dotplus \cdots \dotplus (a_k) = (a_1 + \cdots + a_k).$$

Durch diese Bemerkung und Satz 1 ist die Frage über sämtliche k. H. E. auf die Frage über direkt unzerlegbare k. H. E. (kurz: u. H. E.) zurückgeführt. Aus Satz 1 folgt unmittelbar, daß in einem u. H. E. die eindeutige Primzerlegung immer gilt. Um alle solche Ringe angeben zu können, brauchen wir zwei Hilfssätze.

Hilfssatz 2. *Sei R ein k. H. E., (π) ein Primideal darin und $(\varrho) \supset (\pi)$. Dann ist*

$$(\varrho\,\pi) = (\pi). \tag{4}$$

In der Tat, wegen $(\varrho) \supset (\pi)$ haben wir

$$\pi = \varrho\,\pi'.$$

Aus der Primeigenschaft von π folgt aber $\pi' \in (\pi)$, also $\pi \in (\varrho\,\pi)$ und damit auch (4).

Hilfssatz 3. *Gilt in einem k. H. E. R für das Primideal (π)*

$$(\pi) \supset (\pi^2) \supset \cdots, \tag{5}$$

so ist das Ideal

$$(\sigma) = \bigcap_{i=1}^{\infty} (\pi^i) \tag{6}$$

prim in R.

Wäre nämlich $\alpha\beta \in (\sigma)$ und

$$\alpha = \alpha'\pi^k, \quad \beta = \beta'\pi^l \qquad (\alpha', \beta' \notin (\pi);\ k, l \geqq 0),$$

wobei $k = 0$ oder $l = 0$ bedeutet, daß $\alpha \notin (\pi)$ bzw. $\beta \notin (\pi)$, so hätten wir $\alpha'\beta' \notin (\pi)$, aber wegen (6) ist

$$\alpha'\beta'\pi^{k+l} \in (\pi^{k+l+1}). \tag{7}$$

Sei $(\alpha'\beta', \pi) = (\varrho)$; dann ist $(\pi) \subset (\varrho)$, also nach Hilfssatz 2 besteht auch (4). Aus (7) folgt aber

$$(\varrho\,\pi^{k+l}) \subseteq (\pi^{k+l+1}).$$

Mit (4) zusammen ergibt dies

$$(\pi^{k+l}) = (\pi^{k+l+1}),$$

was aber mit (5) in Widerspruch steht.

Nun können wir beweisen den

Satz 2. *Ein u. H. E. ist entweder nullteilerfrei oder hat ein einziges, und zwar nilpotentes Primideal.*

Beweis. Sei R ein u. H. E. Wir bemerken vor allem, daß in R jedes von (0) verschiedene Primideal maximal ist. In der Tat, nach Satz 1 gilt in R die eindeutige Primzerlegung. Wäre nun das Primideal $(\pi) \neq (0)$ nicht maximal, so wäre es in einem maximalen, also primen Ideal (ϱ) enthalten. Nach Hilfssatz 2 gilt dann aber (4), also $\pi = \pi\varrho\xi$, in Widerspruch mit der Eindeutigkeit der Primzerlegung.

Es sei jetzt (π) ein Primideal in R. Gilt für ihn (5), so ist nach Hilfssatz 3 das durch (6) definierte Ideal (σ) prim, also wegen $(\pi) \supset (\sigma)$ muß $\sigma = 0$ sein. Wir haben erhalten, daß wenn in R für irgendwelches Primideal (5) gilt, so ist in R das Ideal (0) prim, d. h. R ist nullteilerfrei (und damit gilt natürlich (5) für alle Primideale).

Gilt (5) für ein Primideal (π) nicht (also gilt es für kein Primideal), so ist $(\pi^m) = (\pi^{m+1})$ für passendes m, d. h. $\pi^m = \pi^{m+1}\xi$. Wegen der Eindeutigkeit der Primzerlegung in R folgt daher $\pi^m = 0$, d. h. alle Primideale von R sind nilpotent. Wäre nun (τ) ein von (π) verschiedenes Primideal, so wäre auch (τ, π) nilpotent; aus der Maximalität von (τ) und (π) folgt aber $(\tau, \pi) = (1)$: Wiederspruch. In diesem Falle hat also R ein einziges Primideal (π). Damit ist Satz 2 bewiesen.

Jetzt steht die Struktur der k. H. E. schon ganz klar vor uns. Ein solcher Ring ist eine direkte Summe von endlich vielen „Hauptidealintegritätsbereichen" (Typ I) und Ringen mit einem einzigen (maximalen) nilpotenten Primideal (Typ II). Ringe beider Typen I und II sind direkt unzerlegbar, jedes Primideal in ihnen ist maximal und damit gilt in ihnen die Eindeutigkeit der Primzerlegung. Umgekehrt, eine direkte Summe von endlich vielen Ringen vom Typ I und II ist immer ein k. H. E.

Es ist leicht zu sehen, daß die Eindeutigkeit der Primzerlegung nur im unzerlegbaren Falle gilt. Ein direkt zerlegbarer k. H. E. enthält nämlich einen von 0 und Einheiten verschiedenen Idempotenten, dessen Primzerlegung nicht eindeutig ist. Wenn wir aber — statt die Eindeutigkeit im strengen Sinne (d. h. im Sinne, daß in (1) $i_m = j_m$ für jedes m) zu erfordern — nur $\pi_m^{i_m} = \varepsilon_m \pi_m^{j_m}$ mit einer Einheit ε_m voraussetzen, so erhalten wir, daß *die Ringe, in denen die Primzerlegung in diesem schwächeren Sinne eindeutig ist, entweder zu dem Typ I gehören oder eine direkte Summe von endlich vielen Körpern und Ringen vom Typ II sind und umgekehrt, alle solche Ringe erfüllen diese Forderung.* Um die erste Behauptung einzusehen, müssen wir zeigen, daß in einem k. H. E., in welcher die Primzerlegung im schwächeren Sinne ein-

deutig ist, jeder nichttriviale direkte Summand ersten Types ein Körper ist. Wäre nun $R = R_1 \dotplus R_2$, wobei R_1 nullteilerfrei, aber kein Körper ist, so wäre R_2 ein Primideal in R, aber nicht maximal. Nach Hilfssatz 2 gilt dann für $R_2 = (\pi)$ (4) und damit ist π mehrdeutig zerlegbar, also muß $\pi = 0$ und damit $R_2 = 0$ gelten. Umgekehrt, wenn

$$R = K_1 \dotplus \cdots \dotplus K_l \dotplus N_1 \dotplus \cdots \dotplus N_m$$

ist, wo die K_i Körper, die N_j Ringe vom Typ II sind, so sind

$$\mathfrak{p}_i = K_1 \dotplus \cdots \dotplus K_{i-1} \dotplus K_{i+1} \dotplus \cdots \dotplus K_l \dotplus N_1 \dotplus \cdots \dotplus N_m \qquad (i = 1, \ldots, l),$$

$$\mathfrak{p}_{l+j} = K_1 \dotplus \cdots \dotplus K_l \dotplus N_1 \dotplus \cdots \dotplus N_{j-1} \dotplus \mathfrak{q}_j \dotplus N_{j+1} \dotplus \cdots \dotplus N_m \qquad (j = 1, \ldots, m)$$

die sämtlichen Primideale von R; hier bedeutet $\mathfrak{q}_j$ das Primideal von N_j. Sie sind alle maximal (die Faktorringe sind Körper)[2]). Daraus folgt unmittelbar, daß Elemente, die dasselbe Primideal erzeugen, assoziiert sein müssen. Folglich erzeugen in (1) $\pi_1, \ldots, \pi_n$ voneinander verschiedene Primideale. Sind nun z. B. $\pi_s^{i_s}$ und $\pi_s^{j_s}$ nicht assoziiert und ist $(\pi_s) = \mathfrak{p}_k$, so kann (1) nicht bestehen, denn die Komponenten aus K_k (falls $k \leqq l$) bzw. N_{k-l} (falls $k > l$) auf beiden Seiten verschieden sind.

Im allgemeinen Falle gibt es eine in gewissem Sinne minimale Zerlegung, die schon eindeutig bestimmt ist. Sei nämlich $R = R_1 \dotplus \cdots \dotplus R_m$, wo alle R_i u. H. E. sind. Sämtliche Primideale von R entstehen jetzt in der Form

$$\mathfrak{p} = R_1 \dotplus \cdots \dotplus R_{i-1} \dotplus \bar{\mathfrak{p}} \dotplus R_{i+1} \dotplus \cdots \dotplus R_m \qquad (1 \leqq i \leqq m),$$

wo $\bar{\mathfrak{p}}$ ein Primideal in R_i (möglicherweise auch (0)) ist. Es ist klar, daß $\mathfrak{p}$ durch das Element $\pi = \varepsilon_1 + \cdots + \varepsilon_{i-1} + \bar{\pi} + \varepsilon_{i+1} + \cdots + \varepsilon_m$ erzeugt ist, wobei ε_j der in R_j enthaltene Idempotent, $\bar{\pi}$ ein fixiertes Erzeugende von $\bar{\mathfrak{p}}$ ist. *Für jedes Element $a \neq 0$ von R gibt es eine einzige Darstellung in der Form eines Produktes von solchen π*

$$a = \varepsilon \pi_1^{i_1} \ldots \pi_n^{i_n} \qquad (\varepsilon \text{ Einheit}, \ i_s > 0)$$

mit der Eigenschaft, daß aus $a = \varepsilon' \pi_1^{j_1} \ldots \pi_n^{j_n}$, wo ε' eine Einheit und $j_s \geqq 0$ ist, $i_s \leqq j_s$ für $s = 1, \ldots, n$ folgt. Den Beweis überlassen wir dem Leser.

2. Es sei jetzt R ein beliebiger kommutativer Hauptidealring. Nach J. SZENDREI nennen wir das Element $r \in R$ einen *Multiplikator*, falls es eine natürliche Zahl n mit

$$r\xi = n\xi \quad \text{für alle} \quad \xi \in R \tag{8}$$

gibt. Es bezeichne ferner N den Zeroring mit einem unendlich zyklischen

[2]) Wir sehen also, daß die schwächere Eindeutigkeit gleichbedeutend mit der Maximalität sämtlicher Primideale ist.

Modul. Es ist klar, daß N ein kommutativer Hauptidealring ist. Außerdem gilt

Satz 3. *Enthält der kommutative Hauptidealring R keinen Multiplikator, so ist*

$$R \cong R_1 \dotplus N, \tag{9}$$

wobei R_1 entweder 0 oder ein k. H. E. ist.

Beweis. Es sei $R=(\alpha)$. Ein Element ν ist dann und nur dann ein Multiplikator, falls $\nu\alpha = n\alpha$ mit einer natürlichen Zahl n besteht. Daraus folgt, daß $\varrho\alpha + r\alpha = \sigma\alpha + s\alpha$ nur im Fall $r=s$ gelten kann.

Betrachten wir das Ideal $\mathfrak{a}=(p\alpha, \alpha^2)$ mit einer beliebigen Primzahl p. Jedes Element von $\mathfrak{a}$ entsteht in der Form $\xi\alpha + xp\alpha$ ($\xi \in R$) und da $\mathfrak{a}$ ein Hauptideal ist, ist es durch ein solches Element, z. B. durch $\varkappa = \varrho\alpha + rp\alpha$ erzeugt. Es gilt also

$$p\alpha = \sigma\varkappa + s\varkappa = (\sigma\varrho + s\varrho + rp\sigma)\alpha + srp\alpha, \tag{10}$$

$$\alpha^2 = \tau\varkappa + t\varkappa = (\tau\varrho + t\varrho + rp\tau)\alpha + trp\alpha, \tag{11}$$

also aus (10) $srp = p$, $s = r = \pm 1$ und aus (11) $trp = 0$, $t = 0$. Wir können jetzt (11) in der Form $\alpha^2 = \tau\varrho\alpha + p\tau\alpha$ schreiben. Setzen wir $\tau = \zeta\alpha + z\alpha$, so erhalten wir hieraus $\xi\alpha^2 + (zp-1)\alpha^2 = 0$ mit irgendwelchem $\xi \in R$, d. h. $\xi\alpha + (zp-1)\alpha$ ist ein Annullator von α und damit auch des ganzen Ringes R. Sei nun $\mathfrak{o}=(\omega)$ der Annihilator von R und sei $\omega \equiv o\alpha \bmod \alpha^2$. Wegen $\xi\alpha + (zp-1)\alpha \in (\omega)$ ist $\omega \neq 0$. Da ferner $m\omega$ ($m = 0, \pm 1, \ldots$) die sämtlichen Elemente von (ω) sind, ist sogar $o \neq 0$, denn aus $m\omega = \xi\alpha + (zp-1)\alpha$ auch $mo = zp - 1 \equiv -1 \bmod p$ folgt. Aus dem letzten schließen wir sogar $p \nmid o$. Da hier p eine beliebige Primzahl ist, muß $o = \pm 1$ sein, also wegen $m\omega \equiv mo\alpha \bmod \alpha^2$ ist einerseits $(\omega) \cap (\alpha^2) = 0$, andererseits $(\omega, \alpha^2) = R$, d. h.

$$R = (\alpha^2) \dotplus (\omega).$$

Hier ist $(\omega) \cong N$. Als direkter Summand von einem Hauptidealring, ist (α^2) selber ein solcher. Es bleibt also übrig zu zeigen, daß entweder $\alpha^2 = 0$ ist oder (α^2) ein Einselement hat. Wir haben schon gesehen, daß $\omega = \lambda\alpha \pm \alpha$ mit einem $\lambda \in R$ ist. Ohne Beschränkung der Allgemeinheit können wir $\omega = \lambda\alpha - \alpha$ setzen. Aus $\omega\alpha = 0$ folgt dann $\lambda\alpha^2 = \alpha^2$ und auch

$$\lambda^2\alpha^2 = \alpha^2, \tag{12}$$

also falls $\alpha^2 \neq 0$, so ist auch $\lambda^2 \neq 0$. Da ferner $\lambda^2 \in (\alpha^2)$ ist, so bedeutet (12), daß in diesem Falle λ^2 das Einselement von (α^2) ist. Dies vollendet den Beweis des Satzes 3.

Es ist leicht zu sehen, daß auch umgekehrt, jeder Ring von der Form

(9) ein kommutativer Hauptidealring ohne Multiplikator ist. In der Tat, es sei $\mathfrak{a}$ ein Ideal von R. Ist $R_1 = 0$, so ist offenbar $\mathfrak{a} = (m\omega)$ mit einer ganzen Zahl m und mit demjenigen ω, das R erzeugt. Ist dagegen $R_1 \neq 0$, also R ein k. H. E., so ist

$$R = (\omega) \dotplus (\varepsilon),$$

wo ε ein Idempotent, ω ein Annullator von R ist. Dann gilt

$$\mathfrak{a} = (a\omega) \dotplus (\alpha) = (a\omega + \alpha). \tag{13}$$

Die erste Hälfte von (13) folgt aus der allgemeinen Tatsache, daß in einem Ringe R mit $R = R_1 \dotplus R_2$, wo R_1 ein Ring mit Einselement ist, jedes Ideal $\mathfrak{a}$ sich in der Form $\mathfrak{a} = \mathfrak{a}_1 \dotplus \mathfrak{a}_2$ darstellen läßt, wobei $\mathfrak{a}_i$ $(i = 1, 2)$ ein Ideal von R_i ist. Die zweite Gleichung folgt daraus, daß $\varepsilon(a\omega + \alpha) = \alpha$, d. h. $\alpha \in (a\omega + \alpha)$, $a\omega \in (a\omega + \alpha)$ und folglich $\mathfrak{a} \subseteq (a\omega + \alpha)$ ist. Endlich, wegen $r\omega = 0$ $(r \in R)$, $n\omega \neq 0$ $(n = 1, 2, \ldots)$ enthält R keinen Multiplikator. Unsere Behauptung ist damit bewiesen.

Damit haben wir eine Übersicht von den kommutativen Hauptidealringen ohne Multiplikator bekommen. Bezüglich der übriggebliebenen kommutativen Hauptidealringe beweisen wir

Satz 4. *Ein kommutativer Hauptidealring R hat dann und nur dann eine Schreiersche k. H. E.-Erweiterung R^** (d. h. eine Schreiersche Erweiterung R^*, die ein k. H. E. ist), *wenn R einen Multiplikator enthält. In diesem Falle gibt es sogar einen R^* mit $R^*/R \cong I/(n)$, wo I der Ring der ganzen rationalen Zahlen und $n \neq 0$ ist.*

Beweis. Enthält R keinen Multiplikator, so sei (ω) der Annihilator von R. Nach Satz 3 ist (ω) ein von (0) verschiedener direkter Summand von R. Wäre nun R^* eine Schreiersche k. H. E.-Erweiterung von R, so wäre (ω) ein Ideal auch in R^*[3]). Ist $R^* = R_1^* \dotplus \cdots \dotplus R_n^*$, wo jeder Summand ein u. H. E. ist, so ist (ω) in einem R_i^* enthalten, denn (ω) offenbar direkt unzerlegbar ist. Dann gehört R_i^* zum Typ II, denn wegen $\omega^2 = 0$ R_i^* nicht nullteilerfrei sein kann. Bezeichnet $\mathfrak{p}_i$ das Primideal von R_i^* und ist $\mathfrak{p}_i^n = 0$, $\mathfrak{p}_i^{n-1} \neq 0$, so ist es leicht zu sehen, daß $\mathfrak{p}_i^{n-1} = (\omega)$ sein muß. Da ferner $(\mathfrak{p}_i^{n-1})^+ \cong \cong (R_i^*/\mathfrak{p}_i)^+$ ist, muß $R_i^*/\mathfrak{p}_i$ ein Körper mit einem unendlich zyklischen Modul sein. Einen solchen gibt es aber nicht. Dieser Widerspruch vollendet den Beweis der Notwendigkeit.

Sei jetzt $r \in R$ ein Multiplikator, für den (8) gilt, und zwar nehmen wir an, daß n die kleinste natürliche Zahl ist, für die (8) mit passendem $r \in R$ besteht (d. h. n ist ein Teiler von allen solchen Zahlen). Es sei ferner $R = (\alpha)$.

[3]) Siehe [1], Satz 2.

Dann ist offenbar $R/(\alpha^2)$ ein Zeroring mit zyklischem Modul von Ordnung n. Zuerst betrachten wir den Fall, daß der Annihilator von R $\mathfrak{o}=(\omega)\neq(0)$ ist. Wegen

$$n\omega=\nu\omega=0$$

sind dann $\omega,\ldots,(m-1)\omega$, $m\omega=0$ $(m|n)$ sämtliche verschiedene Elemente von $\mathfrak{o}$. Endlich sei

$$\nu\equiv n_1\alpha,\quad \omega\equiv o_1\alpha \mod \alpha^2 \qquad (0\leqq n_1, o_1<n). \tag{14}$$

Ist dabei $o_1\neq(0)$, so können wir ω so wählen, daß

$$o_1|n \tag{15}$$

ist. In der Tat, sei ω^* ein beliebiges Erzeugende von $\mathfrak{o}$ und sei $\omega^*\equiv o^*\alpha \mod \alpha^2$. Es ist klar, daß auch $c\omega^*$ ein Erzeugende von $\mathfrak{o}$ ist, falls $(c, n)=1$ besteht. Wir können jetzt c so wählen, daß $co^*\equiv(o^*, n) \mod n$ gilt. Aus der letzten Kongruenz folgt aber $c\omega^*\equiv(o^*, n)\alpha \mod \alpha^2$, so daß (15) mit $\omega=c\omega^*$, $o_1=(o^*, n)$ erfüllt ist. Wir können sogar erreichen, daß

$$(n_1, n)|o_1 \tag{16}$$

gelte. Zu diesem Zwecke bemerken wir, daß sämtliche verschiedene Elemente von R, für die (8) gilt, $\nu+k\omega$ $(k=0, 1,\ldots,m-1)$ sind. Aus (14) folgt

$$\nu+k\omega\equiv(n_1+ko_1)\alpha \mod \alpha^2.$$

Für ein passendes k gilt dabei (16) für n_1+ko_1 statt n_1[4]); wir dürfen annehmen, daß dies schon für $k=0$ der Fall ist. Damit haben wir auch ν festgesetzt.

Jetzt konstruieren wir einen Erweiterungsring mit Einselement R^* von R folgendermaßen. Sämtliche verschiedene Elemente von R^* seien $\varrho+r$ $(\varrho\in R, r$ ganze Zahl, $0\leqq r<n)$. Die Verknüpfungen in R^* definieren wir durch

$$\begin{aligned}(\varrho+r)+(\sigma+s)&=\left(\varrho+\sigma+\left[\frac{r+s}{n}\right]\nu\right)+\left(r+s-\left[\frac{r+s}{n}\right]n\right),\\ (\varrho+r)(\sigma+s)&=\left(\varrho\sigma+s\varrho+r\sigma+\left[\frac{rs}{n}\right]\nu\right)+\left(rs-\left[\frac{rs}{n}\right]n\right).\end{aligned} \tag{17}$$

Es ist klar, daß R^* ein Ring ist, die Elemente $\varrho+0$ (die wir im folgenden mit ϱ identifizieren werden) bilden in R^* ein mit R isomorphes Ideal, das durch α erzeugt ist und wofür $R^*/\alpha\cong I/(n)$ gilt. Ferner ist das Element $0+1$ (im folgenden durch 1 bezeichnet, sowie die Elemente $0+r$ durch r) das

[4]) Es ist leicht zu sehen, daß es zu jedem Triplet von ganzen rationalen Zahlen a, b, c ein x gibt, so daß $(a+xc, b)|c$ gilt.

Einselement in R^*[5]). Bemerken wir noch, daß jedes Ideal (ϱ) von R auch Ideal von R^* ist, und durch dasselbe ϱ erzeugt wird, ist also ein Hauptideal auch in R^*. Endlich, der Annihilator von (α) in R^* ist wieder gleich (ω). Wir wollen zeigen, daß R^* ein Hauptidealring ist.

Bemerken wir vor allem, daß in R^* jedes Ideal $\mathfrak{a}$ durch höchstens zwei Elemente erzeugbar ist. Aus dem ersten Isomorphiesatz erhalten wir nämlich

$$\mathfrak{a}/\mathfrak{a}\cap(\alpha)\cong(\mathfrak{a},\alpha)/(\alpha).$$

Die rechte Seite dieses Isomorphismus ist ein Ideal in $R^*/(\alpha)$, ist also isomorph mit einem Unterringe $(d)/(n)$ von $I/(n)$, $d|n$. Daher ist der Ring $\mathfrak{a}/\mathfrak{a}\cap(\alpha)$ durch ein einziges Element erzeugbar, und da wegen $\mathfrak{a}\cap(\alpha)\subseteq(\alpha)$ das Ideal $\mathfrak{a}\cap(\alpha)$ ein Hauptideal ist, ist $\mathfrak{a}$ durch zwei Elemente erzeugbar.

Aus dem Bewiesenen folgt, daß in R^* die Maximumbedingung für Ideale erfüllt ist. Darum genügt es zu zeigen, daß in R^* jedes irreduzible Ideal (d. h. jedes Ideal $\mathfrak{a}$, für welches aus $\mathfrak{a}=\mathfrak{b}\mathfrak{c}$ $\mathfrak{b}=\mathfrak{a}$ oder $\mathfrak{c}=\mathfrak{a}$ folgt) ein Hauptideal ist. Hieraus folgt nämlich die Hauptidealeigenschaft für sämtliche Ideale durch vollständige Induktion. Wir werden also zeigen, daß ein Ideal entweder reduzibel oder ein Hauptideal ist.

Betrachten wir zuerst diejenigen Ideale $\mathfrak{a}$, die α enthalten; sie sind alle in der Form $\mathfrak{a}=(\alpha,d)$ darstellbar, wo $d|n$ ist. Sei $dd'=n$. Das Ideal $(\alpha,d)(\alpha)=(\alpha^2,d\alpha)$ sei durch $\gamma=(\beta+bd)\alpha$ erzeugt. Dann ist erstens $(\eta+y)\gamma=d\alpha$ mit passenden η, y und da $(\eta+y)\gamma\equiv ybd\alpha \bmod \alpha^2$ ist, muß

$$(b,d')=1 \tag{18}$$

gelten. Zweitens, mit passenden ξ, x gilt auch $(\xi+x)\gamma=\alpha^2$, also

$$(\xi+x)(\beta+bd+z\omega)=\alpha+t\omega \tag{19}$$

mit beliebigem z. Hieraus sieht man vor allem $xbd\in(\alpha)$, d. h. $n|xbd$ und wegen (18) $d'|x$. Sei $x=d'x'$, $\xi\equiv x_1\alpha$, $\beta\equiv b_1\alpha \bmod \alpha^2$. Dann gehen wir von (19) zur Kongruenz

$$(xb_1+x_1bd)\alpha+xz\omega+x'by\equiv\alpha+t\omega \qquad \bmod \alpha^2$$

über, woher wir auf Grund von (14)

$$x'(d'(b_1+zo_1)+bn_1)+x_1bd\equiv 1+to_1 \qquad \bmod n \tag{20}$$

bekommen. Wir führen noch die Bezeichnung

$$(d'(b_1+zo_1)+bn_1, bd, n)=d_z$$

ein. Aus (20) folgt

$$(d_z, o_1)=1. \tag{21}$$

[5]) Über die Konstruktion und die nachfolgenden Bemerkungen siehe [1].

Wegen (18) und $d|n$ gilt auch $d_z=(d'(b_1+zo_1)+bn_1, d)$. Wir können jetzt z_0 so wählen, daß $d_{z_0}|d'o_1$ sei (siehe die Fußnote [4]), also wegen (21) $d_{z_0}|d'$. Dann ist aber $d_{z_0}|bn_1$ und wegen (18) $(d_{z_0}, b)=1$, d. h.

$$d_{z_0}|n_1. \tag{22}$$

Da andererseits $d_{z_0}|n$ ist, ergibt sich aus (22), (16) und (21) $d_{z_0}=1$. Einfachheitshalber sei $z_0=0$. Dann ist

$$(\alpha, d)=(\beta+bd). \tag{23}$$

In der Tat, es gilt

$$d'(\beta+bd)\alpha\equiv(d'b_1+bn_1)\alpha \qquad \bmod \alpha^2,$$
$$(\beta+bd)\alpha\equiv bd\alpha \qquad \bmod \alpha^2.$$

Wegen (18) wird mit passendem u auch $u(\beta+bd)\alpha\equiv d\alpha \bmod \alpha^2$. Da aber jetzt $(d'b_1+bn_1, d)=d_0=1$ ist, gibt es in $(\beta+bd)$ ein Element ϱ mit $\varrho\equiv\alpha \bmod \alpha^2$. Hieraus und aus $\alpha^2\in(\beta+bd)$ folgt $\alpha\in(\beta+bd)$ und dann auch $d\in(\beta+bd)$, also $(\alpha, d)\subseteq(\beta+bd)$. Da die umgekehrte Inklusion trivial ist, ist (23) richtig. Damit haben wir bewiesen, daß jedes Ideal $\mathfrak{a}$ mit $\alpha\in\mathfrak{a}$ ein Hauptideal ist.

Nehmen wir jetzt an: $\alpha\notin\mathfrak{a}$. Wir haben schon gesehen, daß $\mathfrak{a}$ durch zwei Elemente erzeugbar ist; aus den dort gesagten sieht man sogar, daß für eines der Erzeugenden ein β gewählt werden kann, wofür $(\beta)=\mathfrak{a}\cap(\alpha)$ gilt. Es durchläufe dabei $\varrho+r$ sämtliche Elemente von $\mathfrak{a}$ und bezeichne d den größten gemeinsamen Teiler der so bekommenen r; dann gibt es natürlich in $\mathfrak{a}$ Elemente $\sigma+sd$ mit $\left(s, \frac{n}{d}\right)=1$ und es ist klar, daß jedes solche Element mit β zusammen schon $\mathfrak{a}$ erzeugt:

$$\mathfrak{a}=(\beta, \sigma+sd).$$

Es sei jetzt $\mathfrak{a}(\alpha)=(\tau)$. Dann ist $\tau=(\xi+x)\beta\alpha+(\eta+y)(\sigma+sd)\alpha$. Hier ist $\tau=ysd\alpha \bmod \alpha^2$ und es ist klar, daß $\left(ys, \frac{n}{d}\right)=1$ gelten muß. Darum erzeugt β auch zusammen mit $\delta+qd=(\xi+x)\beta+(\eta+y)(\sigma+sd)$ dasselbe Ideal $\mathfrak{a}$. Wir haben also:

$$\mathfrak{a}=(\beta, \delta+qd);\quad \mathfrak{a}\cap(\alpha)=(\beta);\ \mathfrak{a}(\alpha)=((\delta+qd)\alpha) \tag{24}$$

und $\left(q, \frac{n}{d}\right)=1$.

Offenbar enthält das Ideal (α, d) unser Ideal $\mathfrak{a}$. Da (α, d) ein Hauptideal ist, gilt mit einem passenden $\mathfrak{b}$ sogar

$$(\alpha, d)\mathfrak{b}=\mathfrak{a}.$$

Wegen $\alpha \notin \mathfrak{a}$ ist $\mathfrak{a} \neq (\alpha, d)$. Es genügt also zu zeigen, daß entweder $\mathfrak{b} \neq \mathfrak{a}$, oder $\mathfrak{a}$ ein Hauptideal ist.

Ist $\left(d, \frac{n}{d}\right) = d_1 \neq 1$, so besteht der erste Fall dieser Alternative. Wäre nämlich $(\alpha, d)\mathfrak{a} = \mathfrak{a}$, so wäre auch $(\alpha^2, d\alpha)\mathfrak{a} = \mathfrak{a}(\alpha)$. Aber es ist

$$(\alpha^2, d\alpha)\mathfrak{a} = (\beta\alpha^2, d\beta\alpha, (\delta + qd)\alpha^2,\ d(\delta + qd)\alpha) \subseteq (\alpha^2, d_1 d\alpha),$$

wo doch $(\delta + qd)\alpha \in \mathfrak{a}(\alpha)$, $(\delta + qd)\alpha \notin (\alpha^2, d_1 d\alpha)$, was unmöglich ist.

Ist $\left(d, \frac{n}{d}\right) = 1$, so sei $\beta = (\gamma + c)\alpha$, $(c, n) = \bar{d}$. Wir unterscheiden zwei Fälle, je nachdem $\bar{d} = d$ gilt oder nicht. Zuerst bestehe der zweite Fall; wegen (24) gilt jedenfalls $\bar{d} | d$. Wir zeigen, daß wieder $\mathfrak{b} \neq \mathfrak{a}$ ist. Wäre nämlich $(\alpha, d)\mathfrak{a} = \mathfrak{a}$, so wäre auch

$$(25) \qquad (\beta) = \mathfrak{a} \cap (\alpha) = (\alpha, d)\mathfrak{a} \cap (\alpha) = (d\beta, (\delta + qd)\alpha, d(\delta + qd)) \cap (\alpha).$$

Jedes Element der rechten Seite, u. a. auch β, läßt sich in der Form

$$\beta = d(\xi + x)\beta + (\eta + y)(\delta + qd)\alpha + d(\zeta + z)(\delta + qd) \qquad (zqd^2 \in (\alpha))$$

darstellen. Aber $zqd^2 \in (\alpha)$ ist gleichbedeutend mit $n | zqd^2$, d. h. $\frac{n}{d} \Big| zqd$. Wegen $\left(qd, \frac{n}{d}\right) = 1$ folgt hieraus $\frac{n}{d} \Big| z$; dann ist aber schon $zqd \in (\alpha)$ und damit $\beta \in (\alpha^2, d\alpha)$, im Widerspruch mit der Annahme $\bar{d} \neq d$.

Nun betrachten wir den Fall $\left(d, \frac{n}{d}\right) = 1$, $\bar{d} = d$. Dann gilt

$$(\alpha, d)(\gamma + c + z\omega, \delta + qd) = (\alpha, \delta + qd)(\gamma + c + z\omega, \delta + qd) =$$
$$= (\beta, c(\delta + qd), qd(\delta + qd)) = \mathfrak{a},$$

das letzte wegen $\left(c, qd, \frac{n}{d}\right) = 1$ und wegen der Gleichung

$$(\beta, c(\delta + qd), qd(\delta + qd)) \cap (\alpha) = (\beta).$$

Ist nun für irgendwelches z das Element $\gamma + c + z\omega$ in $\mathfrak{a}$ nicht enthalten, so gilt für das entsprechende Ideal $\mathfrak{b} \neq \mathfrak{a}$. Ist dagegen $\gamma + c + z\omega \in \mathfrak{a}$ für jedes z, so ist $\gamma + c \in \mathfrak{a}$, $\omega \in \mathfrak{a}$. Dabei gilt wegen (24) $(\delta + qd)\alpha = (\lambda + l)(\gamma + c)\alpha$ mit passenden λ, l, also

$$\delta + qd = (\lambda + l)(\gamma + c) + t\omega$$

mit irgendwelchem t. Da aber $\omega \in \mathfrak{a} \cap (\alpha) = ((\gamma + c)\alpha)$ ist, können wir $t = 0$ setzen. Dies bedeutet, daß $\mathfrak{a} = (\gamma + c)$ ist.

Es bleibt noch der Fall, wo $\mathfrak{o}=0$, d. h. α kein Nullteiler ist, übrig. Der Ring R^* mit den Verknüpfungen (17) ist auch in diesem Falle eine Schreiersche Erweiterung von R mit Einselement. Das Element α ist in R^* auch kein Nullteiler, denn aus $(\varrho+r)\alpha=0$ folgt $r\alpha=-\varrho\alpha\in(\alpha^2)$, also $r=0$ und damit $\varrho\alpha=0$, also $\varrho=0$. Ist nun $\mathfrak{a}$ ein Ideal in R^*, so sei $\mathfrak{a}(\alpha)=((\beta+b)\alpha)$. Für $\lambda+l\in\mathfrak{a}$ gilt dann

$$(\lambda+l)\alpha=(\xi+x)(\beta+b)\alpha,$$

also wegen der Regularität von α auch $\lambda+l=(\xi+x)(\beta+b)$, d. h. $\mathfrak{a}\subseteq(\beta+b)$. Andererseits, wenn $\gamma_1+c_1, \gamma_2+c_2, \ldots$ ein Erzeugendensystem von $\mathfrak{a}$ ist, so gilt für ein passendes m

$$(\beta+b)\alpha=(\xi_1+x_1)(\gamma_1+c_1)\alpha+\cdots+(\xi_m+x_m)(\gamma_m+c_m)\alpha,$$

also auch

$$\beta+b=(\xi_1+x_1)(\gamma_1+c_1)+\cdots+(\xi_m+x_m)(\gamma_m+c_m),$$

d. h. $\beta+b\in\mathfrak{a}$ und damit $\mathfrak{a}=(\beta+b)$. Hiermit ist Satz 4 bewiesen.

Es ist leicht zu sehen, daß auch umgekehrt, falls R ein k. H. E. und (α) ein Ideal in R ist, und zwar so, daß $R/(\alpha)\cong I/(n)$ mit einer natürlichen Zahl n gilt, dann (α) selbst ein Hauptidealring ist. Damit können wir die erhaltenen Ergebnisse folgenderweise zusammenfassen:

Jeder kommutative Hauptidealring R zerfällt in eine direkte Summe $R=R_1\dotplus R_2$, wobei $R_1=0$ oder R_1 ein k. H. E. ist und für R_2 einer der folgenden drei Fälle besteht:

$$1.\ R_2=0, \qquad 2.\ R_2\cong N, \qquad 3.\ R_2=R_{21}\dotplus\cdots\dotplus R_{2n},$$

wo jeder R_{2i} ein Ideal in einem u. H. E. R_{2i}^* ist und $R_{2i}^*/R_{2i}\cong I/(n_i)$ mit einer natürlichen Zahl n_i gilt, wobei $(n_i, n_j)=1$ für $i\neq j$.

Es ist nicht schwer zu zeigen, daß eine so erhaltene direkte Zerlegung eines beliebigen kommutativen Hauptidealringes in eine direkte Summe von unzerlegbaren Hauptidealringen (bis auf Ordnung der Summanden) eindeutig ist.

Literatur

[1] B. Brown—N. H. McCoy, Rings with unit element which contain a given ring, *Duke Math. J.*, **13** (1946), 9—20.

(Eingegangen am 26. April 1960)

On random generating elements of a finite Boolean algebra

By A. RÉNYI in Budapest

Dedicated to Professor L. Rédei on his 60th birthday

We consider finite Boolean algebras. As it is well known the number of elements of a finite Boolean algebra is equal to an integral power of two, and if $\mathcal{A}_n$ is a Boolean algebra having 2^n elements ($n=0, 1, 2, \ldots$) then $\mathcal{A}_n$ is isomorphic with the set of all subsets of a set S_n containing exactly n elements. In the present paper we consider the following problem to which the author was led by some problems in information theory: let us choose at random k elements of the Boolean algebra $\mathcal{A}_n$, and let $\mathcal{A}'$ denote the least Boolean subalgebra of $\mathcal{A}_n$ which contains these elements; calculate the probability that $\mathcal{A}'=\mathcal{A}_n$. By other words the question is: what is the probability that k elements of $\mathcal{A}_n$ chosen at random should generate $\mathcal{A}_n$?

We shall calculate this probability for every k, however we are interested in the first place in the question how large k should be in order that the k elements of $\mathcal{A}_n$ selected at random should generate the whole Boolean algebra $\mathcal{A}_n$ with a prescribed probability p where $0<p<1$.

To make the question determined, one has to define what should be understood by the random choice of the elements of $\mathcal{A}_n$. We shall solve our problem under two different definitions of random choice.

Definition 1. We suppose that at every choice every element of $\mathcal{A}_n$ has the same probability to be chosen, and that the subsequent choices are independent. This implies that if $A_1, A_2, \ldots, A_k$ is an arbitrary ordered sequence of elements of $\mathcal{A}_n$ (the same element of $\mathcal{A}_n$ may occur more than once in the sequence $A_1, A_2, \ldots, A_k$) then the probability that exactly these sets will be chosen (in the given order) is equal to $\frac{1}{2^{nk}}$.

Definition 2. We suppose that the first element A_1 is selected so that each element of $\mathcal{A}_n$ has the same probability to be chosen and that at

subsequent choices all those elements which have not yet been selected have the same probability to be chosen as the next. This implies that the randomly chosen elements $A_1, A_2, \ldots, A_k$ are all different and that for any ordered k-tuple $A_1, A_2, \ldots, A_k$, consisting of different elements of $\mathcal{A}_n$ the probability that exactly this k-tuple will be chosen (in the given order) is equal to $\frac{1}{2^n(2^n-1)\ldots(2^n-k+1)}$.

In § 1 and § 2 we solve our problem when Definition 1 or Definition 2 is adopted, respectively. In § 3 we generalize the question considered in § 1.

Before going into details I should like to say a few words about the connection of the problem considered in this paper with information theory. Let x be an unknown element of a set S_n which has n elements. We get information about x in the form that we are informed whether x belongs or not to the subsets $A_1, A_2, \ldots, A_k$ of S_n. Each such answer contains at most one unit of information; thus to determine x uniquely we need at least $\{\log_2 n\}$ such answers ($\{x\}$ denotes the least integer $\geqq x$) as the uncertainty concerning x is equal to $\log_2 n$. Now as well known, there can be in fact chosen $\{\log_2 n\}$ such subsets $A_1^*, A_2^*, \ldots, A_{\{\log_2 n\}}^*$ that every element x of S_n is uniquely determined by the information to which of the sets $A_1^*, A_1^*, \ldots, A_{\{\log_2 n\}}^*$ it belongs and to which not. For instance let the elements of S_n be labelled with the numbers $0, 1, \ldots, n-1$ and let A_j^* $(j = 1, 2, \ldots, \{\log_2 n\})$ denote the subset of those elements of S_n which are labelled by such a number m which when written in the binary system has its j-th digit equal to 1, i. e. is of the form

$$m = \sum_{h=1}^{\{\log_2 n\}} b_h \cdot 2^{h-1} \quad \text{(where } b_h = 1 \text{ or } b_h = 0\text{) with } b_j = 1.$$

Then clearly if it is known whether x belogs to A_j^* or not for $j = 1, 2, \ldots, \{\log_2 n\}$, then the binary expansion of x and thus x itself is uniquely determined. This can be expressed also in the following way: to any two elements x and $y \neq x$ of S_n there is at least one among the sets $A_1^*, A_2^*, \ldots, A_{\{\log_2 n\}}^*$ which separates the elements x and y, that is one of them is contained in this set and the other not.

We shall call such a system of sets which may be used to separate any two elements of a set a *separating set of subsets*. Evidently a separating set of subsets of S_n has at least $\{\log_2 n\}$ elements. We shall call a separating system of subsets of S_n consisting of exactly $\{\log_2 n\}$ sets an *optimal separating system*.

Now the question arises that if we do not choose the subsets $A_1, A_2, \ldots, A_k$

in such an optimal and systematic way, but choose them at random, how many subsets have to be chosen in order that the system of sets obtained should be a separating system, with a prescribed probability p. Clearly this is equivalent to demanding that the least algebra $\mathcal{A}'$ of subsets of S_n containing the sets $A_1, A_2, \ldots, A_k$ should be the set of all subsets of S_n. As a matter of fact the requirement that the sets $A_1, A_2, \ldots, A_k$ should form a separating system for the set S_n is equivalent with the assertion that the atoms of the least algebra $\mathcal{A}'$ containing $A_1, A_2, \ldots, A_k$ should consist each of only one element of S_n, and this is equivalent with saying that the subsets $A_1, A_2, \ldots, A_k$ generate the set of all subsets of S_n.

Of course this is possible only if $k \geqq \{\log_2 n\}$, thus at least $\{\log_2 n\}$ sets are needed for this purpose, and the question is exactly this: how much larger k should be than $\{\log_2 n\}$? Theorem 1 gives an answer to this question.

§ 1. Random choice of subsets according to Definition 1

In this § we suppose that the random choice of the elements $A_1, A_2, \ldots, A_k$ of the Boolean algebra $\mathcal{A}_n$ is subject to Definition 1, i. e. these elements are chosen independently of each other and each may be equal with the same probability $\left(\text{i. e. with probability } \frac{1}{2^n}\right)$ to each of the 2^n elements of $\mathcal{A}_n$. Let $P(\ldots)$ denote the probability of the event in the brackets.

We prove the following

Theorem 1. *Let $E_{n,k}$ denote the event that the random elements $A_1, A_2, \ldots, A_k$ of the finite Boolean algebra $\mathcal{A}_n$ (having 2^n elements) generate the whole algebra $\mathcal{A}_n$, supposing that these elements are chosen independently and each element of $\mathcal{A}_n$ has the same probability to be selected at every choice. Then we have*

$$P(E_{n,k}) = \prod_{j=1}^{n-1}\left(1-\frac{j}{2^k}\right). \tag{1}$$

Proof. Without restricting the generality we may suppose that the Boolean algebra $\mathcal{A}_n$ in question is the set of all subsets of a set S_n having n elements, which we denote by $a_1, a_2, \ldots, a_n$. Every subset A of S_n can be characterized completely by the sequence of numbers $\varepsilon_h(A)$ $(h = 1, 2, \ldots, n)$ where $\varepsilon_h(A) = 1$ or $= 0$ according to whether A contains a_h or not. If A is selected at random so that each of the 2^n subsets of S_n has the same probability to be chosen, then the $\varepsilon_h(A)$ $(h = 1, 2, \ldots, n)$ are independent random variables each taking on the values 1 and 0 with probability $\frac{1}{2}$. As a

matter of fact if $\delta_1, \delta_2, \ldots, \delta_n$ is an arbitrary sequence of zeros and ones there is exactly one subset A of S_n for which $\varepsilon_h(A) = \delta_h$ for $h = 1, 2, \ldots, n$ and thus

$$P(\varepsilon_1(A) = \delta_1, \varepsilon_2(A) = \delta_2, \ldots, \varepsilon_n(A) = \delta_n) = \frac{1}{2^n} \tag{2}$$

for each such sequence $\delta_1, \delta_2, \ldots, \delta_n$.

Let us consider now the random variables $\varepsilon_h(A_j)$ $(h = 1, 2, \ldots, n; j = 1, 2, \ldots, k)$. According to what has been said and to Definition 1 the random variables $\varepsilon_h(A_j)$ $(h = 1, 2, \ldots, n; j = 1, 2, \ldots, k)$ are all independent and each takes on the values 1 and 0 with probability $\frac{1}{2}$. Consequently the random k-dimensional vectors $\mathfrak{V}_h = (\varepsilon_h(A_1), \varepsilon_h(A_2), \ldots, \varepsilon_h(A_k))$ $(h = 1, 2, \ldots, n)$ are also independent, and each takes on any of its possible 2^k values with probability $\frac{1}{2^k}$. Now clearly the event $E_{n,k}$ is equivalent with the statement that the vectors $\mathfrak{V}_1, \mathfrak{V}_2, \ldots, \mathfrak{V}_n$ are all different. Thus we have

$$P(E_{n,k}) = \frac{\prod_{j=0}^{n-1}(2^k - j)}{2^{kn}} = \prod_{j=1}^{n-1}\left(1 - \frac{j}{2^k}\right),$$

which proves Theorem 1.

We deduce from Theorem 1 by some easy calculations the following

Corollary. *If n_j and k_j are two sequences of positive integers such that the limit*

$$\lim_{j \to +\infty} (k_j - 2 \log_2 n_j) = c \tag{3}$$

exists, then

$$\lim_{j \to +\infty} P(E_{n_j, k_j}) = \begin{cases} 1 & \text{if } c = +\infty, \\ e^{-1/2^{c+1}} & \text{if } c \text{ is finite}, \\ 0 & \text{if } c = -\infty. \end{cases} \tag{4}$$

Theorem 1 shows that if we choose the subsets $A_1, A_2, \ldots, A_k$ of the set S_n at random then the number of such sets which are required, in order that these sets should with considerable probability generate the full Boolean algebra of subsets of S_n, is roughly twice as large as the minimal number of systematically selected subsets which have this property. Especially if $k \sim 2 \log_2 n$ then choosing k subsets of S_n at random these will generate the full Boolean algebra with a probability tending to $e^{-1/2} = 0{,}6065\ldots$.

An other formulation of Theorem 1 is as follows: let us choose at random (according to Definition 1) elements of $\mathfrak{A}_n$ and denote them by

$A_1, A_2, \ldots$. Let $\mathcal{A}^{(k)}$ be the least subalgebra of $\mathcal{A}_n$ containing $A_1, A_2, \ldots, A_k$. Let ν_n denote the least integer for which $\mathcal{A}^{(\nu_n)} = \mathcal{A}_n$. Then ν_n is a random variable which has the probability distribution

$$P(\nu_n \leqq k) = \prod_{j=1}^{n-1}\left(1-\frac{j}{2^k}\right). \tag{5}$$

It follows that

$$\lim_{n\to+\infty} P(\nu_n - 2\log_2 n \leqq c) = e^{-\frac{1}{2^{c+1}}}. \tag{6}$$

Note that it follows from (1) that $P(E_{nk})$ vanishes (as it should) for $2^k < n$ while in the case $2^k = n$ we have

$$P(E_{2^k,k}) = \frac{2^k!}{2^{k\cdot 2^k}}. \tag{7}$$

Thus the probability to find by random choice an optimal separating system of subsets is fairly small. The numerator $2^k!$ of the fraction on the right of (7) is clearly nothing else than the number of different optimal separating systems for S_{2^k}. That this number is $2^k!$ can be proved also directly as follows: each set in an optimal separating system for the set S_{2^k} has to consist clearly of 2^{k-1} elements, the second set has to dissect the first set as well as its complementary set into two subsets of 2^{k-2} elements each, the third set has to dissect all of these four subsets into two subsets of 2^{k-3} elements each, etc. Thus we obtain for the number $O(k)$ of optimal separating systems

$$O(k) = \binom{2^k}{2^{k-1}}\cdot\binom{2^{k-1}}{2^{k-2}}^2\cdot\binom{2^{k-2}}{2^{k-3}}^4\cdots\binom{2}{1}^{2^{k-1}} = 2^k! \tag{8}$$

which is equivalent with (7).

Of course in the number $2^k!$ each optimal separating system is counted in every possible order of its elements. Thus the number $O^*(k)$ of essentially different optimal separating system for S_{2^k} is

$$O^*(k) = \frac{2^k!}{k!}. \tag{9}$$

The result of the Corollary of Theorem 1 is rather surprising as one would have expected that with random selection a much larger number of sets is necessary in the average to generate the whole algebra. Let us remember that in principle among the sets $A_1, A_2, \ldots, A_k$ the same set may occur more than once (though the probability of this is rather small). In the next § we shall show that the result remains valid if this is excluded, i. e. if we adopt Definition 2 for the random selection of sets.

§ 2. Random choice of subsets according to Definition 2

Let us denote by $E^*_{n,k}$ the event that if the selection of sets is made according to Definition 2, the selected sets $A_1, A_2, \ldots, A_k$ generate the Boolean algebra of all subsets of S_n. Clearly we have

$$P(E^*_{n,k}) = \frac{M(n,k)}{2^{nk}} \tag{10}$$

where $M(n,k)$ denotes the number of such matrices having k rows and n columns each element of which is equal to 0 or 1, which have the property that all its row vectors are different and all its column vectors are different.

The exact formula for $M(n,k)$ is rather complicated. We shall consider here only the asymptotic behaviour of $P(E^*_{n,k})$ and prove that the Corollary of Theorem 1 holds for $P(E^*_{n_j,k_j})$ instead of $P(E_{n_j,k_j})$ too. This can be shown as follows: we have clearly

$$P(E^*_{n,k}) = \frac{P(E_{n,k}B_{n,k})}{P(B_{n,k})} \tag{11}$$

where the product of two sets denotes their intersection and $B_{n,k}$ denotes the event that if the subsets $A_1, A_2, \ldots, A_k$ of S_n are chosen at random according to Definition 1 they turn out to be all different. If $\bar{B}_{n,k}$ denotes the event contrary to $B_{n,k}$, it follows that

$$\frac{P(E_{n,k}) - P(\bar{B}_{n,k})}{1 - P(\bar{B}_{n,k})} \leqq P(E^*_{n,k}) \leqq \frac{P(E_{n,k})}{1 - P(\bar{B}_{n,k})}. \tag{12}$$

Now clearly

$$P(\bar{B}_{n,k}) \leqq \frac{\binom{k}{2}}{2^n} = o(1) \quad \text{if} \quad k = o(2^{\frac{n}{2}}). \tag{13}$$

It follows from (12), (13) and (4) that if

$$\lim_{j \to +\infty} (k_j - 2\log_2 n_j) = c \tag{14}$$

then

$$\lim_{j \to +\infty} P(E^*_{n_j,k_j}) = \begin{cases} 1 & \text{if} \quad c = +\infty, \\ e^{-1/2^{c+1}} & \text{if} \quad c \quad \text{is finite}, \\ 0 & \text{if} \quad c = -\infty. \end{cases} \tag{15}$$

Thus the same asymptotic results hold for $P(E^*_{nk})$ as for $P(E_{nk})$.

§ 3. Generalizations

We may ask the following question. If we choose n and k so that the probability of E_{nk} should be essentially less than 1, what can be said about the structure of the least subalgebra $\mathcal{A}'$ of $\mathcal{A}_n$ which contains the random sets $A_1, A_2, \ldots, A_k$. Let $B_1, B_2, \ldots, B_r$ be the atoms of $\mathcal{A}'$, then $B_1, B_2, \ldots, B_r$ are disjoint subsets of S_n whose union is equal to S_n. If there are r_s atoms B_i which consist of exactly s elements of S_n then

$$\sum_{s=1}^{n} s r_s = n \quad \text{and} \quad \sum_{s=1}^{n} r_s = r \leqq 2^k \tag{16}$$

and the sequence $(r_1, r_2, \ldots, r_n)$ may be called the *signature* of $\mathcal{A}'$. Clearly $\mathcal{A}' = \mathcal{A}_n$ if and only if the signature of $\mathcal{A}'$ is $(n, 0, 0, \ldots, 0)$.

Now we may ask what is the probability that $\mathcal{A}'$ should have a prescribed signature $(r_1, r_2, \ldots, r_n)$ (we suppose (16) to be satisfied). According to what has been said in § 1 this problem is equivalent with the following one: put n balls into 2^k urns independently from each other; what is the probability that there will be among the 2^k urns exactly r_s urns which contain exactly s balls $(s = 1, 2, \ldots, n)$? The answer to this question may be easily given by elementary combinatorial considerations: the probability in question is

$$\frac{2^k! \cdot n!}{2^{kn} \cdot \left(\prod_{s=1}^{n} r_s! \, (s!)^{r_s} \right) \left(2^k - \sum_{s=1}^{n} r_s \right)!} \tag{17}$$

Especially one gets from (17) if $r_1 = n$, $r_s = 0$ for $s > 1$ Theorem 1 as a special case.

Other results of a similar type on systems of random subsets of a finite set will be given elsewhere ([1], [2]). The theory of systems of random subsets of a finite set can be developed along similar lines as the theory of random graphs as worked out by P. ERDŐS and the author of the present paper (see [3]).

References

[1] RÉNYI A., Egy általános módszer valószínűségszámítási tételek bizonyítására és annak néhány alkalmazása, *Magyar Tud. Akad. Mat. Fiz. Oszt. Közl.* (in print).

[2] A. RÉNYI, On random subsets of a finite set, *Mathematica* (Cluj) (in print).

[3] P. ERDŐS and A. RÉNYI, On the evolution of random graphs, *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, **5** (1960), 17—61.

(Received January 18, 1961)

Die einstufig nichtregulären bzw. nichtprimen Ringe

Von O. STEINFELD in Budapest

Meinem verehrten Lehrer, Herrn Professor L. Rédei zum 60. Geburtstag gewidmet

Die nullteilerfreien Ringe[1]) heißen auch *regulär*. Nach L. RÉDEI nennen wir jeden nichtregulären Ring, dessen echte Unterringe regulär sind, *einstufig nichtregulär*. RÉDEI hat in seiner Arbeit[2]) den folgenden interessanten Satz bewiesen.

Satz 1. *Die sämtlichen einstufig nichtregulären Ringe sind die Zeroringe von Primzahlordnung*[3]) *und die direkten Summen von zwei endlichen Primkörpern.*

Einen Ring nennt man *prim*, in dem die Null ein Primideal[4]) ist. Jeder nichtprime Ring, dessen echte Unterringe prim sind, heißt *einstufig nichtprim*.

Wir wollen in dieser Arbeit einerseits einen neuen Beweis für den Satz von RÉDEI geben, anderseits beweisen wir den folgenden

Satz 2. *Die sämtlichen einstufig nichtprimen Ringe sind die Zeroringe von Primzahlordnung und die direkten Summen von zwei endlichen Primkörpern.*

Aus den Sätzen 1 und 2 folgt unmittelbar

Korollar. *Ein Ring ist dann und nur dann einstufig nichtregulär, wenn er einstufig nichtprim ist.*

Wir bemerken, daß ein regulärer Ring immer prim ist. Die vollen Matrizenringe über einem Schiefkörper sind prim, aber nichtregulär. Die Tatsache, daß die Klasse der einstufig nichtregulären Ringe und die der einstufig nichtprimen Ringe übereinstimmen, ist also ein wenig überraschend.

Wir schicken den folgenden Hilfssatz voraus.

---

[1]) Unter einem Ring verstehen wir immer einen assoziativen Ring.

[2]) L. RÉDEI, Die einstufig nichtregulären Ringe, *Acta Sci. Math.*, **20** (1959), 238—244.

[3]) Ein Ring, dessen Quadrat 0 ist, heißt ein *Zeroring*. Unter der *Ordnung* eines endlichen Ringes verstehen wir die Anzahl seiner Elemente.

[4]) Ein Ideal $\mathfrak{p}$ eines Ringes R wird *prim* (oder ein *Primideal*) genannt, wenn für irgendwelche Ideale $\mathfrak{a}, \mathfrak{b}$ von R aus $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ entweder $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$ folgt.

Hilfssatz. *Ein Ring R ohne echte Unterringe ist entweder ein Zeroring von Primzahlordnung oder ein endlicher Primkörper.*

Beweis. Besitzt der Ring R ein Element $a(\neq 0)$ mit $Ra=0$, so ist das annullierende Rechtsideal[5]) von R selbst der Ring R. R ist also in diesem Falle ein Zeroring von Primzahlordnung.

Hat der Ring R kein von Null verschiedenes Element a mit $Ra=0$, so sind für jedes Element $a(\neq 0)$ von R

$$Ra=R \quad \text{und} \quad aR=R \tag{1}$$

gültig. R ist also ein Schiefkörper, der wegen der Voraussetzung ein endlicher Primkörper sein muß.[6])

Beweis von Satz 1. Ist R ein Zeroring von Primzahlordnung, so ist R nichtregulär, ferner hat R keine echten Unterringe, deshalb ist R tatsächlich einstufig nichtregulär.

Es sei R die direkte Summe der endlichen Primkörper K und L. Das Produkt von zwei von Null verschiedenen Elementen des Ringes R ist dann und nur dann Null, wenn das eine Element in K, das andere in L liegt, also die zwei miteinander R erzeugen. Hiernach ist R wieder einstufig nichtregulär.[7])

Umgekehrt sei R ein einstufig nichtregulärer Ring. Nach der Voraussetzung hat R zwei Elemente $\alpha\neq 0$, $\beta\neq 0$ mit

$$\alpha\beta=0 \qquad (\alpha\neq 0,\ \beta\neq 0). \tag{2}$$

Das annullierende Linksideal $\mathfrak{l}$ des Elementes β ist wegen (2) von Null verschieden.

Gilt $\mathfrak{l}=R$, so ist das annullierende Rechtsideal $\mathfrak{r}$ von R wegen $R\beta=0$ $(\beta\neq 0)$ von Null verschiedenen. $\mathfrak{r}$ kann wegen $R\mathfrak{r}=0$ kein echter Unterring von R sein. R ist also in diesem Falle ein Zeroring von Primzahlordnung.

Wenn $\mathfrak{l}\subset R$ gültig ist, so gilt wegen $\mathfrak{l}\beta=0$ auch

$$\beta\mathfrak{l}\cdot\beta\mathfrak{l}=\beta\cdot\mathfrak{l}\beta\cdot\mathfrak{l}=0. \tag{3}$$

$\beta\mathfrak{l}$ ist also wegen $\beta\mathfrak{l}\subseteqq\mathfrak{l}\subset R$ ein echter, nichtregulärer Unterring von R, deshalb muß

$$\beta\mathfrak{l}=0 \qquad (\beta\neq 0) \tag{4}$$

bestehen. Die Elemente, die das Linksideal $\mathfrak{l}$ von links annullieren, bilden ein

---

[5]) Unter dem *annullierenden Rechtsideal* einer Untermenge H des Ringes R verstehen wir die Menge aller Elemente von R, die die Untermenge H von rechts annullieren. Ähnlich definiert man das *annullierende Linksideal* von H.

[6]) Vgl. mit dem Beweis von Lemma 1 der Arbeit von F. A. Szász, Note on rings in wich every proper left-ideal is cyclic, *Fundamenta Math.*, **44** (1957), 330—332.

[7]) Dieser Teil des Beweises stimmt mit dem Beweis von L. Rédei vollständig überein.

zweiseitiges Ideal $\mathfrak{m} \neq 0$. Wegen $\mathfrak{l}^2 \neq 0$ ist $R\mathfrak{l} \neq 0$, woraus $\mathfrak{m} \subset R$ folgt. R besitzt also ein zweiseitiges Ideal $\mathfrak{m}$ mit der Eigenschaft

$$\mathfrak{m}\mathfrak{l} = 0 \qquad (0 \subset \mathfrak{m} \subset R;\ 0 \subset \mathfrak{l} \subset R). \tag{5}$$

Bezeichne $\mathfrak{n}$ das annullierende Rechtsideal des Ideals $\mathfrak{m}$. Wegen (5) und wegen $\mathfrak{m}R \supseteq \mathfrak{m}^2 \neq 0$ ist $\mathfrak{n}$ ein von Null verschiedenes, echtes (zweiseitiges) Ideal von R mit der Eigenschaft

$$\mathfrak{m}\mathfrak{n} = 0 \qquad (0 \subset \mathfrak{m} \subset R;\ 0 \subset \mathfrak{n} \subset R). \tag{6}$$

Wegen (6) besteht auch $\mathfrak{m} \cap \mathfrak{n} = 0$.

Da die direkte Summe $\mathfrak{m} \oplus \mathfrak{n}$ der Ideale $\mathfrak{m}, \mathfrak{n}$ nach (6) Nullteiler hat, muß

$$\mathfrak{m} \oplus \mathfrak{n} = R \tag{7}$$

bestehen. Die Ideale $\mathfrak{m}$ und $\mathfrak{n}$ können keine echten Unterringe enthalten, denn im entgegengesetzten Falle hätte R von Null verschiedene, echte, nichtreguläre Unterringe, was unmöglich ist. $\mathfrak{m}$ und $\mathfrak{n}$ sind also infolge des Hilfssatzes endliche Primkörper, womit Satz 1 bewiesen ist.

Beweis von Satz 2. Da ein Zeroring R von Primzahlordnung nichtprim und ohne echte Unterringe ist, ist R tatsächlich einstufig nichtprim.

Ist R die direkte Summe von zwei endlichen Primkörpern, so ist R nichtprim und besitz kein von Null verschiedenes, nilpotentes Element. Da die Ordnung von R das Produkt von zwei (nicht notwendig verschiedenen) Primzahlen ist, ist ein beliebiger echter Unterring $R'(\neq 0)$ von R von Primzahlordnung. R' hat also keinen echten Unterring $(\neq 0)$, deshalb muß R' infolge des Hilfssatzes ein Primkörper, also ein primer Ring sein.

Umgekehrt sei R ein einstufig nichtprimer Ring. Nach der Definition enthält R zwei Ideale $\mathfrak{a} \neq 0$ und $\mathfrak{b} \neq 0$ mit

$$\mathfrak{a}\mathfrak{b} = 0. \tag{8}$$

Ist unter den Idealen $\mathfrak{a}, \mathfrak{b}$ das eine gleich dem Ring R, so muß auch das andere mit R übereinstimmen. Im entgegengesetzten Falle hätte nämlich R einen echten, nichtprimen Unterring. R ist also jetzt ein Zeroring von Primzahlordnung.

Wenn beide Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von R verschieden sind, so ist wegen (8)

$$\mathfrak{a} \cap \mathfrak{b} = 0 \qquad (0 \subset \mathfrak{a},\ \mathfrak{b} \subset R) \tag{9}$$

gültig. In diesem Falle ist R die direkte Summe der Ideale $\mathfrak{a}, \mathfrak{b}$, d. h.

$$R = \mathfrak{a} \oplus \mathfrak{b}.$$

$\mathfrak{a}$ und $\mathfrak{b}$ können keine echten Unterringe $(\neq 0)$ enthalten, also sind sie infolge des Hilfssatzes endliche Primkörper. Damit ist der Beweis beendet.

(Eingegangen am 24. September 1960)

Über zerteilte Parallelogramme

Von JÁNOS SURÁNYI in Budapest

Professor L. Rédei zu seinem 60. Geburtstag gewidmet

1. Der folgende Satz von DELONE [2] fand vielfältige Anwendungen in der Geometrie der Zahlen:

Satz I. *Es sei ein Parallelogrammgitter und ein Koordinatensystem in der Ebene gegeben, derart, daß kein Gitterpunkt auf den Koordinatenachsen liegt. Dann gibt es ein Parallelogramm mit Gitterpunkten als Eckpunkte, die alle in verschiedenen Quadranten der Koordinatenebene liegen, und so daß das abgeschlossene Parallelogramm keinen weiteren Gitterpunkt enthält.*

Ein Parallelogramm mit den erwähnten Eigenschaften nenne ich nach DELONE „zerteilt".

Mehrere Beweise dieses Satzes sind bekannt, darunter ein sehr einfacher Beweis von L. RÉDEI [5]. Ich fand einen weiteren einfachen Beweis, den ich auf RÉDEIS Veranlassung hier darlege. Ich nenne, wie üblich, die Gebiete $x>0, y>0$; $x<0, y>0$; $x<0, y<0$; $x>0, y<0$ der Reihe nach den ersten, zweiten, dritten bzw. vierten Quadranten. A und B seien zwei Gitterpunkte des ersten bzw. des zweiten Quadranten, ihre Projektionen auf die X-Achse seien P bzw. Q. Wir wählen die Gitterpunkte A, B so, daß das abgeschlossene Viereck $ABQP$ keinen Gitterpunkt des ersten und zweiten Quadranten außerhalb A und B enthält. Wir betrachten das durch die Strecke AB und die Halbgeraden AP und BQ begrenzte Halbstreifen S und die erste zu AB parallele, durch Gitterpunkte gehende Gerade g, die S durchschneidet. An g liegen unendlich viele Gitterpunkte, die nach einander in dem Abstand AB folgen. Die zur y-Achse am nächsten liegenden Gitterpunkte von g mit negativer bzw. positiver Abszisse seien C und D. Wenigstens einer von ihnen, etwa C, liegt im Inneren oder an der Grenze von S (Abb. 1). (Liegt D in S, so ist der Beweis mutatis mutandis derselbe.)

Nach seiner Wahl, liegt C im dritten Quadranten. Liegt D im vierten Quadranten, so ist $ABCD$ ein zerteiltes Parallelogramm. Liegt aber D im

ersten Quadranten, so sind die Geraden BC und AD benachbarte, zueinander parallele, durch Gitterpunkte gehende Geraden. Es seien A' bzw. D' die zur X-Achse am nächsten liegenden Gitterpunkte mit positiver bzw. negativer Ordinate. Da A näher zur y-Achse liegt als D, muß D' ferner von dieser Achse liegen als A', und beide liegen ferner von der Y-Achse als A. So liegt A' im ersten und D' im vierten Quadranten. In diesem Falle ist also $A'BCD'$ ein zerteiltes Parallelogramm. Damit ist der Satz bewiesen.

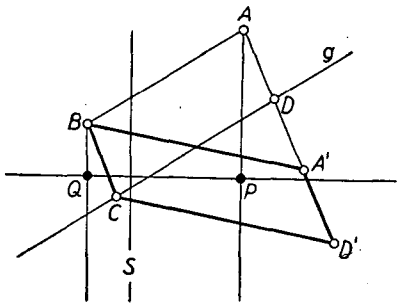

Abb. 1

2. Der Satz gilt auch ohne irgendwelche Voraussetzungen bezüglich der Achsen, wenn man etwa die negative X-Achse und die positive Y-Achse zum zweiten Quadranten, die positive X-Achse, die negative Y-Achse und den Punkt $O(0,0)$ zum vierten Quadranten hinzufügt. Der Beweis kann ohne Änderungen beibehalten werden.

3. Als Anwendung gebe ich geometrische Beweise für drei Sätze über das Produkt von zwei binären linearen Formen:

Satz II (MINKOWSKI [4]). *Es seien zwei inhomogene binäre lineare Formen*

$$x = a_1u + b_1v + c_1, \quad y = a_2u + b_2v + c_2$$

mit $\Delta = |a_1b_2 - a_2b_1| > 0$ *gegeben. Dann gibt es ganze Werte von* u *und* v *mit*

$$|xy| \leqq \frac{\Delta}{4}. \tag{1}$$

Satz III (DAVENPORT—HEILBRONN [1]). *Bei den obigen Bezeichnungen gibt es ganze Werte von* u *und* v *mit* $x>0, y>0$ *und*

$$xy \leqq \Delta. \tag{2}$$

Satz IV (KORKINE—ZOLATAREFF [3]). *Es seien zwei homogene lineare Formen*

$$x = a_1u + b_1v, \quad y = a_2u + b_2v$$

mit $\Delta = |a_1b_2 - a_2b_1| > 0$ *gegeben. Dann gibt es ganze, von* $u = v = 0$ *verschiedene Werte* u *und* v *mit*

$$|xy| \leqq \frac{\Delta}{\sqrt{5}}.$$

Die Punkte (x, y) mit ganzen Werten von u und v bilden einen Paral-

lelogrammgitter in der Ebene, worin der Inhalt der Fundamentalparallelogramme[1]) gleich Δ ist. Das Gitter ist homogen bzw. inhomogen, je nach dem die linearen Formen x, y homogen bzw. inhomogen sind. Der erste Fall wird — entsprechend der Bemerkung im Abschnitt 2 — als spezialfall des letzteren behandelt. Das Produkt $|xy|$ kann etwa als der doppelte Inhalt des rechtwinkligen Dreiecks, dessen Ecken O, $P(x, y)$ und die Projektion von P auf eine der Achsen sind, gedeutet werden. Diese Dreiecke werde ich der Kürze halber als Projektionsdreiecke von P bezüglich der x- bzw. y-Achse nennen.

4. Gibt es einen Gitterpunkt an einer der Achsen, so gilt für seine Koordinaten $xy = 0 < \Delta/4$. Im übrigen Fall sei $ABCD$ ein zerteiltes Parallelogramm, dessen Ecken in der angegebenen Reihenfolge im ersten, zweiten, dritten und vierten Quadranten liegen. Die Diagonalen zerteilen dieses Parallelogramm in vier Dreiecke vom gleichen Inhalt $\Delta/4$. Der Punkt O liege etwa im Dreieck, dessen eine Seite AB ist. Dann gilt $OAB \leqq \Delta/4$.

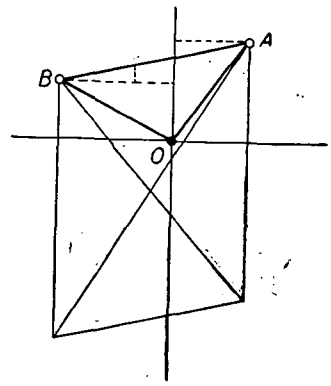

Abb. 2

Die y-Achse zerteilt das Dreieck OAB in zwei Dreiecke, von denen das eine im Projektionsdreieck bezüglich der y-Achse seiner Gitterpunktecke enthalten ist, das andere enthält das entsprechende Projektionsdreieck (Abb. 2). Wenn der Inhalt des Teildreiecks mit der letzteren Eigenschaft nicht größer als der des anderen Teils ist, dann ist dieser Inhalt, also auch der des entsprechenden Projektionsdreiecks höchstens gleich $\Delta/8$. Im Gegenfalle spiegeln wir den über OAB übergreifenden Teil des Projektionsdreiecks der erst erwähnten Art über den Mittelpunkt von AB. Dieses Spiegelbild liegt in OAB, aber außerhalb des anderen Projektionsdreiecks. In diesem Fall ist also der Gesamtinhalt der beiden Projektionsdreiecke kleiner als der Inhalt von OAB. Der Inhalt des kleineren Projektionsdreiecks ist also in beiden Fällen höchstens gleich $\Delta/8$, für seine Gitterpunktecke ist somit (1) erfüllt.[2])

Der Beweis zeigt auch, daß das Gleichheitszeichen weggelassen werden kann, es sei denn, daß $ABCD$ ein Rechteck mit achsenparallelen Seiten und mit dem Mittelpunkt O ist.

---

[1]) D. h. ein Parallelogramm, dessen Eckpunkte Gitterpunkte sind, das aber keinen weiteren Gitterpunkt weder im Inneren noch am Rande enthält. Alle solche Parallelogramme haben denselben Inhalt.

[2]) Dieser Beweis ist im wesentlichen das geometrische Analogon des eleganten Beweises von D. B. Sawyer [6].

5. Zum Beweis des Satzes III benutzen wir Satz I in der im Abschnitt 2 erwähnten schärferen Form. $ABCD$ sei ein zerteiltes Parallelogramm, wobei die Achsen auf die angedeutete Art zum zweiten bzw. zum vierten Quadranten hinzugefügt werden. Die Ecken sollen in der angegebenen Reihenfolge zum ersten, zweiten, dritten bzw. vierten Quadranten gehören. Man kann annehmen, daß B und D nicht beide an der x-Achse liegen, sonst vertauscht man die Rolle der x- und y-Achsen. Wir nehmen die zu BD parallele Gerade g durch A und daran die zur x-Achse am nächsten liegenden Gitterpunkte A' und E der ersten bzw. des vierten Quadranten (Abb. 3).

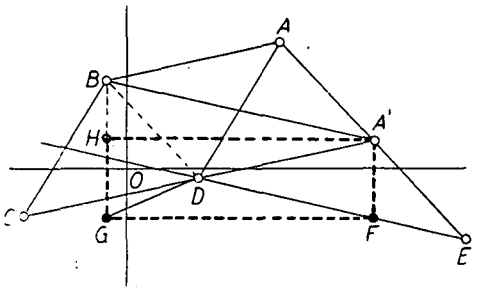

Abb. 3

Da B zum zweiten, D zum vierten Quadranten gehört, liegt E nicht näher zur Y-Achse als A'. Enthält das Parallelogramm $A'BDE$ den Punkt O, so enthält es auch das ganze zu A' gehörende Projektionsdreieck bezüglich der x-Achse. Der Inhalt dieses Projektionsdreiecks ist also nicht größer als $\Delta/2$, da der Inhalt eines Dreiecks, enthalten in einem Parallelogramm, kann die Hälfte des Inhalts des Parallelogramms nicht übertreffen, Gleichheit besteht nur dann, wenn zwei Ecken des Dreiecks benachbarte Ecken des Parallelogramms sind und das dritte Eck des Dreiecks an der gegenüberliegenden Seite des Parallelogramms liegt.

6. Sei nun O außerhalb des Parallelogramms $A'BDE$. Dann liegt wenigstens eine der Projektionen von A' an der x- und y-Achse zwischen den Geraden g und BD. Sonst hätte nämlich die zu BD parallele nächste Gerade, die an der anderen Seite von BD liegt als g (Abb. 4), keinen Punkt mit dem dritten Quadranten gemeinsam, obwohl diese Gerade doch durch C geht.

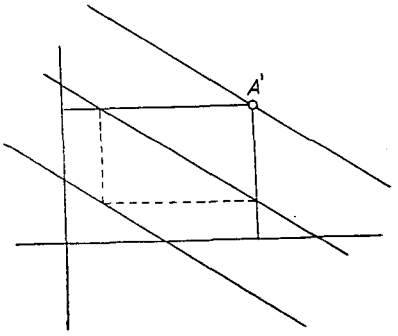

Abb. 4

Liegt die Projektion auf die x-Achse zwischen den beiden Geraden, so schneidet die durch A' gehende, zur y-Achse parallele Gerade die Gerade DE im vierten Quadranten. Zieht man noch durch B eine zur y-Achse parallele Gerade, so schließen diese Geraden, ferner die Geraden BA' und DE ein Parallelogramm vom Inhalt Δ ein und dieser Inhalt ändert sich nicht, wenn

man noch die durch B gehende, zur y-Achse parallele Seite an ihrer Geraden so wegschiebt, daß das Parallelogramm in ein Rechteck $A'FGH$ übergeht (siehe Abb. 3). Dieses Rechteck enthält schon den Punkt O, woraus die Behauptung folgt.

Wenn nur die Projektion von A' an der y-Achse zwischen den Geraden g und BD liegt, so betrachten wir das Parallelogramm zwischen den Geraden g, BD, ferner den durch A' und durch E gehenden, zur x-Achse parallelen Geraden, und schieben die an der letzterwähnten Geraden liegende Seite entlang dieser Geraden so weg, daß das Parallelogramm in ein Rechteck übergeht. Dieses enthält den Punkt O, der Satz III gilt also auch in diesem Falle.

Man kann aus dem Beweis wieder ablesen, daß das Gleichheitszeichen nur dann nicht weggelassen werden kann, wenn an einer der Achsen unendlich viele Gitterpunkte liegen und die nächste durch Gitterpunkte gehende parallele Gerade, die den ersten Quadranten durchschneidet, die andere Achse in einem Gitterpunkt schneidet.

7. Entsprechend dem Satz IV betrachten wir nun homogene lineare Formen und einen homogenen Gitter. Bei den Vereinbarungen des Abschnitts 2 gibt es dabei auch zerteilte Parallelogramme. Da aber der Punkt O in jedem zerteilten Parallelogramm enthalten ist, ist er hier der zum vierten Quadranten gehörige Eckpunkt jedes zerteilten Parallelogramms. Die zum ersten, zweiten und dritten Quadranten gehörigen Ecken seien P_1, P_2, P_3. Wenn der erste und der dritte die Koordinaten x_1, y_1, bzw. $-x_3, -y_3$ haben, sind die Koordinaten des zweiten $x_2 = -(x_3 - x_1)$, $y_2 = (y_1 - y_3)$. Ich wende noch die Bezeichnungen $m_i = |x_i y_i|$ $(i = 1, 2, 3)$ und $m = \min(m_1, m_2, m_3)$ an. Dann ist

$$m_2 = (x_3 - x_1)(y_1 - y_3) = x_1 y_3 + x_3 y_1 - m_1 - m_3. \tag{3}$$

Man kann andererseits Δ als der doppelte Inhalt des Dreiecks OP_1P_3 folgendermaßen mit den Koordinaten ausdrücken:

$$\Delta = x_3 y_1 - x_1 y_3. \tag{4}$$

Aus den beiden Gleichungen erhält man nach Quadrierung des letzteren

$$\Delta^2 = (x_3 y_1 + x_1 y_3)^2 - 4 x_1 y_1 x_3 y_3 = (m_1 + m_2 + m_3)^2 - 4 m_1 m_3 =$$
$$= (m_1 - m_3)^2 + m_2(2m_1 + m_2 + 2m_3) \geqq 5m^2.$$

Es gilt also

$$m = \min(|x_1 y_1|, |x_2 y_2|, |x_3 y_3|) \leqq \frac{\Delta}{\sqrt{5}},$$

womit auch Satz IV bewiesen wurde. Man sieht gleich, daß das Gleichheits-

zeichen nur im Falle $m_1 = m_2 = m_3 = m = \Delta/\sqrt{5}$ nicht weggelassen werden kann. An Hand der Gleichungen (3), (4) kann man einsehen, daß in diesem Falle die Koordinaten der Gitterpunkte in folgender Form dargestellt werden können:

$$x = x_1\left(u + \frac{\sqrt{5}+1}{2}v\right); \quad y = y_1\left(u - \frac{\sqrt{5}-1}{2}v\right) \qquad (\Delta = \sqrt{5}\,|x_1 y_1|).$$

Literatur

[1] H. Davenport—H. Heilbronn, Assymmetric inequalities for nonhomogeneous linear forms, *Journal London Math. Soc.*, **22** (1947), 53—61.

[2] Б. Н. Делоне, Алгорифм разделенных параллелограммов, Известия Академии Наук СССР, Сер. мат., **11** (1947), 505—538. Deutsche Übersetzung in *Sowjetwissenschaft*, **2** (1948), 178—210.

[3] A. Korkine—G. Zolotareff, Sur les formes quadratiques, *Math. Annalen*, **6** (1873), 366—389.

[4] H. Minkowski, Über die Annäherung an eine reelle Größe durch rationale Zahlen, *Math. Annalen*, **54** (1901), 91—124.

[5] L. Rédei, Neuer Beweis eines Satzes von Delone über ebene Punktgitter, *Journal London Math. Soc.*, **34** (1959), 205—207. (Hier sind auch weitere Literaturangaben zu finden.)

[6] D. B. Sawyer, The product of two non-homogeneous linear forms, *Journal London Math. Soc.*, **23** (1949), 250—251.

(Eingegangen am 3. Mai 1960)

Über die Einbettung von Ringen in Oberringe mit Einselement

Von HANNS JOACHIM WEINERT in Potsdam (Deutschland)

Herrn Prof. Dr. Ladislaus Rédei verehrungsvoll gewidmet

Einleitung

Bekanntlich läßt sich mit Hilfe des Ringes Γ der ganzen Zahlen zu jedem Ring $\mathfrak{R}$ ein Oberring $\mathfrak{R}^* = \langle \Gamma, \mathfrak{R} \rangle$ mit Einselement konstruieren, indem man in der Produktmenge $\Gamma \times \mathfrak{R}$ die Rechenoperationen

$$(\gamma, r) + (\delta, s) = (\gamma + \delta, r + s),$$
$$(\gamma, r) \cdot (\delta, s) = (\gamma \cdot \delta, \gamma s + \delta r + r \cdot s)$$

definiert und jeweils $r \in \mathfrak{R}$ mit $(0, r)$ sowie $\gamma \in \Gamma$ mit (γ, o) identifiziert. Hat der Ring $\mathfrak{R}$ die Charakteristik $\nu \neq 0$, so kann man dabei Γ durch den Restklassenring $\Gamma/(\nu)$ ersetzen und erhält einen Oberring $\mathfrak{R}_\nu^* = \langle \Gamma/(\nu), \mathfrak{R} \rangle$ der gleichen Charakteristik ν (vgl. etwa [1], S. 22). Allerdings ist damit für das eigentliche Ziel solcher Einbettungen, nämlich Untersuchungen über Ringe ohne Einselement auf solche mit Einselement zurückzuführen, meist nicht sehr viel gewonnen. So lehrt schon die Betrachtung einfacher Beispiele, daß ein solcher Oberring von $\mathfrak{R}$ im allgemeinen ganz andere Eigenschaften hat und (abgesehen von der Existenz eines Einselementes) viel unbequemer ist als $\mathfrak{R}$ selbst, und daß es andererseits zu $\mathfrak{R}$ Oberringe mit Einselement geben kann, deren Struktur der von $\mathfrak{R}$ weit mehr entspricht. Damit ergeben sich im wesentlichen die drei folgenden, natürlich weitgehend zusammenhängenden Aufgabenstellungen:

I) Einen Überblick über alle möglichen Oberringe von $\mathfrak{R}$ zu gewinnen, die ein Einselement enthalten.

Zweckmäßiger Weise konzentriert man sich dabei auf solche Ringe, die von ihrem Einselement e und den Elementen aus $\mathfrak{R}$ erzeugt werden, deren Elemente also in der Form

$$\gamma e + r \quad \text{mit} \quad \gamma \in \Gamma, \; r \in \mathfrak{R}$$

geschrieben werden können. Der Kürze halber wollen wir sie *Einselementoberringe* von $\mathfrak{R}$ nennen. Insbesondere ist jeder minimale Oberring mit Eins-

element (also ein Ring, der $\mathfrak{R}$ und ein Einselement, aber keinen echten Unterring dieser Art enthält) ein solcher Einselementoberring, aber nicht umgekehrt.

II) Bestimmte Einselementoberringe von $\mathfrak{R}$ zu betrachten, deren Struktur der des Ausgangsringes so weit als möglich angepaßt ist, und diese Ringe unter allen anderen bzw. durch besondere Eigenschaften auszuzeichnen.

III) Zu untersuchen, welche Eigenschaften sich jeweils von den unter I) oder II) behandelten Ringen auf $\mathfrak{R}$ bzw. umgekehrt übertragen.

Die Lösung der ersten Fragestellung wurde von B. BROWN und N. MCCOY in [3] gegeben, die „vollständige Mengen von Erweiterungen von $\mathfrak{R}$" betrachten und gewisse Eigenschaften dieser Systeme untersuchen. Eine solche Menge $\mathfrak{S}$ besteht dabei aus Oberringen von $\mathfrak{R}$ mit Einselement, derart daß jeder andere Ring dieser Art einen Unterring enthält, der zu einem Ring aus $\mathfrak{S}$ (relativ bezüglich $\mathfrak{R}$) isomorph ist. Mit Hilfe der für die vorliegende Arbeit benötigten Begriffsbildungen können wir ihrem grundlegenden Resultat ([3], Theorem 2) die folgende Wendung geben: Jeder Einselementoberring $\mathfrak{S}$ von $\mathfrak{R}$ ist Bild von $\mathfrak{R}^*$ bei einem bezüglich $\mathfrak{R}$ relativen Homomorphismus[1]), dessen Kern aus allen ganzzahligen Vielfachen eines Elementes $a - a \in \mathfrak{R}^*$ besteht, wobei $a \cdot r = r \cdot a = ar$ für alle $r \in \mathfrak{R}$ erfüllt ist, und umgekehrt. Einen entsprechenden Beweis, der sich für den so formulierten Satz ohne weitere Vorbereitungen leicht führen läßt, geben wir zusammen mit einigen Erläuterungen in § 1.

Die zweite Fragestellung wurde bisher nur für nullteilerfreie Ringe von J. SZENDREI ([7], vgl. auch [5], § 85) bzw. für Boolesche Ringe von M. H. STONE [6] gelöst. Diese Autoren zeigen, daß es zu jedem nullteilerfreien bzw. Booleschen Ring $\mathfrak{R}$ einen ebensolchen minimalen Oberring $\mathfrak{R}'$ mit Einselement gibt, und daß $\mathfrak{R}'$ jeweils durch diese drei Forderungen bis auf Isomorphie (relativ bezüglich $\mathfrak{R}$) eindeutig bestimmt ist. Nun kann man sich leicht überlegen, daß in beiden Fällen dieser Oberring $\mathfrak{R}'$ unter allen Einselementoberringen von $\mathfrak{R}$ auch dadurch ausgezeichnet werden kann, daß er sich nicht mehr echt homomorph relativ bezüglich $\mathfrak{R}$ auf einen anderen Einselementoberring von $\mathfrak{R}$ abbilden läßt[2]). Diese Forderung ist aber von speziellen Eigenschaften von $\mathfrak{R}$ unabhängig, und in der Tat werden sich ganz allgemein die ihr genügenden Einselementoberringe von $\mathfrak{R}$ — wir wollen sie kurz *strenge Einselementoberringe* von $\mathfrak{R}$ nennen — als die im Sinne von II) strukturell einfachsten Oberringe von $\mathfrak{R}$ mit Einselement herausstellen. Dabei kann insbesondere die sicher

[1]) Ein bezüglich $\mathfrak{R}$ relativer Homomorphismus eines Oberringes von $\mathfrak{R}$ auf einen ebensolchen Ring soll für die Teilmenge $\mathfrak{R}$ die identische Abbildung induzieren.

[2]) Bei uns wird sich dies, wie auch die Aussagen von SZENDREI und STONE selbst, aus allgemeineren Überlegungen ergeben.

naheliegende Forderung der Minimalität entfallen, da wir zeigen werden (§2, (6)), daß ein strenger Einselementoberring von $\mathfrak{R}$ stets minimal ist.

Weiterhin erhalten wir in §2 nach einigen vorbereitenden Überlegungen (erwähnt sei nur ein idealtheoretisches Durchschnittskriterium (3) für strenge Einselementoberringe), daß es in den wichtigsten Fällen zu einem Ring $\mathfrak{R}$ bis auf relative Isomorphie bezüglich $\mathfrak{R}$ nur einen strengen Einselementoberring $\mathfrak{R}'$ gibt, nämlich dann, wenn der Annullator $\mathfrak{N}$ von $\mathfrak{R}$ nur aus dem Nullelement besteht. Für $\mathfrak{N} \neq (o)$ existieren dagegen (von einem trivialen Fall abgesehen) stets mehrere strenge Einselementoberringe von $\mathfrak{R}$, die nicht relativ bezüglich $\mathfrak{R}$ isomorph sind, sodaß sich im allgemeinen kein bestimmter Ring im Sinne von II) mehr auszeichnen läßt.

Für den Fall $\mathfrak{N} = (o)$, den wir in §3 im Hinblick auf die dritte Fragestellung näher untersuchen, können weitere Kriterien (u. a. die Nullteilerfreiheit) dafür angegeben werden, daß ein Einselementoberring $\mathfrak{S}$ von $\mathfrak{R}$ bereits die Struktur des strengen Einselementoberringes $\mathfrak{R}'$ von $\mathfrak{R}$ hat. Ferner ist mit $\mathfrak{R}$ auch $\mathfrak{R}'$ nullteilerfrei und damit also der einzige Einselementoberring von $\mathfrak{R}$ mit dieser Eigenschaft, womit der Satz von SZENDREI in unsere Untersuchungen einbezogen ist. Allgemeiner stellt sich heraus, daß jedes links- bzw. rechtsreguläre Element von $\mathfrak{R}$ diese Eigenschaft beim Übergang zu $\mathfrak{R}'$ behält, wenn nur der Links- bzw. Rechtsannullator von $\mathfrak{R}$ nur aus dem Nullelement besteht. Damit können die Zusammenhänge von $\mathfrak{R}$ und $\mathfrak{R}'$ bei der Quotientenbildung untersucht werden, und man erhält: Jeder Links- bzw. Rechtsquotientenring $\mathfrak{Q}(\mathfrak{R}, \mathfrak{T})$[3]) von $\mathfrak{R}$ stimmt mit einem ebensolchen Quotientenring $\mathfrak{Q}(\mathfrak{R}', \mathfrak{T}')$ von $\mathfrak{R}'$ überein; weiterhin ist $\mathfrak{R}'$ in jedem Quotientenring von $\mathfrak{R}$ und zwar stets echt enthalten. Wir bemerken noch, daß bei derartigen Überlegungen $\mathfrak{N} = (o)$ ohnehin erfüllt sein muß, also keine echte Einschränkung der Allgemeinheit bedeutet.

Die Untersuchung idealtheoretischer Zusammenhänge in §4 wird dagegen ohne die Voraussetzung $\mathfrak{N} = (o)$ durchgeführt, und zwar zunächst sogar für $\mathfrak{R}$ und einen beliebigen Einselementoberring $\mathfrak{S}$ von $\mathfrak{R}$, wobei sich u. a. die gleichzeitige Gültigkeit des Oberkettensatzes für $\mathfrak{R}$ und $\mathfrak{S}$ ergibt. Für die Übertragung des eingeschränkten Unterkettensatzes muß man für $\mathfrak{S}$ aber wieder einen strengen Einselementoberring $\mathfrak{R}'$ wählen; von gewissen Ausnahmen (vgl. (14)) abgesehen, gilt dann auch dieser Satz für $\mathfrak{R}$ und $\mathfrak{R}'$ gleichzeitig. Das hat zur Folge, daß entsprechende Sätze der Idealtheorie nur für Ringe mit Einselement bewiesen zu werden brauchen und damit von selbst auch für Ringe ohne Einselement gelten. Als Beispiel hierzu sei der Satz von H. GRELL [4] genannt, nach dem sich der eingeschränkte Unterkettensatz von

[3]) Vgl. Fußnote 14 (§ 3).

einem kommutativen, nullteilerfreien Ring $\mathfrak{R}$ mit Einselement auf alle Oberringe dieser Art überträgt, deren Quotientenkörper endlich algebraisch über dem von $\mathfrak{R}$ sind.

§ 1

Jeder Einselementoberring $\mathfrak{S}$ von $\mathfrak{R}$ ist vermöge der Zuordnung

$$\gamma + r \to \gamma e + r$$

homomorphes Bild des Ringes $\mathfrak{R}^*$. Der Kern dieses bezüglich $\mathfrak{R}$ relativen Homomorphismus ist damit ein Ideal $\mathfrak{a}^*$ von $\mathfrak{R}^*$, welches $\mathfrak{a}^* \cap \mathfrak{R} = (o)$ erfüllt, und umgekehrt ist jeder Restklassenring von $\mathfrak{R}^*$ nach einem solchen Ideal $\mathfrak{a}^*$ (nach Identifizierung der Restklassen $r + \mathfrak{a}^*$ mit den Elementen $r \in \mathfrak{R}$) ein Einselementoberring von $\mathfrak{R}$. Weiterhin ist jedes Ideal $\mathfrak{a}^*$ von $\mathfrak{R}^*$ mit $\mathfrak{a}^* \cap \mathfrak{R} = (o)$ ein Hauptideal, welches aus allen ganzzahligen Vielfachen eines Elementes

$$\alpha + a' = \alpha - a \in \mathfrak{R}^*$$

besteht. In den Elementen $\gamma + r$ von $\mathfrak{a}^*$ kann nämlich jede ganze Zahl γ höchstens einmal auftreten, und alle ganzen Zahlen dieser Art bilden ein Ideal (α) von Γ. Für $\mathfrak{a}^* \neq (o)$ kann also α stets positiv gewählt werden, während $\alpha = 0$ natürlich $a = o$ impliziert. Wegen

$$\left.\begin{aligned} (\alpha - a)\cdot r &= \alpha r - a\cdot r \\ r\cdot(\alpha - a) &= \alpha r - r\cdot a \end{aligned}\right\} \in \mathfrak{a}^* \cap \mathfrak{R} = (o)$$

erfüllt dabei das Element $a \in \mathfrak{R}$

$$(*) \qquad a\cdot r = r\cdot a = \alpha r \quad \text{für alle } r \in \mathfrak{R},$$

d. h., die Multiplikation mit a wirkt auf alle Ringelemente wie die Vielfachenbildung mit der ganzen Zahl α. Gilt umgekehrt $(*)$ für ein Element $a \in \mathfrak{R}$ und eine ganze Zahl α, so erfüllt das von $\alpha - a$ erzeugte Ideal $\mathfrak{a}^* = (\alpha - a)$ von $\mathfrak{R}^*$ obige Durchschnittsbedingung, wenn nur wieder der Fall $\alpha = 0$, $a \neq o$ ausgeschlossen wird. Nennen wir noch ein solches Element a von $\mathfrak{R}$, zu dem eine ganze Zahl α gemäß $(*)$ korrespondiert, ein *α-Element von $\mathfrak{R}$* (in [3] „α-fier"), so haben wir bereits die mit Theorem 2 von [3] gleichwertige Aussage:

(1) *Die Einselementoberringe von $\mathfrak{R}$ sind (bis auf relative Isomorphie bezüglich $\mathfrak{R}$) gerade die wie oben als Oberringe von $\mathfrak{R}$ aufzufassenden Restklassenringe $\mathfrak{R}^*/(\alpha - a)$, wobei a und $\alpha \geqq 0$ auf alle möglichen Arten so zu wählen sind, daß a α-Element von $\mathfrak{R}$ ist unter Ausschluß der Fälle $\alpha = 0$, $a \neq o$.*

Ist e das Einselement von $\mathfrak{S} = \mathfrak{R}^*/(\alpha - a)$, so läuft die Restklassenbildung modulo $(\alpha - a)$ gerade darauf hinaus, in $\mathfrak{S}$ alle ganzzahligen Vielfachen $\tau\alpha e$ von αe mit den Elementen $\tau a \in \mathfrak{R}$ zu identifizieren. Wegen

$\tau a e = \tau a$ für alle $\tau \in \Gamma$ ist die Charakteristik μ von $\mathfrak{S}$ das a-fache der additiven Ordnung η_a von a, also $\mu = a\eta_a$[4]), wobei natürlich $\eta_a = 0$ für ein Element unendlicher Ordnung zu setzen ist — letzteres einfach im Einklang damit, daß man auch „Charakteristik 0" statt „Charakteristik ∞" sagt.

Weiterhin können wir jedes Element von $\mathfrak{S}$ nun sogar eindeutig als Summe der Form

$$\gamma e + r$$

schreiben, wenn wir r alle Elemente von $\mathfrak{R}$, und γ

für $a = 0$ (also $a = o$ und $\mathfrak{S} = \mathfrak{R}^*$) alle ganzen Zahlen,

für $a \geqq 2$ die Zahlen $0, 1, \ldots, a-1$

durchlaufen lassen[5]).

Alle Rechnungen können dann (unter Beachtung der Charakteristik) völlig formal vorgenommen werden, wenn man nur für $a \geqq 2$ jeweils ae durch das a-Element a von $\mathfrak{R}$ ersetzt. Selbstverständlich ist mit $\mathfrak{R}$ auch $\mathfrak{S}$ kommutativ.

Für einen gewissen Überblick über die damit existierenden Einselementoberringe von $\mathfrak{R}$ übernehmen wir aus [3] noch folgende leicht ersichtliche Aussagen über die a-Elemente von $\mathfrak{R}$, die wir zusammenfassend auch *Operatorelemente* von $\mathfrak{R}$ nennen wollen:

Alle a-Elemente von $\mathfrak{R}$ bilden einen Unterring $\mathfrak{G}$ von $\mathfrak{R}$, die korrespondierenden ganzen Zahlen[6]) ein Ideal $(\varkappa)$ von Γ, wobei $\varkappa \geqq 0$ eine Invariante von $\mathfrak{R}$ ist (in [3] „mode" genannt).

Die Gesamtheit der 0-Elemente von $\mathfrak{R}$ ist der Annullator $\mathfrak{N}$ von $\mathfrak{R}$, und die ihnen zugeordneten ganzen Zahlen sind gerade das von der Charakteristik ν von $\mathfrak{R}$ erzeugte Ideal (ν) von Γ[7]). Wegen $(\varkappa) \supseteq (\nu)$ gilt $\varkappa | \nu$.

Genau für $\mathfrak{R} = (o)$ ist das Nullelement o von $\mathfrak{R}$ das einzige 0-Element von $\mathfrak{R}$ im oben festgelegten Sinne. Entsprechend gilt: Die Gesamtheit aller a-Elemente mit festem a ist eine Restklasse der additiven Zerlegung von $\mathfrak{R}$ nach $\mathfrak{N}$, d. h., man erhält alle diese Elemente aus einem a-Element a in der Form

$$a' = a + n \quad \text{mit} \quad n \in \mathfrak{N}^{8}).$$

---

[4]) Daraus folgt auch sofort die in [3] als Hilfssatz über die a-Elemente bewiesene Aussage $\nu | a\eta_a$ für die Charakteristik ν von $\mathfrak{R}$.

[5]) Für $a = 1$ wäre das zugehörige a als „1-Element" von $\mathfrak{R}$ Einselement im üblichen Sinne und $\mathfrak{S} = \mathfrak{R}$.

[6]) Man beachte, daß bei Charakteristik ν jedes a-Element a von $\mathfrak{R}$ zugleich $(a + \tau\nu)$-Element für jedes $\tau \in \Gamma$ ist.

[7]) Wir werden diese Begriffsbildungen mitunter auch „einseitig" benötigen, also von a-Linkselementen, dem Linksannulator $\mathfrak{N}_L$ von $\mathfrak{R}$ usf. sprechen.

[8]) Dabei kann a insbesondere als das $\frac{a}{\varkappa}$-fache eines $\varkappa$-Elements k von $\mathfrak{R}$ geschrieben werden.

Damit ist $\mathfrak{S}/\mathfrak{N}$ isomorph zu dem von $\varkappa$ bzw. $[\varkappa]_\nu$ erzeugten Unterring von Γ bzw. $\Gamma/(\nu)$.

Aus

$$\varkappa(k+n)=k\cdot(k+n)=k\cdot k=\varkappa k,$$

also $\varkappa n=o$ für ein beliebiges $\varkappa$-Element k und jedes 0-Element n von $\mathfrak{N}$ folgt noch $\eta_n|\varkappa$ für die Ordnungen η_n der Elemente des Annullators $\mathfrak{N}$ von $\mathfrak{N}$.

§ 2

Aus unserer Kennzeichnung der Einselementoberringe von $\mathfrak{N}$ als relativ homomorphe Bilder von $\mathfrak{N}^*$ ergibt sich zunächst unmittelbar:

(2) *Zwischen zwei Einselementoberringen von $\mathfrak{N}$ besteht genau dann ein bezüglich $\mathfrak{N}$ relativer Homomorphismus*

$$\mathfrak{N}^*/\mathfrak{a}^* \backsimeq \mathfrak{N}^*/\mathfrak{b}^*,$$

wenn für die zugehörigen Ideale $\mathfrak{b}^*=(\beta-b)\supseteq\mathfrak{a}^*=(\alpha-a)$ gilt, es also eine ganze Zahl τ mit $\alpha=\tau\beta$, $a=\tau b$ gibt.

Die Existenz eines echten relativen Homomorphismus entspricht also der Möglichkeit, in $\mathfrak{N}^*/\mathfrak{a}^*$ weitere Identifizierungen von Operatorelementen von $\mathfrak{N}$ mit Vielfachen des Einselementes von $\mathfrak{N}^*/\mathfrak{a}^*$ vorzunehmen. Wir wenden unsere Aufmerksamkeit daher solchen Einselementoberringen $\mathfrak{N}'=\mathfrak{N}^*/\mathfrak{a}^*$ zu, die nicht mehr echt homomorph relativ bezüglich $\mathfrak{N}$ abgebildet werden können und die wir bereits in der Einleitung *strenge* Einselementoberringe von $\mathfrak{N}$ genannt haben. Sie sind nach (1) und (2) dadurch ausgezeichnet, daß das Ideal $\mathfrak{a}^*$ von $\mathfrak{N}^*$ in bezug auf die Eigenschaft $\mathfrak{a}^*\cap\mathfrak{N}=(o)$ maximal ist. Daraus ergibt sich:

(3) *Ein Einselementoberring $\mathfrak{N}'$ von $\mathfrak{N}$ ist dann und nur dann streng, wenn für jedes zweiseitige Ideal $\mathfrak{a}'$ von $\mathfrak{N}'$ gilt:*

$$\text{Aus}\quad \mathfrak{a}'\cap\mathfrak{N}=(o)\quad \text{folgt}\quad \mathfrak{a}'=(o).$$

Ist nämlich $\mathfrak{a}^*$ ein solches Ideal von $\mathfrak{N}^*$, so enthält jedes Ideal $\mathfrak{b}^*\supset\mathfrak{a}^*$ von $\mathfrak{N}^*$ ein Element $r\neq o$ aus $\mathfrak{N}$, so daß das gleiche für sein Bild $\mathfrak{b}'$ von $\mathfrak{N}'$ und damit für alle Ideale $\mathfrak{a}'\neq(o)$ von $\mathfrak{N}'$ gilt. Die Umkehrung ist klar. Insbesondere ist damit auch gezeigt, daß die Nichtexistenz eines echten Homomorphismus von $\mathfrak{N}'$, der für $\mathfrak{N}$ eine beliebige isomorphe Abbildung induziert, gleichwertig ist mit der Nichtexistenz eines echten Homomorphismus von $\mathfrak{N}'$, der für $\mathfrak{N}$ die identische Abbildung induziert.

(4) *Es gibt wenigstens einen strengen Einselementoberring $\mathfrak{N}'$ von $\mathfrak{N}$, der die gleiche Charakteristik ν wie $\mathfrak{N}$ hat.*

Das ergibt sich sofort daraus, daß der in der Einleitung erwähnte Einselementoberring $\mathfrak{N}_\nu^*=\mathfrak{N}^*/(\nu-o)$ von $\mathfrak{N}$ entweder selbst schon streng ist,

oder auf einen strengen Einselementoberring $\mathfrak{R}'$ von $\mathfrak{R}$ relativ homomorph abgebildet werden kann, wobei jedoch die Charakteristik ν erhalten bleiben muß. Allgemeiner läßt sich natürlich jeder Einselementoberring der Charakteristik ν auch als relativ homomorphes Bild von $\mathfrak{R}_\nu^*$ gewinnen, und man kann für diese Ringe alle Betrachtungen entsprechend unter Ersetzung von $\mathfrak{R}^*$ durch $\mathfrak{R}_\nu$ durchführen.

Da nach den Ausführungen in § 1 für $\mathfrak{R}=(o)$ alle Operatorelemente von $\mathfrak{R}$ gerade die ganzzahligen Vielfachen des dann eindeutig bestimmten $\varkappa$-Elementes k von $\mathfrak{R}$ sind, ist das Ideal $(\varkappa-k)$ von $\mathfrak{R}^*$ eindeutig bestimmtes Oberideal aller Ideale $\mathfrak{a}^*=(a-a)$ von $\mathfrak{R}^*$ mit $\mathfrak{a}^*\cap\mathfrak{R}=(o)$, und wir erhalten aus (2):

(5) *Besteht der Annullator eines Ringes $\mathfrak{R}$ nur aus dem Nullelement, so gibt es einen bis auf relative Isomorphie bezüglich $\mathfrak{R}$ eindeutig bestimmten strengen Einselementoberring von $\mathfrak{R}$:*

$$\mathfrak{R}'=\mathfrak{R}^*/(\varkappa-k).$$

Er ist relativ homomorphes Bild jedes Einselementoberringes von $\mathfrak{R}$, kann aber eben selbst nicht mehr echt homomorph relativ bezüglich $\mathfrak{R}$ abgebildet werden. Weiterhin hat $\mathfrak{R}'$ die gleiche Charakteristik wie $\mathfrak{R}$ und ist als Oberring von $\mathfrak{R}$ mit Einselement minimal.

Die beiden letzten Behauptungen ergeben sich sofort aus (4) und dem nachfolgenden Satz (6). Wir bemerken noch, daß für einen Booleschen Ring $\mathfrak{R}$ stets $\mathfrak{R}=(o)$ und $\varkappa=2$ gilt, und der Ring $\mathfrak{R}'=\mathfrak{R}^*/(2-o)$ Boolescher Oberring von $\mathfrak{R}$ mit Einselement ist, während alle anderen Einselementoberringe $\mathfrak{R}^*/(a-o)$ mit $a=0, 4, 6, 8, \ldots$ eine von 2 verschiedene Charakteristik haben.

Abgesehen von dem trivialen Fall $\varkappa=0$, für den $\mathfrak{R}^*$ stets der einzige Einselementoberring von $\mathfrak{R}$ ist, ist die Bedingung $\mathfrak{R}=(o)$ für Satz (5) auch notwendig[9]): Für $\mathfrak{R}=\{o, n, n', \ldots\}\neq(o)$ liefern dann nämlich schon die mit einem festen $\varkappa$-Element k gebildeten Ideale von $\mathfrak{R}^*$

$$(\varkappa-k),\ (\varkappa-(k+n)),\ (\varkappa-(k+n')),\ \ldots$$

strenge Einselementoberringe von $\mathfrak{R}$, von denen ersichtlich keine zwei relativ bezüglich $\mathfrak{R}$ isomorph sind[10]). Weitere Ideale

$$(\tau\varkappa-(\tau k+n))$$

[9]) Im Falle $\varkappa=1$ hat $\mathfrak{R}$ selbst ein Einselement, und es gilt a fortiori $\mathfrak{R}=(o)$.

[10]) Es gibt sogar Beispiele dafür, daß zwei solche strengen Einselementoberringe $\mathfrak{R}_1'$ und $\mathfrak{R}_2'$ eines geeigneten Ringes $\mathfrak{R}$ überhaupt nicht isomorph aufeinander abgebildet werden können.

dieser Art entstehen, wenn man ein $\tau\varkappa$-Element $\tau k+n$ verwendet, welches nicht das τ'-fache eines $\frac{\tau}{\tau'}\varkappa$-Elementes ist; man kann zeigen, daß dafür (unabhängig von der Wahl des $\varkappa$-Elementes k) notwendig und hinreichend ist, daß es kein $\tau' \in \Gamma$ und kein $n' \in \mathfrak{R}$ mit $\tau' | \tau$ und $n = \tau' n'$ gibt. Auch ist die Existenz solcher Ideale stets gewährleistet: Wegen $\varkappa n' = o$ für alle $n' \in \mathfrak{R}$ ist das $\varkappa^2$-Element $\varkappa k+n$ mit $n \neq o$ aus $\mathfrak{R}$ nicht $\varkappa$-faches irgendeines $\varkappa$-Elementes $k+n'$. Damit kann der Ring

$$\mathfrak{R}^*/(\varkappa^2-(\varkappa k+n))$$

gemäß (2) auf keinen der Ringe

$$\mathfrak{R}^*/(\varkappa-(k+n')),\quad n' \text{ durchläuft } \mathfrak{R}$$

relativ homomorph abgebildet werden, sodaß diese Ringe nicht alle strengen Einselementoberringe von $\mathfrak{R}$ ausmachen können.

Bevor wir die sich aus (5) ergebenden Verhältnisse näher untersuchen, wobei sich der Ring $\mathfrak{R}'$ auch als Verallgemeinerung des SZENDREIschen Ringes im nullteilerfreien Falle herausstellen wird, beweisen wir allgemein den Satz:

(6) *Jeder strenge Einselementoberring $\mathfrak{R}'$ von $\mathfrak{R}$ ist minimaler Oberring von $\mathfrak{R}$ mit Einselement*[11]).

Es sei $\mathfrak{S} = \mathfrak{R}^*/(\alpha-a)$ ein Einselementoberring von $\mathfrak{R}$ mit dem Einselement e, und $\mathfrak{S}$ enthalte einen echten Unterring $\mathfrak{S}' \supset \mathfrak{R}$ mit dem Einselement e'[12]). Wir werden zeigen, daß dann $\mathfrak{S}$ ein Ideal $(\beta e-b) \neq (o)$ mit $(\beta e-b) \cap \mathfrak{R} = (o)$ besitzt, also nicht streng ist. Als Element von $\mathfrak{S}$ läßt sich e' eindeutig in der Form $e' = \delta e + r_0$ mit $1 < \delta < \alpha$ schreiben, wobei $-r_0 = \delta e - e'$ ein $(\delta-1)$-Element von $\mathfrak{R}$ ist. Wir betrachten alle ganzen Zahlen γ mit $\gamma e' \in \mathfrak{R}$. Diese bilden ein Ideal (β) von Γ, welches ersichtlich α, wegen $e' \notin \mathfrak{R}$ aber nicht 1 enthält. Dann gilt $\beta | \alpha$, und

$$\beta e' = \beta\delta e + \beta r_0 \in \mathfrak{R}$$

ist ein β-Element b von $\mathfrak{R}$; aus $\beta\delta e \in \mathfrak{R}$ folgt außerdem noch $\beta\delta = \tau\alpha$ und $\beta\delta e = \tau a$. Das Ideal $(\beta e-b)$ von $\mathfrak{S}$ enthält also nur ganzzahlige Vielfache

[11]) Einfache Gegenbeispiele (für nicht strenge Einselementoberringe) lassen sich leicht bilden: Ist etwa $\mathfrak{R}$ ein Ring mit der Charakteristik 4 und mit $\varkappa=0$ oder $\varkappa=2$, so enthält der Einselementoberring $\mathfrak{R}^*/(12-o) = \{\gamma e + r\}$ echt den von $e'=9e$ und $\mathfrak{R}$ erzeugten Einselementoberring von $\mathfrak{R}$ mit dem Einselement e', der natürlich zu $\mathfrak{R}^*/(4-o)$ relativ isomorph ist.

[12]) Den Fall, daß $\mathfrak{R}$ schon ein Einselement enthält und damit selbst der einzige strenge Einselementoberring von $\mathfrak{R}$ ist, dürfen wir von vorn herein ausschliessen.

von $\beta e - b$, und $\gamma(\beta e - b) \in \mathfrak{N}$ kann nur für solche $\gamma \in \Gamma$ eintreten, die $\gamma\beta = \sigma\alpha$ erfüllen. Wir zeigen, daß dann stets

$$\gamma(\beta e - b) = \gamma(\beta e - \beta e') = \sigma\alpha e - \sigma\alpha e' = o$$

gilt, indem wir $\alpha e' = a = \alpha e$ beweisen. Dazu schreiben wir das $(\delta - 1)$-Element $-r_0$ von $\mathfrak{N}$ mit Hilfe eines $\varkappa$-Elementes k von $\mathfrak{N}$ in der Form

$$-r_0 = \frac{\delta - 1}{\varkappa} k + n_0 \quad \text{mit} \quad n_0 \in \mathfrak{N},$$

und das α-Element a von $\mathfrak{N}$ entsprechend

$$a = \frac{\alpha}{\varkappa} k + n_1 \quad \text{mit} \quad n_1 \in \mathfrak{N}.$$

Da die Ordnung jedes Elementes aus $\mathfrak{N}$ ein Teiler von $\varkappa$ ist, gilt $\beta n_0 = o$ wegen $\varkappa | \beta$ und $(\delta - 1) n_1 = o$ wegen $\varkappa | \delta - 1$, sodaß unter weiterer Beachtung von $\beta\delta = \tau\alpha$ folgt:

$$\alpha e' = \frac{\alpha}{\beta}(\beta e') = \frac{\alpha}{\beta}(\beta\delta e + \beta r_0) = \frac{\alpha}{\beta}\left(\tau\frac{\alpha}{\varkappa} k + \tau n_1 - \beta\frac{\delta - 1}{\varkappa} k - \beta n_0\right) =$$

$$= \frac{\alpha}{\beta}\left(\frac{\beta}{\varkappa} k + \tau n_1\right) = \frac{\alpha}{\varkappa} k + \delta n_1 = \frac{\alpha}{\varkappa} k + n_1 = a.$$

§ 3

In diesem Paragraphen betrachten wir den wichtigen Fall, daß der Annullator $\mathfrak{N}$ von $\mathfrak{N}$ nur aus dem Nullelement besteht. Dann gestattet es die Begriffsbildung des relativen Homomorphismus, gemäß (5) genau einen Einselementoberring $\mathfrak{N}'$ von $\mathfrak{N}$ (natürlich bis auf relative Isomorphie bezüglich $\mathfrak{N}$) als strengen Einselementoberring auszuzeichnen. $\mathfrak{N}'$ ist dann der einzige Einselementoberring von $\mathfrak{N}$, in dem jedes γ-Element c von $\mathfrak{N}$ mit allen entsprechenden Vielfachen $(\gamma + \tau\nu)e$ des Einselementes von $\mathfrak{N}'$ identifiziert ist. Da andernfalls ein γ_0-Element c_0 mit $\gamma_0 e - c_0 \neq o$ existieren würde, welches alle Elemente $r \in \mathfrak{N}$ annulliert, erhalten wir:

(7) *Hinreichend dafür, daß ein Einselementoberring $\mathfrak{S}$ von $\mathfrak{N}$ (bis auf relative Isomorphie bezüglich $\mathfrak{N}$) mit dem strengen Einselementoberring $\mathfrak{N}'$ von $\mathfrak{N}$ überstimmt, ist die Existenz eines Elementes $r_0 \neq o$ aus $\mathfrak{N}$, welches von keinem Element aus $\mathfrak{S} \setminus \mathfrak{N}$ annulliert wird — erst recht also die Nullteilerfreiheit von $\mathfrak{S}$.*

Beispiel. In dem Ring $\mathfrak{R}=\begin{pmatrix}P&0\\P&0\end{pmatrix}$ aller Matrizen $\begin{pmatrix}r_1&0\\r_2&0\end{pmatrix}$ mit Elementen r_i aus dem Körper P der rationalen Zahlen ist das Nullelement $o=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ das einzige (zweiseitige!) Operatorelement. Es gilt also $\mathfrak{R}=(o)$ und $z=0$, und der strenge Einselementoberring $\mathfrak{R}'$ von $\mathfrak{R}$ hat die Struktur $\mathfrak{R}'=\mathfrak{R}^*=\left\langle \Gamma,\begin{pmatrix}P&0\\P&0\end{pmatrix}\right\rangle$. Andererseits ist $\mathfrak{S}=\begin{pmatrix}P&0\\P\Gamma&\end{pmatrix}\subset\mathfrak{M}_2(P)$ Einselementoberring von $\mathfrak{R}$, und das Element $r_0=\begin{pmatrix}0&0\\1&0\end{pmatrix}$ wird von keinem Element aus $\mathfrak{S}\setminus\mathfrak{R}$ annulliert. Es müssen also $\mathfrak{R}'$ und $\mathfrak{S}$ relativ isomorph bezüglich $\mathfrak{R}$ sein, und in der Tat vermittelt die Zuordnung

$$(\gamma,r)=\left(\gamma,\begin{pmatrix}r_1&0\\r_2&0\end{pmatrix}\right)\to\begin{pmatrix}r_1+\gamma&0\\r_2&\gamma\end{pmatrix}$$

den (einzig möglichen) Isomorphismus dieser Art.

Die letzte Bemerkung in (7) ist bereits die Eindeutigkeitsaussage des Satzes von SZENDREI. Die Existenzaussage entspricht dem folgenden Satz:

(8) *Mit $\mathfrak{R}$ ist auch $\mathfrak{R}'$ nullteilerfrei.*

Aus $(\gamma e+r)(\delta e+s)=o$ folgt nämlich mit beliebigen x und y aus $\mathfrak{R}$

$$x(\gamma e+r)(\delta e+s)y=(\gamma x+xr)(\delta y+sy)=o$$

das Verschwinden eines Produktes von Elementen aus $\mathfrak{R}$. Ist nun etwa $\delta y_0+sy_0\neq o$ für ein festes $y_0\in\mathfrak{R}$, so gilt

$$\gamma x+xr=o,\quad \text{d.h.}\quad x(-r)=\gamma x\quad \text{für alle}\quad x\in\mathfrak{R}.$$

Also ist $-r$ γ-Rechtselement von $\mathfrak{R}$. Wegen der Nullteilerfreiheit[13]) von $\mathfrak{R}$ ist $-r$ dann auch γ-Linkselement von $\mathfrak{R}$, woraus sich nach der eben hervorgehobenen Eigenschaft von $\mathfrak{R}'$ $\gamma e=-r$, also $\gamma e+r=o$ ergibt. Entsprechend schließt man, wenn $\delta y+sy=o$ für alle $y\in\mathfrak{R}$ gilt.

Ein ähnlicher Schluß lehrt:

(9) *Ein Element $s\in\mathfrak{R}$, welches in $\mathfrak{R}$ nicht rechter (linker) Nullteiler ist, hat jedenfalls dann die gleiche Eigenschaft in $\mathfrak{R}'$, wenn der Rechtsannullator $\mathfrak{R}_R$ (Linksannullator $\mathfrak{R}_L$) von $\mathfrak{R}$ gleich (o) ist.*

[13]) Es gilt nämlich sogar bereits: Ist der Rechtsannullator $\mathfrak{R}_R$ von $\mathfrak{R}$ gleich (o), so ist jedes γ-Rechtselement c von $\mathfrak{R}$ auch γ-Linkselement (und entsprechend für γ-Linkselemente mit $\mathfrak{R}_L=(o)$). Aus $xc=\gamma x$ für alle $x\in\mathfrak{R}$ folgt nämlich für alle $z\in\mathfrak{R}$

$$z(cx-\gamma z)=\gamma zx-\gamma zx=o,\quad \text{also}\quad cx-\gamma x=o.$$

Wir gehen wieder von $(\gamma e+r)s=o$ zu

$$x(\gamma e+r)s=(\gamma x+xr)s=o \quad \text{für alle} \quad x\in\mathfrak{R}$$

über und erhalten auf Grund unserer Voraussetzung über $\mathfrak{R}_R$ wie eben $\gamma e+r=o$.

Insbesondere behalten also Elemente, die in $\mathfrak{R}$ regulär (d. h. weder linke noch rechte Nullteiler) sind, diese Eigenschaft beim Übergang zu $\mathfrak{R}'$, da ja die Existenz eines solchen Elementes bereits $\mathfrak{R}_L=\mathfrak{R}_R=\mathfrak{R}=(o)$ nach sich zieht. Darauf aufbauend können wir die Zusammenhänge zwischen $\mathfrak{R}$ und $\mathfrak{R}'$ und den aus ihnen durch Quotientenbildung entstehenden Ringen klären, wobei wir alle Aussagen für Linksquotientenringe[14]) formulieren.

Vorbereitend dazu stellen wir fest: Ist $\mathfrak{T}$ eine geeignete Halbgruppe von $\mathfrak{R}$, d. h. existieren zu $\varrho\in\mathfrak{T}$, $r\in\mathfrak{R}$ stets $\sigma\in\mathfrak{T}$, $s\in\mathfrak{R}$ mit $s\varrho=\sigma r$[15]), so ist $\mathfrak{T}$ auch geeignete Halbgruppe von $\mathfrak{R}'$; sind nämlich $\varrho\in\mathfrak{T}$, $r'\in\mathfrak{R}'$ vorgegeben, so ist $\varrho^2\in\mathfrak{T}$, $\varrho r'\in\mathfrak{R}$, und es gilt

$$s(\varrho^2)=\sigma(\varrho r'), \quad \text{also} \quad (s\varrho)\varrho=(\sigma\varrho)r' \quad \text{mit} \quad \sigma\varrho\in\mathfrak{T},\ s\varrho\in\mathfrak{R}.$$

Ist umgekehrt $\mathfrak{T}'$ eine geeignete Halbgruppe von $\mathfrak{R}'$ und $\mathfrak{T}'\cap\mathfrak{R}$ nicht leer, so ist $\mathfrak{T}=\mathfrak{T}'\cap\mathfrak{R}$ geeignete Halbgruppe von $\mathfrak{R}$; denn zu $\varrho\in\mathfrak{T}$, $r\in\mathfrak{R}$ existieren dann $\sigma'\in\mathfrak{T}'$, $s'\in\mathfrak{R}'$ mit

$$s'\varrho=\sigma' r, \quad \text{woraus} \quad (\varrho s')\varrho=(\varrho\sigma')r$$

mit $\varrho s'\in\mathfrak{R}$ und $\varrho\sigma'\in\mathfrak{T}'\cap\mathfrak{R}=\mathfrak{T}$ folgt.

(10) *Jeder Linksquotientenring $\mathfrak{Q}(\mathfrak{R},\mathfrak{T})$ von $\mathfrak{R}$ stimmt mit dem Linksquotientenring $\mathfrak{Q}(\mathfrak{R}',\mathfrak{T})$ von $\mathfrak{R}'$ und darüber hinaus mit allen Linksquotientenringen $\mathfrak{Q}(\mathfrak{R}',\mathfrak{T}')$, $\mathfrak{T}'\cap\mathfrak{R}=\mathfrak{T}$ überein, und es gilt*

$$\mathfrak{Q}(\mathfrak{R},\mathfrak{T})=\mathfrak{Q}(\mathfrak{R}',\mathfrak{T}')\supset\mathfrak{R}'.$$

Insbesondere kann also $\mathfrak{R}'$ nicht als Quotientenring von $\mathfrak{R}$ gewonnen werden.

Offensichtlich gilt nämlich $\mathfrak{Q}(\mathfrak{R}',\mathfrak{T}')\supseteq\mathfrak{Q}(\mathfrak{R},\mathfrak{T})$; es kann aber auch umgekehrt jedes Element $\varrho'^{-1}r'\in\mathfrak{Q}(\mathfrak{R}',\mathfrak{T}')$ als Element von $\mathfrak{Q}(\mathfrak{R},\mathfrak{T})$ geschrieben werden. Ist nämlich $\varrho\in\mathfrak{T}$, so erst recht $\varrho\in\mathfrak{T}'$, und es gilt

$$\varrho'^{-1}r'=\varrho'^{-1}(\varrho^{-1}\varrho)r'=(\varrho\varrho')^{-1}(\varrho r')$$

---

[14]) Ist $\mathfrak{o}$ ein beliebiger Ring, $\mathfrak{m}$ eine Halbgruppe regulärer Elemente aus $\mathfrak{o}$, so bezeichne $\mathfrak{Q}(\mathfrak{o},\mathfrak{m})$ einen Oberring von $\mathfrak{o}$ mit Einselement, in dem jedes $a\in\mathfrak{m}$ invertierbar ist und dessen Elemente in der Form $a^{-1}a$ mit $a\in\mathfrak{m}$, $a\in\mathfrak{o}$ geschrieben werden können. Nach [2] existiert ein solcher Linksquotientenring $\mathfrak{Q}(\mathfrak{o},\mathfrak{m})$ genau dann, wenn zu je zwei Elementen $a\in\mathfrak{m}$, $a\in\mathfrak{o}$ zwei Elemente $\sigma\in\mathfrak{m}$, $s\in\mathfrak{o}$ existieren, die $sa=\sigma a$ erfüllen (im folgenden werden wir solche Halbgruppen $\mathfrak{m}$ kurz „geeignet" nennen); $\mathfrak{Q}(\mathfrak{o},\mathfrak{m})$ ist dann bis auf Isomorphie eindeutig bestimmt.

[15]) Für den Rest das Paragraphen bezeichnen $\varrho,\varrho',\sigma,\sigma'$ ausnahmsweise keine ganzen Zahlen, sondern Elemente aus geeigneten Halbgruppen $\mathfrak{T}$ von $\mathfrak{R}$ bzw. $\mathfrak{T}'$ von $\mathfrak{R}'$.

mit $\varrho\varrho' \in \mathfrak{T}' \cap \mathfrak{R} = \mathfrak{T}$, $\varrho r' \in \mathfrak{R}$. Der Rest der Behauptung ergibt sich einfach daraus, daß kein reguläres Element ϱ von $\mathfrak{R}$ in $\mathfrak{R}'$ invertierbar ist, denn aus $(\gamma e + r)\varrho = e$ folgte ja $\gamma\varrho + r\varrho = e \in \mathfrak{R}$.

Bildet insbesondere die Gesamtheit aller regulären Elemente von $\mathfrak{R}$ eine geeignete Halbgruppe, so lehren unsere Überlegungen die Übereinstimmung der maximalen Linksquotientenringe von $\mathfrak{R}$ und $\mathfrak{R}'$, im nullteilerfreien Falle also der Linksquotientenkörper.

§ 4

Wir wenden uns nunmehr einigen Aussagen über die Ideale in einem Ring $\mathfrak{R}$ ohne Einselement zu, wobei wir insbesondere auf Zusammenhänge mit Eigenschaften der Ideale in einem (festen, aber zunächst beliebigen) Einselementoberring $\mathfrak{S} = \mathfrak{R}^*/(\alpha - a)$ von $\mathfrak{R}$ abzielen. Dabei gelten die hier für Linksideale formulierten Überlegungen ebenso für zweiseitige Ideale.

Zunächst bestimmt jedes Linksideal $\mathfrak{L} \neq (o)$ von $\mathfrak{S}$ ein Verengungsideal $\mathfrak{l} = \mathfrak{L} \cap \mathfrak{R}$ von $\mathfrak{R}$, während umgekehrt für jedes Linksideal $\mathfrak{l}$ von $\mathfrak{R}$ stets $\mathfrak{S}\mathfrak{l} = \mathfrak{l}$ gilt. Insbesondere ist eine Basis von $\mathfrak{l}$ als Ideal von $\mathfrak{R}$ zugleich eine Basis von $\mathfrak{l}$ als Ideal von $\mathfrak{S}$ und umgekehrt[16]).

Als nächstes untersuchen wir alle Linksideale von $\mathfrak{S}$ mit dem gleichen Verengungsideal $\mathfrak{l}$. Ist $\mathfrak{L} \supset \mathfrak{l}$ ein solches Ideal und λ die kleinste positive ganze Zahl, die in den Elementen $\gamma e + r \in \mathfrak{L}$, etwa in $\lambda e + r_0 \in \mathfrak{L}$, auftritt, so gilt:

$$(*) \qquad \mathfrak{L} = \Gamma(\lambda e + r_0) + \mathfrak{l}.$$

Für jedes $\gamma e + r \in \mathfrak{L}$ ist nämlich die Zahl γ ersichtlich ein Vielfaches $\tau\lambda$ von λ (für $\alpha \geqq 2$ beachte man $\lambda | \alpha$), und unsere Behauptung folgt aus

$$(\gamma e + r) - \tau(\lambda e + r_0) = r - \tau r_0 \in \mathfrak{L} \cap \mathfrak{R} = \mathfrak{l}.$$

Jedes Oberideal $\mathfrak{L}$ von $\mathfrak{l}$ mit $\mathfrak{L} \cap \mathfrak{R} = \mathfrak{l}$ ist also durch die nichtnegative ganze Zahl λ[17]) und die durch r_0 bestimmte Restklasse von $\mathfrak{R}$ nach $\mathfrak{l}$ gekennzeichnet. Die Gesamtheit seiner Elemente kann in der Form

$$\{\tau\lambda e + x_\tau\} \quad \text{mit} \quad \begin{cases} \tau \in \Gamma & \text{für} \quad \alpha = 0 \\ 0 \leqq \tau < \dfrac{\alpha}{\lambda} & \text{für} \quad \alpha \geqq 2 \end{cases}, \; x_\tau \in \tau r_0 + \mathfrak{l}$$

angegeben werden, wobei x_τ jeweils alle Elemente der von τr_0 bestimmten Restklasse modulo $\mathfrak{l}$ durchläuft. Diese Überlegungen führen uns zu dem Hilfssatz:

---

[16]) Allgemein kann man die Ideale von $\mathfrak{R}$ als $\mathfrak{S}$-Moduln bzw. einheitlich als $\mathfrak{R}^*$-Moduln auffassen.

[17]) Offenbar ist $\lambda = 0$ gleichwertig mit $\mathfrak{L} = \mathfrak{l}$.

(11) *Sind* $\mathfrak{L}_1$ *und* $\mathfrak{L}_2$ *zwei Linksideale von* $\mathfrak{S}$ *mit den Verengungsidealen* $\mathfrak{l}_1$ *und* $\mathfrak{l}_2$ *und den zugehörigen ganzen Zahlen* λ_1 *und* λ_2, *so folgt aus* $\mathfrak{L}_1 \supseteq \mathfrak{L}_2$ *stets*

$$\mathfrak{l}_1 \supseteq \mathfrak{l}_2 \quad \textit{und} \quad \lambda_1 | \lambda_2,$$

wobei genau für $\mathfrak{l}_1 = \mathfrak{l}_2$ *und* $\lambda_1 = \lambda_2 = \lambda$ *sogar* $\mathfrak{L}_1 = \mathfrak{L}_2$ *gilt.*

Es ist alles unmittelbar ersichtlich bis auf die letzte Behauptung. Zu ihrem Beweis verwenden wir die eben angegebenen Darstellungen

$$\mathfrak{L}_1 = \{\tau\lambda e + x_\tau\} \supseteq \{\sigma\lambda e + y_\sigma\} = \mathfrak{L}_2$$

mit $x_\tau \in \tau r_0 + \mathfrak{l}$ und entsprechend $y_\sigma \in \sigma s_0 + \mathfrak{l}$. Nun muß für jedes σ das Element $\sigma\lambda e + \sigma s_0$ gleich einem der Elemente $\tau\lambda e + x_\tau$ sein, was unter Beachtung der eindeutigen Schreibweise der Elemente von $\mathfrak{S}$ nur für $\tau = \sigma$ möglich ist, woraus $\sigma s_0 \in \sigma r_0 + \mathfrak{l}$ folgt. Dann gilt aber $\sigma r_0 + \mathfrak{l} = \sigma s_0 + \mathfrak{l}$ für jedes σ, folglich auch $\mathfrak{L}_1 = \mathfrak{L}_2$.

Die Aussage (11) bzw. die ihr zu Grunde liegende Beziehung (*) für die Ideale von $\mathfrak{S}$ ergeben nun eine verhältnismäßig weitgehende Entsprechung zwischen den idealtheoretischen Gesetzmäßigkeiten in $\mathfrak{R}$ und $\mathfrak{S}$. Insbesondere erhält man sofort:

(12) *Gilt in* $\mathfrak{R}$ *der Oberkettensatz für Linksideale, so auch in* $\mathfrak{S}$, *und umgekehrt.*

Auch der eingeschränkte Unterkettensatz gilt natürlich in $\mathfrak{R}$, wenn er in $\mathfrak{S}$ erfüllt ist; dagegen ist seine Übertragung von $\mathfrak{R}$ auf $\mathfrak{S}$ überhaupt nur diskutierbar, wenn wir $\mathfrak{S} = \mathfrak{R}' = \mathfrak{R}^*/(a - a)$ nun wirklich als strengen Einselementoberring von $\mathfrak{R}$ voraussetzen. Ist nämlich

$$\mathfrak{L}_1 \supset \mathfrak{L}_2 \supset \cdots \supseteq \mathfrak{A} \neq (o)$$

eine Unterkette, die in $\mathfrak{S}$ auf das zweiseitige Ideal $\mathfrak{A}$ zuläuft[18]), so entspricht ihr die Kette der Verengungsideale

$$\mathfrak{l}_1 \supseteq \mathfrak{l}_2 \supseteq \cdots \supseteq \mathfrak{a} \neq (o)$$

in $\mathfrak{R}$, und es ist eben $\mathfrak{A} \cap \mathfrak{R} = \mathfrak{a} \neq (o)$ nach (3) nur dann allgemein gewährleistet, wenn $\mathfrak{S}$ strenger Einselementoberring von $\mathfrak{R}$ ist. Es bleibt die Frage, ob unendlich viele $\mathfrak{L}_1 \supset \mathfrak{L}_2 \supset \cdots$ zum gleichen Verengungsideal $\mathfrak{l}$ gehören können. Nach (11) ist das ausgeschlossen, wenn die zugehörigen Zahlen $\lambda_1, \lambda_2, \ldots$ von vornherein beschränkt sind, also für $\alpha \geqq 2$. Für $\alpha = 0$, d. h. für $\mathfrak{R}^*/(0 - o) = \mathfrak{R}^* = \langle I, \mathfrak{R}\rangle$ existieren dagegen stets nichtabbrechende eingeschränkte Unterketten von (sogar zweiseitigen) Idealen, etwa

$$\mathfrak{R}^* 2 + \mathfrak{R} \supset \mathfrak{R}^* 4 + \mathfrak{R} \supset \cdots \supseteq \mathfrak{R} \neq (o).$$

[18]) Der Einheitlichkeit halber bezeichnen wir jetzt auch die zweiseitigen Ideale eines Einselementoberringes mit großen Buchstaben.

Trotzdem läßt sich ein Erhaltungssatz der eingeschränkten Unterkettenbedingung für strenge Einselementoberringe verhältnismäßig allgemein aussprechen. Ist nämlich $\mathfrak{R}' = \mathfrak{R}^* = \mathfrak{R}^*/(0-o)$ strenger Einselementoberring von $\mathfrak{R}$, so ist $\varkappa = 0$, d. h. $\mathfrak{R}$ ein Ring der Charakteristik $\nu = 0$, der nur Annullatoren als Operatorelemente enthält. Die wichtigsten Ringe dieser Art erfüllen aber den eingeschränkten Unterkettensatz selbst nicht:

(13) *Existiert in einem kommutativen Ring* $\mathfrak{R}$ *mit* $\varkappa = 0$ *ein reguläres Element* r, *so bilden die Ideale*

$$(r^2, 2r) \supset (r^2, 4r) \supset \cdots \supseteq (r^2) \neq (o)$$

eine nicht abbrechende eingeschränkte Unterkette[19]).

Es genügt offensichtlich zu zeigen, daß $(r^2, 2\tau r)$ stets $(r^2, 4\tau r)$ echt enthält. Aus der Annahme der Gleichheit folgte aber

$$2\tau r = x_1 r^2 + \gamma_1 r^2 + 4\tau x_2 r + 4\tau\gamma_2 r$$

mit $x_i \in \mathfrak{R}$, $\gamma_i \in \Gamma$, also

$$2\tau(1-2\gamma_2)r = (x_1 r + \gamma_1 r + 4\tau x_2)r.$$

Da r als reguläres Element bei Charakteristik 0 von unendlicher Ordnung ist, besagt dies, daß ein (von o verschiedenes) ganzzahliges Vielfaches von r gleich dem Produkt von r mit einem Ringelement s ist:

$$\gamma r = sr.$$

Dann wäre aber r wegen $(\gamma - s)r = o$ und $\gamma \neq s$ Nullteiler in $\mathfrak{R}' = \mathfrak{R}^*$, was nach den Betrachtungen in § 3 ausgeschlossen ist.

Dagegen kann in einem nichtkommutativen Ring $\mathfrak{R}$ mit $\varkappa = 0$ der eingeschränkte Unterkettensatz durchaus gelten. So hat z. B. der bereits betrachtete Ring

$$\mathfrak{R} = \begin{pmatrix} P & 0 \\ P & 0 \end{pmatrix} \quad \text{nur} \quad \mathfrak{a} = \begin{pmatrix} 0 & 0 \\ P & 0 \end{pmatrix},$$

als nichttriviales zweiseitiges Ideal, und es existiert kein Linksideal, welches $\mathfrak{a}$ umfaßt. Wir können also zusammenfassend formulieren:

(14) *Der eingeschränkte Unterkettensatz gilt für* $\mathfrak{R}$ *und einen strengen Einselementoberring* $\mathfrak{R}'$ *von* $\mathfrak{R}$ *gleichzeitig, abgesehen von den Fällen:*

1. $\varkappa = 0$, $\mathfrak{R}$ *nichtkommutativ;*
2. $\varkappa = 0$, $\mathfrak{R}$ *kommutativ, aber jedes Element von* $\mathfrak{R}$ *ist Nullteiler.*

In diesen Fällen gilt der eingeschränkte Unterkettensatz (wie stets bei $\varkappa = 0$*) für* $\mathfrak{R}' = \mathfrak{R}^*$ *nicht, obwohl er für* $\mathfrak{R}$ *erfüllt sein kann.*

[19]) Positiv gewendet bedeutet dies z. B.: Jeder Unterring eines algebraischen Zahlkörpers enthält (von 0 verschiedene) ganze rationale Zahlen.

Wie bereits in der Einleitung erwähnt, ergibt sich hieraus und aus den Überlegungen in § 3 sofort, daß der GRELLsche Übertragungssatz der eingeschränkten Unterkettenbedingung auf Oberringe von $\mathfrak{R}$, deren Quotientenkörper endlich algebraisch über dem von $\mathfrak{R}$ sind, auch ohne die Voraussetzung der Existenz von Einselementen ausgesprochen werden kann.

Wir wollen diese Überlegungen noch mit einigen Bemerkungen über Restklassenringe $\mathfrak{R}/\mathfrak{a}$ von $\mathfrak{R}$ abrunden. Zunächst ist klar, daß für jeden Einselementoberring $\mathfrak{S}$ von $\mathfrak{R}$ der Restklassenring $\mathfrak{S}/\mathfrak{a}$ Einselementoberring von $\mathfrak{R}/\mathfrak{a}$ ist. Doch brauchen sich dabei keine Eigenschaften von $\mathfrak{S}$ bezüglich $\mathfrak{R}$ wie „minimal" oder „streng" auf $\mathfrak{S}/\mathfrak{a}$ bezüglich $\mathfrak{R}/\mathfrak{a}$ zu übertragen. Nun folgt aber aus (11), daß es unter allen Idealen $\mathfrak{A}$ von $\mathfrak{S}$, die $\mathfrak{a}$ als Verengungsideal haben, stets ein maximales gibt, etwa $\tilde{\mathfrak{A}}$. Man kann also von $\mathfrak{S}/\mathfrak{a}$ zu $\mathfrak{S}/\tilde{\mathfrak{A}}$ übergehen, und erhält so in der Tat einen strengen und damit minimalen Einselementoberring von $\mathfrak{R}/\mathfrak{a}$.

Übrigens ist das Bild $\bar{a}$ eines α-Elementes a von $\mathfrak{R}$ auch wieder α-Element von $\mathfrak{R}/\mathfrak{a}$, doch brauchen nicht alle Operatorelemente von $\mathfrak{R}/\mathfrak{a}$ Bilder von Operatorelementen von $\mathfrak{R}$ zu sein.

Literaturverzeichnis

[1] A. A. ALBERT, *Modern higher algebra*, 5. Aufl. (Chicago, 1947).

[2] K. ASANO, Über die Quotientenbildung von Schiefringen, *J. Math. Soc. Japan*, **1** (1949), 73—78.

[3] B. BROWN—N. H. MCCOY, Rings with unit element which contain a given ring, *Duke Math. J.*, **13** (1946), 9—20.

[4] H. GRELL, Über die Erhaltung der Kettensätze der Idealtheorie, *Ber. Math.-Tagung Tübingen 1946* (1947), S. 67.

[5] L. RÉDEI, *Algebra* I (Leipzig, 1959).

[6] M. H. STONE, The theory of representations for Boolean algebras, *Transactions Amer. Math. Soc.*, **40** (1936), 37—111.

[7] J. SZENDREI, On the extension of rings without divisors of zero, *Acta Sci. Math.*, **13** (1949—50), 231—234.

(Eingegangen am 30. November 1959, in veränderter Form am 31. Oktober 1960)

Über vertauschbare Kontraktionen des Hilbertschen Raumes

Von S. BREHMER in Potsdam (Deutschland)

1. Es seien T_1, T_2 zwei *vertauschbare* Kontraktionen eines Hilbertschen Raumes $\mathfrak{H}$. SZ.-NAGY hat die Frage untersucht[1]) ob in einem Erweiterungsraum $\mathfrak{K}$ zwei *vertauschbare* unitäre Transformationen U_1, U_2 existieren derart, daß die Relationen

$$(P^{(2)}) \qquad \text{pr}\, U_1^{n_1} U_2^{n_2} = T_1^{n_1} T_2^{n_2}\ ^2)$$

für alle *nicht negativen* ganzen Zahlen n_1, n_2 erfüllt sind. Dieses Problem ist in voller Allgemeinheit noch nicht gelöst. In [A] wird gezeigt, daß die gesuchten unitären Transformationen existieren, wenn man für T_1, T_2 Doppelvertauschbarkeit voraussetzt ($T_1 T_2 = T_2 T_1$ und $T_1 T_2^* = T_2^* T_1$). In dieser Arbeit wird bewiesen, daß neben *Vertauschbarkeit* auch jede der beiden folgenden Bedingungen hinreichend ist:

$(B_1^{(2)})$ T_1 ist isometrisch, d. h. $\|T_1 f\| = \|f\|$ für alle $f \in \mathfrak{H}$;[3])

$(B_2^{(2)})$ $\|T_1\|^2 + \|T_2\|^2 \leqq 1$.

Beide Bedingungen werden auf den Fall beliebig vieler *vertauschbarer* Kontraktionen T_ω ($\omega \in \Omega$) verallgemeinert:

(B_1) alle Transformationen T_ω sind isometrisch;

(B_2) $\sum\limits_{\omega \in \Omega} \|T_\omega\|^2 \leqq 1$.

Ist eine dieser beiden Bedingungen erfüllt, was für (B_2) *offensichtlich nur im*

[1]) S. den Anhang zu F. RIESZ—B. SZ.-NAGY, *Vorlesungen über Funktionalanalysis* (Berlin, 1956). Diese Stelle wird in folgendem als [A] zitiert.

[2]) Ist A eine Transformation von $\mathfrak{K}$ und P die Projektion von $\mathfrak{K}$ auf $\mathfrak{H}$, so ist pr A die durch $(\text{pr}\, A) f = PAf$ für alle $f \in \mathfrak{H}$ definierte Transformation von $\mathfrak{H}$.

[3]) Der Verfasser hat darüber hinaus bewiesen, daß auch folgende Bedingung hinreichend ist: „Die Elemente f, für die $\|T_1 f\| = \|f\|$ *oder* $\|T_2^* f\| = \|f\|$ ist, spannen den Raum $\mathfrak{H}$ auf." Hierfür liegt z. Zt. nur ein recht langwieriger Beweis vor.

Falle abzählbar unendlich vieler von 0 verschiedener T_ω möglich ist, so existiert in einem Erweiterungsraum $\mathfrak{R}$ ein System von vertauschbaren unitären Transformationen $\{U_\omega\}_{\omega\in\Omega}$ derart, daß

$$\text{(P)} \qquad \text{pr}\, U_{\omega_1}^{n_1} \dots U_{\omega_p}^{n_p} = T_{\omega_1}^{n_1} \dots T_{\omega_p}^{n_p}$$

für alle endlichen Teilsysteme $\{\omega_1, \dots, \omega_p\} \subseteq \Omega$ und alle Systeme nicht negativer ganzer Zahlen $n_1, \dots, n_p$ gilt.

Für die Anregung zur Bearbeitung dieses Themas spreche ich Herrn Professor BÉLA SZ.-NAGY meinen herzlichen Dank aus.

2. Wir führen die folgenden Bezeichnungen ein. Jeder Kontraktion T (T_k, T_ω usw.) ordnen wir die von einem komplexen Parameter z (z_k, z_ω usw.) abhängigen Transformationen

$$\text{(1)} \qquad S = zT, \quad R = \sum_{k=1}^{\infty} S^k$$

zu. Für $r = |z| < 1$ gelten dann die Relationen

$$\text{(2)} \qquad (I+R)S = R, \quad (I-S)^{-1} = I+R.$$

Für einen beliebigen Operator A definieren wir ferner:

$$\text{(3)} \qquad A^{(n)} = \begin{cases} A^n & \text{für} \quad n = 0, 1, 2, \dots, \\ A^{*|n|} & \text{für} \quad n = -1, -2, \dots . \end{cases}$$

Es seien nun zwei vertauschbare Kontraktionen T_1, T_2 gegeben. Wir bilden die Transformation

$$W = T(r, \varphi_1, \varphi_2) = \sum_{n_1=-\infty}^{\infty} \sum_{n_2=-\infty}^{\infty} r^{|n_1|+|n_2|} e^{i(n_1\varphi_1+n_2\varphi_2)} T(n_1, n_2)$$

mit

$$T(n_1, n_2) = \begin{cases} T_1^{(n_1)} T_2^{(n_2)} & \text{für} \quad n_1 n_2 \geqq 0, \\ T_2^{*|n_2|} T_1^{n_1} & \text{für} \quad n_1 > 0, n_2 < 0, \\ T_1^{*|n_1|} T_2^{n_2} & \text{für} \quad n_1 < 0, n_2 > 0. \end{cases}$$

Unsere Behauptung ist bewiesen, wenn gezeigt werden kann, daß die Transformation W für $r<1$ *positiv* ist. Man schließt dann nämlich ebenso wie in [A] bei dem für den Fall der Doppelvertauschbarkeit geführten Beweis, daß in einem Erweiterungsraum zwei vertauschbare unitäre Transformationen U_1, U_2 existieren derart, daß $\text{pr}\, U_1^{n_1} U_2^{n_2} = T(n_1, n_2)$ für alle ganzzahligen n_1, n_2 ist. Insbesondere sind dann die Relationen $(P^{(2)})$ für alle nicht negativen n_1, n_2 erfüllt.

Zum Beweis, daß W positiv ist, formen wir W unter Verwendung von (3) und (1) um:

$$W=\sum_{n_1 n_2 \geqq 0} S_1^{(n_1)} S_2^{(n_2)}+\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty} S_2^{*n_2} S_1^{n_1}+\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty} S_1^{*n_1} S_2^{n_2}=$$

$$=I+\sum_{n_1=1}^{\infty}(S_1^{n_1}+S_1^{*n_1})+\sum_{n_2=1}^{\infty}(S_2^{n_2}+S_2^{*n_2})+\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}(S_1^{n_1}S_2^{n_2}+S_1^{*n_1}S_2^{*n_2})+$$

$$+\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}(S_2^{*n_2}S_1^{n_1}+S_1^{*n_1}S_2^{n_2})=I+2\,\mathrm{Re}\,(R_1+R_2+R_1R_2+R_2^*R_1).$$

Die rechte Seite kann man auch in der Form

$$(I+R_1^*)(I+R_2^*)\cdot(I+R_1)(I+R_2)-R_1^*(I+R_2^*)\cdot(I+R_1)R_2-$$
$$-R_2^*(I+R_1^*)\cdot(I+R_2)R_1+R_1^*R_2^*\cdot R_1R_2$$

schreiben, wovon man sich durch Ausmultiplizieren überzeugt. Hierbei ist zu beachten, daß die Faktoren nur links bzw. nur rechts von dem Punkt vertauscht werden dürfen. Ersetzt man hier alle Faktoren R_i bzw. R_i^* durch $(I+R_i)S_i$ bzw. $(I+R_i^*)S_i^*$, so erhält man

$$W=(I+R_1^*)(I+R_2^*)(I-S_1^*S_1-S_2^*S_2+S_1^*S_2^*S_1S_2)(I+R_2)(I+R_1).$$

Für alle $f\in\mathfrak{H}$ ist somit

$$(Wf,f)=((I-S_1^*S_1-S_2^*S_2+S_1^*S_2^*S_1S_2)(I+R_1)(I+R_2)f,(I+R_1)(I+R_2)f)$$

oder, mit $(I+R_1)(I+R_2)f=g$,

$$(Wf,f)=\|g\|^2-\|S_1g\|^2-\|S_2g\|^2+\|S_1S_2g\|^2$$
$$=\|g\|^2-r^2\|T_1g\|^2-r^2\|T_2g\|^2+r^4\|T_1T_2g\|^2.$$

Ist W positiv für alle $r<1$, so ist die rechte Seite auch für $r=1$ positiv:

$$\|g\|^2-\|T_1g\|^2-\|T_2g\|^2+\|T_1T_2g\|^2\geqq 0. \tag{4}$$

Ist umgekehrt (4) für alle $g\in\mathfrak{H}$ erfüllt, so ist $(Wf,f)\geqq 0$ auch für $r<1$. Zum Beweis dieser Behauptung betrachten wir das Polynom

$$p(r^2)=\|g\|^2-r^2\|T_1g\|^2-r^2\|T_2g\|^2+r^4\|T_1T_2g\|^2$$

für $g\neq 0$. Dann ist $p(0)>0$ und nach Voraussetzung (4) ist $p(1)\geqq 0$. Nähme nun $p(r^2)$ für ein $r^2<1$ einen negativen Wert an, so gäbe es im Intervall $0<r^2\leqq 1$ zwei verschiedene reelle Nullstellen des Polynoms und die Faktorzerlegung hätte die Gestalt

$$p(r^2)=\|g\|^2(1-ar^2)(1-br^2),$$

wobei $a\geqq 1$ und $b>1$ sein müßte. Das ist wegen

$$ab\|g\|^2=\|T_1T_2g\|^2\leqq\|g\|^2$$

ein Widerspruch. Folglich ist $p(r^2)=(Wf,f)\geqq 0$ für alle $r<1$. Die Bedingung (4) ist also hinreichend dafür, daß W positiv ist. Es bleibt zu beweisen, daß jede der Bedingungen $(B_1^{(2)})$ und $(B_2^{(2)})$ hinreichend für (4) ist. Aus $(B_2^{(2)})$ folgt

$$\|g\|^2-\|T_1g\|^2-\|T_2g\|^2+\|T_1T_2g\|^2\geqq$$

$$\geqq\|g\|^2-\|T_1\|^2\|g\|^2-\|T_2\|^2\|g\|^2=(1-\|T_1\|^2-\|T_2\|^2)\|g\|^2\geqq 0,$$

und aus $(B_1^{(2)})$ folgt

$$\|g\|^2-\|T_1g\|^2-\|T_2g\|^2+\|T_1T_2g\|^2=0$$

für alle $g\in\mathfrak{H}$. Damit sind alle unsere Behauptungen für den Fall zweier Kontraktionen bewiesen.

3. Es sei nun $\{T_\omega\}_{\omega\in\Omega}$ ein System von vertauschbaren Kontraktionen. Auf der additiven Gruppe G aller Vektoren $\mathfrak{n}=\{n_\omega\}_{\omega\in\Omega}$ mit ganzzahligen Komponenten n_ω, die fast alle gleich Null sind, definieren wir die Operatorfunktion

$$T(\mathfrak{n})=\prod_{n_\omega<0}T_\omega^{(n_\omega)}\cdot\prod_{n_\omega\geqq 0}T_\omega^{(n_\omega)}.$$

Ferner bilden wir zu einem beliebigen, aber fest gewählten Teilsystem $\{\omega_1,\ldots,\omega_p\}\subseteq\Omega$ die Untergruppe $G_p\subseteq G$ der Vektoren $\mathfrak{n}$ mit $n_\omega=0$ für $\omega\neq\omega_i$ $(i=1,\ldots,p)$ und setzen zur Vereinfachung der Schreibweise

$$T_{\omega_i}=T_i,\quad n_{\omega_i}=n_i\qquad(i=1,\ldots,p).$$

In Verallgemeinerung des oben für $p=2$ geführten Beweises werden wir zeigen, daß die Transformation

$$W_p=T(r,\varphi_1,\ldots,\varphi_p)=\sum_{\mathfrak{n}\in G}r^{|n_1|+\ldots+|n_p|}e^{i(n_1\varphi_1+\ldots+n_p\varphi_p)}T(\mathfrak{n}) \tag{5}$$

unter der Voraussetzung (B_1) bzw. (B_2) für $r<1$ *positiv* ist. Wie in [A] kann hieraus gefolgert werden, daß $T(\mathfrak{n})$ auf der zu beliebigen $\omega_1,\ldots,\omega_p\in\Omega$ gebildeten Untergruppe G_p und damit auf der Gruppe G selbst positiv definit ist. Aus dem „Hauptsatz" von [A] folgt dann die Existenz eines Systems von vertauschbaren unitären Transformationen U_ω, das nach unserer Definition von $T(\mathfrak{n})$ den geforderten Bedingungen (P) genügt.

Wir fassen die Indizes der Komponenten des Vektors $\mathfrak{n}\in G_p$, für die $n_i>0$ bzw. $n_j<0$ bzw. $n_k=0$ ist, zu den Indexsystemen

$$\begin{aligned}I_\varrho&:1\leqq i_1<\cdots<i_\varrho\leqq p,\\ J_\sigma&:1\leqq j_1<\cdots<j_\sigma\leqq p,\\ K_\tau&:1\leqq k_1<\cdots<k_\tau\leqq p\end{aligned} \tag{6}$$

mit $\varrho+\sigma+\tau=p$ zusammen. Die Systeme I_0, J_0, K_0 sind hierbei als „leer" zu betrachten. Die Summation über alle $\mathfrak{n}\in G_p$ in (5) kann ersetzt werden

durch eine Summation über alle Indexsysteme $I_\varrho, J_\sigma, K_\tau$, die den Bedingungen (6) genügen und eine Permutation der Zahlen $1, \ldots, p$ bilden, verbunden mit einer Summation der Komponenten n_{i_λ} von 1 bis ∞ und der Komponenten n_{j_ν} von -1 bis $-\infty$. Setzen wir zur Vereinfachung $m_j = -n_j$, so gilt

$$W_p = \sum_{\varrho+\sigma+\tau=p} \sum_{I_\varrho, J_\sigma, K_\tau} \sum_{m_{k_1}=1}^{\infty} \cdots \sum_{m_{j_\sigma}=1}^{\infty} \sum_{n_{i_1}=1}^{\infty} \cdots \sum_{n_{i_\varrho}=1}^{\infty} S(\mathfrak{n})$$

mit $S(\mathfrak{o}) = I$ und

$$S(\mathfrak{n}) = S_{j_1}^{*m_{j_1}} \cdots S_{j_\sigma}^{*m_{j_\sigma}} S_{i_1}^{n_{i_1}} \cdots S_{i_\varrho}^{n_{i_\varrho}}$$

für $\mathfrak{n} \neq \mathfrak{o}$. Es folgt

$$W_p = \sum_{\varrho+\sigma+\tau=p} \sum_{I_\varrho, J_\sigma, K_\tau} R_{j_1}^* \ldots R_{j_\sigma}^* R_{i_1} \ldots R_{i_\varrho}, \tag{7}$$

wobei zu ergänzen ist, daß die zweite Summe für $\tau = p$ aus dem einzigen Glied I bestehen soll. Wir behaupten, daß (7) auch in der Form

$$\begin{aligned} W_p = & \prod_{j=1}^{p} (I + R_j^*) \prod_{i=1}^{p} (I + R_i) - \\ & - \sum_{1 \leqq \nu_1 \leqq p} \prod_{j=1}^{p} (I + R_j^*) S_{\nu_1}^* S_{\nu_1} \prod_{i=1}^{p} (I + R_i) + \\ & + \sum_{1 \leqq \nu_1 < \nu_2 \leqq p} \prod_{j=1}^{p} (I + R_j^*) S_{\nu_1}^* S_{\nu_2}^* S_{\nu_1} S_{\nu_2} \prod_{i=1}^{p} (I + R_i) - \\ & - + \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & + (-1)^p \prod_{j=1}^{p} (I + R_j^*) S_1^* \ldots S_p^* S_1 \ldots S_p \prod_{i=1}^{p} (I + R_i) \end{aligned} \tag{8}$$

geschrieben werden kann. Zunächst erkennt man, daß beim Ausmultiplizieren der in der ersten Zeile von (8) stehenden Produkte jeder Summand von (7) genau einmal auftritt. Darüber hinaus ergeben sich nur Produkte, in denen gesternte und ungesternte Faktoren mit *gleichen* Indizes auftreten, z. B.

$$R_{j_1}^* \ldots R_{j_\sigma}^* \; R_{i_1}^* \ldots R_{i_\varrho}^* \; R_{i_1} \ldots R_{i_\varrho}. \tag{9}$$

Diese Faktoren treten aber auch in den folgenden Zeilen von (8) auf, wenn wir alle Faktoren S_ν mit Hilfe der Relation $S_\nu (I + R_\nu) = R_\nu$ eliminieren und dann ausmultiplizieren. Der Summand (9) tritt in der ersten Zeile von (8) genau $\binom{\varrho}{0}$-mal, in der zweiten $\binom{\varrho}{1}$-mal, in der dritten $\binom{\varrho}{2}$-mal auf, usw. Bei den sukzessiven Additionen und Subtraktionen heben sich alle diese Summanden wegen

$$\sum_{i=0}^{p} (-1)^{i+1} \binom{\varrho}{i} = 0 \qquad (\varrho = 1, \ldots, p)$$

heraus. Damit ist (8) bewiesen. Mit

$$g = \prod_{i=1}^{p} (I + R_i) f$$

folgt

$$(W_p f, f) = \left(\left(I + \sum_{k=1}^{p} (-1)^k \sum_{1 \leqq i_1 < \ldots < i_k \leqq p} S_{i_1}^* \ldots S_{i_k}^* S_{i_1} \ldots S_{i_k} \right) g, g \right) =$$

(10)

$$= \|g\|^2 + \sum_{k=1}^{p} (-1)^k \sum_{1 \leqq i_1 < \ldots < i_k \leqq p} r^{2k} \| T_{i_1} \ldots T_{i_k} g \|^2.$$

Die rechte Seite ist eine endliche alternierende Reihe mit den Gliedern

$$a_k = \sum_{1 \leqq i_1 < \ldots < i_k \leqq p} r^{2k} \| T_{i_1} \ldots T_{i_k} g \|^2.$$

Es sei nun (B_2) erfüllt. Dann gilt

$$a_{k+1} = \sum_{1 \leqq i_1 < \ldots < i_{k+1} \leqq p} r^{2k+2} \| T_{i_1} \ldots T_{i_{k+1}} g \|^2 \leqq$$

$$\leqq \sum_{1 \leqq i_1 < \ldots < i_{k+1} \leqq p} r^{2k+2} \| T_{i_{k+1}} \|^2 \cdot \| T_{i_1} \ldots T_{i_k} g \|^2 \leqq$$

$$\leqq r^2 \sum_{i=1}^{p} \| T_i \|^2 \sum_{1 \leqq i_1 < \ldots < i_k \leqq p} r^{2k} \| T_{i_1} \ldots T_{i_k} g \|^2 \leqq a_k,$$

d. h. die Glieder nehmen monoton ab. Für die nach dem ersten negativen Glied abbrechende Partialsumme gilt, wiederum wegen (B_2),

$$\|g\|^2 - \sum_{i=1}^{p} r^2 \| T_i g \|^2 \geqq \|g\|^2 \left(1 - \sum_{i=1}^{p} \| T \|^2 \right) \geqq 0.$$

Diese Partialsumme bildet eine obere Schranke für die Partialsummen der Reihe (10) mit den monoton abnehmenden Gliedern a_k. Folglich ist W_p positiv, und die Bedingung (B_2) ist hinreichend.

Ist die Bedingung (B_1) erfüllt, so folgt aus (10)

$$(W_p f, f) = \|g\|^2 + \sum_{k=1}^{p} (-1)^k \binom{p}{k} r^{2k} \|g\|^2 = (1 - r^2)^p \|g\|^2 \geqq 0.$$

Damit ist auch die letzte Behauptung bewiesen[4]).

(Eingegangen am 2. Mai 1960)

[4]) Ist $p > 2$, so kann daraus, daß (10) für $r = 1$ und für alle $g \in \mathfrak{H}$ positiv ist, nicht gefolgert werden, daß $W_p \geqq O$ ist. Ein Analogon zur Bedingung (4) kann also im allgemeinen Fall nicht formuliert werden.

Bemerkungen zur vorstehenden Arbeit des Herrn S. Brehmer*)

Von BÉLA SZ.-NAGY in Szeged

Sei $\mathbf{T}=\{T_\omega\}_{\omega\in\Omega}$ ein System von *vertauschbaren* Kontraktionen des Hilbertschen Raumes $\mathfrak{H}$. Es wird gefragt, unter welchen Bedingungen existiert ein System $\mathbf{U}=\{U_\omega\}_{\omega\in\Omega}$ von ebenfalls *vertauschbaren* unitären Operatoren eines geeigneten Hilbertschen Erweiterungsraumes $\mathfrak{K}$ derart, daß die Relation

$$\prod_{\omega} T_\omega^{n_\omega} = \mathrm{pr} \prod_{\omega} U_\omega^{n_\omega} \tag{1}$$

für beliebige nichtnegative ganze Exponenten n_ω gilt, von denen nur endlich viele von 0 verschieden sind.

Eine hinreichende Bedingung ist die folgende[1]):

(A) Die Operatoren T_ω sind alle *doppelvertauschbar*, d. h. für $\omega\neq\omega'$ sind nicht nur T_ω und $T_{\omega'}$, sondern auch T_ω und $T_{\omega'}^*$ vertauschbar.

In der vorstehenden Arbeit beweist Herr S. BREHMER die folgende weitere hinreichende Bedingung:

(B) Für jedes endliche Teilsystem $\mathbf{T}_0=\{T_\omega\}_{\Omega_0}$, für jedes $h\in\mathfrak{H}$ und für $0\leqq r<1$ gilt:

$$\sum_{k=0}^{s}(-1)^k r^{2k}\sum_{v\in V_k(\Omega_0)}\|T(v)h\|^2\geqq 0;$$

hier bezeichnet s die Anzahl der Elemente von T_0, $V_k(\Omega_0)$ die Menge der aus der Indexmenge Ω_0 gebildeten Kombinationen k-ter Klasse, und für eine solche Kombination $v=\{\omega_1,\omega_2,\ldots,\omega_k\}$ wird

$$T(v)=T_{\omega_1}T_{\omega_2}\cdots T_{\omega_k}$$

gesetzt [im Falle der leeren Kombination ist $T(v)=I$].

*) S. BREHMER, Über vertauschbare Kontraktionen des Hilbertschen Raumes, *Acta Sci. Math.*, **22** (1961), 106–111.

[1]) B. SZ.-NAGY, *Fortsetzung linearer Transformationen des Hilbertschen Raumes mit Austritt aus dem Raum*, Anhang zu den *Vorlesungen über Funktionalanalysis* von F. Riesz und B. Sz.-Nagy (Berlin, 1956).

Bemerkung 1. Man kann die obigen Bedingungen gleichzeitig verallgemeinern. *Es genügt vorauszusetzen, daß* (B) *für diejenigen endlichen Teilsysteme* $\mathbf{T}_0'$ *gilt, deren Elemente* $T_{\omega'}$ *nicht mit allen anderen Elementen* T_ω *von* $\mathbf{T}$ $(\omega \neq \omega')$ *doppelvertauschbar sind.*

Beweis. Man hat zu zeigen, daß (B) dann für *jedes* endliche Teilsystem $\mathbf{T}_0$ von $\mathbf{T}$ gilt. Sei $\mathbf{T}_0'' = \{T_\omega\}_{\omega \in \Omega''}$ die Menge derjenigen Elemente von $\mathbf{T}_0$, die mit allen anderen Elementen von $\mathbf{T}$ doppelvertauschbar sind, und sei $\mathbf{T}_0' = \{T_\omega\}_{\omega \in \Omega'}$ die Menge der übrigen Elemente von $\mathbf{T}_0$; $\mathbf{T}_0'$ möge aus s', $\mathbf{T}_0''$ aus s'' Elementen bestehen (s' oder s'' kann evtl. auch gleich 0 sein). Da jede aus der Indexmenge $\Omega' \cup \Omega''$ gebildete Kombination k-ter Klasse sich aus einer aus der Indexmenge Ω' gebildeten Kombination k'-ter Klasse und einer aus der Indexmenge Ω'' gebildeten Kombination k''-ter Klasse zusammensetzt $(k' + k'' = k)$, so ist

$$S = \sum_{k=0}^{s'+s''} (-1)^k r^{2k} \sum_{v \in V_k(\Omega' \cup \Omega'')} \|T(v)h\|^2 =$$

$$= \sum_{k=0}^{s'+s''} (-1)^k r^{2k} \sum_{\substack{0 \leqq k' \leqq s' \\ 0 \leqq k'' \leqq s'' \\ k'+k''=k}} \sum_{\substack{v' \in V_{k'}(\Omega') \\ v'' \in V_{k''}(\Omega'')}} \|T(v')\,T(v'')h\|^2 = \tag{2}$$

$$= \sum_{0 \leqq k' \leqq s'} \sum_{0 \leqq k'' \leqq s''} (-1)^{k'+k''} r^{2(k'+k'')} \sum_{v' \in V_{k'}(\Omega')} \sum_{v'' \in V_{k''}(\Omega'')} \|T(v')\,T(v'')h\|^2.$$

Mit der Benützung der Doppelvertauschbarkeit der Elemente des Systems $\mathbf{T}_0''$ untereinander erhalten wir:

$$S = \sum_{k'=0}^{s'} (-1)^{k'} r^{2k'} \sum_{v' \in V_{k'}(\Omega')} \left[\sum_{k''=0}^{s''} (-1)^{k''} r^{2k''} \sum_{v'' \in V_{k''}(\Omega'')} (T^*(v'')T(v'')T(v')h,\, T(v')h) \right]$$

$$= \sum_{k'=0}^{s'} (-1)^{k'} r^{2k'} \sum_{v' \in V_{k'}(\Omega')} \left(\prod_{\omega \in \Omega''} (I - r^2 T_\omega^* T_\omega) \cdot T(v')h,\, T(v')h \right).$$

Nun ist $P = \prod_{\omega \in \Omega''} (I - r^2 T_\omega^* T_\omega)$, als Produkt vertauschbarer positiver Operatoren selbst positiv, und da P mit den Elementen von $\mathbf{T}_0'$ doppelvertauschbar ist, so ist $P^{1/2}$ es auch. Also gilt:

$$S = \sum_{k'=0}^{s'} (-1)^{k'} r^{2k'} \sum_{v' \in V_{k'}(\Omega')} \|T(v')P^{1/2}h\|^2.$$

Wegen der Gültigkeit der Bedingung (B) für das System $\mathbf{T}_0'$ folgt hieraus $S \geqq 0$, w. z. b. w.

Nach BREHMER[2]) gilt Bedingung (B) für ein System $\mathbf{T}=\{T_\omega\}_{\omega\in\Omega}$ insbesondere in den folgenden zwei Fällen:

(B_1) alle Operatoren T_ω sind isometrisch;

(B_2) $\sum_{\omega\in\Omega}\|T_\omega\|^2\leqq 1$.

Bemerkung 2. *Allgemeiner, gilt* (B) *im Falle* $\mathbf{T}=\mathbf{T}_1\cup\mathbf{T}_2$, *wobei das Teilsystem* $\mathbf{T}_1$ *der Bedingung* (B_1) *und das Teilsystem* $\mathbf{T}_2$ *der Bedingung* (B_2) *genügt.*

Beweis. Sei $\mathbf{T}_0=\mathbf{T}_0'\cup\mathbf{T}_0''$ ein endliches Teilsystem von $\mathbf{T}$ mit $\mathbf{T}_0'=\{T_\omega\}_{\omega\in\Omega'}\subseteqq\mathbf{T}_1$ und $\mathbf{T}_0''=\{T_\omega\}_{\omega\in\Omega''}\subseteqq\mathbf{T}_2$; $\mathbf{T}_0'$ möge aus s', $\mathbf{T}_0''$ aus s'' Elementen bestehen. Da $T(v')$ für jede aus Ω' gebildete Kombination v' isometrisch und da die Anzahl der aus Ω' gebildeten Kombinationen k'-ter Klasse gleich $\binom{s'}{k'}$ ist, so hat man (vgl. (2)):

$$S=\sum_{k=0}^{s'+s''}(-1)^k r^{2k}\sum_{v\in V_k(\Omega'\cup\Omega'')}\|T(v)h\|^2=$$

$$=\sum_{k'=0}^{s'}\sum_{k''=0}^{s''}(-1)^{k'+k''}r^{2(k'+k'')}\binom{s'}{k'}\sum_{v''\in V_{k''}(\Omega'')}\|T(v'')h\|^2=$$

$$=(1-r^2)^{s'}\sum_{k''=0}^{s''}(-1)^{k''}r^{2k''}\sum_{v''\in V_{k''}(\Omega'')}\|T(v')h\|^2.$$

Da $1-r^2>0$ und da $\mathbf{T}_0''$ der Bedingung (B_2), also auch der Bedingung (B) genügt, so hat man $S\geqq O$, w. z. b. w.

(Eingegangen am 20. Mai 1960)

[2]) A. a. O.

Points séparés dans le spectre d'une C^*-algèbre

Par J. DIXMIER à Paris

Soit A une C^*-algèbre. Soit $\hat{A}$ le spectre de A, c'est-à-dire l'ensemble des classes de représentations irréductibles non nulles de A dans un espace hilbertien, muni d'une topologie à la JACOBSON (cf. [4]). L'étude de l'espace topologique $\hat{A}$ est importante puisque le dual d'un groupe localement compact est un espace de ce type.

Quand $\hat{A}$ est séparé, $\hat{A}$ est localement compact. Malheureusement, $\hat{A}$ n'est pas séparé en général. On cherche alors des propriétés se rapprochant le plus possible de la séparation. Par exemple, si A est CCR ([7]), $\hat{A}$ contient une partie ouverte localement compacte partout dense; toutefois, il n'existe pas dans $\hat{A}$ de partie ouverte localement compacte plus grande que toutes les autres (la réunion de deux parties ouvertes localement compactes de $\hat{A}$ n'est pas séparée en général). Dans cet ordre d'idées, il serait naturel de dire qu'un point π de $\hat{A}$ est „séparé'' dans $\hat{A}$ si, pour tout π' de $\hat{A}$ distinct de π, π et π' admettent des voisinages disjoints (une définition un peu différente est donnée plus loin; elle équivaut à la précédente quand A est une CCR-algèbre). Il s'agit alors de prouver que l'ensemble des points séparés de $\hat{A}$ est „le plus grand possible''. C'est l'objet des prop. 1, 2 et 3 ci-dessous. Les exemples connus laisseraient supposer que, lorsque A est une CCR-algèbre séparable, l'ensemble des points séparés de $\hat{A}$ contient une partie ouverte partout dense de A. On verra malheureusement (prop. 4) qu'il n'en est rien.

Il est facile (cf. § 1) de relier la notion de point séparé à la continuité des fonctions $\pi \to \|\pi(x)\|$ sur $\hat{A}$ (x: élément fixé de A). Dans la dernière partie de ce travail, on étudie la continuité des fonctions $x \to \mathrm{Tr}\pi(x)$ (x, élément positif fixé de A). On prouve d'abord (ceci n'a rien à voir avec la notion de point séparé) que cette fonction est toujours semi-continue inférieurement. On améliore ensuite ce résultat sur l'ensemble des points séparés de $\hat{A}$.

§ 1. Définition et existence des points séparés

Définition. Soit X un espace topologique. Un point b de X sera dit *séparé dans* X si, pour tout point b' de X non adhérent à b, les points b et b' admettent des voisinages disjoints.

Soient A une C^*-algèbre, et $\pi_0 \in \hat{A}$. Les conditions suivantes sont équivalentes:

(i) π_0 est séparé dans $\hat{A}$;

(ii) pour tout $x \in A$ tel que $\pi_0(x) = 0$, la fonction $\pi \to \|\pi(x)\|$ sur $\hat{A}$ est continue en π_0;

(iii) pour tout $x \in A$, la fonction $\pi \to \|\pi(x)\|$ est continue en π_0;

(iv) pour tout élément hermitien $x \in A$ et tout $\varepsilon > 0$, il existe un voisinage U de π_0 dans $\hat{A}$ tel que, pour tout $\pi \in U$, le spectre de $\pi(x)$ soit contenu dans un ε-voisinage de $\{0\} \cup S$ (en désignant par S le spectre de $\pi_0(x)$).

Les raisonnements prouvant ces équivalences sont connus (et on peut aussi faire référence au th. 2.1 de [4]). Donnons de brèves indications: (i) $\Rightarrow$ (ii) se démontre par le raisonnement de [7], p. 235, 1.21—30; (ii) $\Rightarrow$ (iv) par le raisonnement de [7], p. 228, 1.18—22; (iv) $\Rightarrow$ (iii) par le raisonnement de [7], p. 235, 1.31—36; (iii) $\Rightarrow$ (i) est évident compte tenu de la semi-continuité inférieure de la fonction $\pi \to \|\pi(x)\|$ ([4], lemme 2.1).

Lemme 1. *Soient A une C^*-algèbre, et $x_0 \in A$. L'ensemble des points de continuité de la fonction $\pi \to \|\pi(x_0)\|$ sur $\hat{A}$ est un G_δ partout dense de $\hat{A}$.*

Pour tout $\pi \in \hat{A}$, soit $f(\pi) = \|\pi(x_0)\|$. Alors f est semi-continue inférieurement, et $\hat{A}$ est un espace de Baire ([3], th. 1). La démonstration du lemme est alors classique. Toutefois, comme $\hat{A}$ n'est pas nécessairement séparé ni à base dénombrable, nous la reproduisons pour la commodité du lecteur. Pour tout entier $n > 0$, soit B_n l'ensemble des points de $\hat{A}$ où l'oscillation de f est $\geqq 1/n$. C'est un ensemble fermé dans $\hat{A}$ (car l'oscillation d'une fonction est semi-continue supérieurement). Supposons que B_n contienne une partie ouverte non vide U. Soit $\alpha = \sup_{\pi \in U} f(\pi)$. Il existe $\pi_0 \in U$ tel que $f(\pi_0) > \alpha - \frac{1}{2n}$. Donc, pour tout π d'un voisinage de π_0, on a $\alpha - \frac{1}{2n} < f(\pi) \leqq \alpha$. Donc l'oscillation de f en π_0 est $\leqq \frac{1}{2n}$, ce qui est absurde. Donc B_n est rare. Donc $\bigcup_n B_n$ est un F_σ maigre. Or son complémentaire dans $\hat{A}$ est l'ensemble des points de continuité de f.

Proposition 1. *Soit A une C^*-algèbre séparable. L'ensemble des points séparés dans $\hat{A}$ est un G_δ partout dense de $\hat{A}$.*

Soit (x_i) une suite partout dense dans A. Soit $\pi_0 \in \hat{A}$. Les conditions suivantes sont équivalentes: *a*) pour tout $x \in A$, la fonction $\pi \to \|\pi(x)\|$ sur $\hat{A}$ est continue en π_0; *b*) pour tout i, la fonction $\pi \to \|\pi(x_i)\|$ sur $\hat{A}$ est continue en π_0. Or la condition *a*) signifie que π_0 est séparé dans $\hat{A}$. Donc l'ensemble des points séparés de $\hat{A}$ est égal à $C_1 \cap C_2 \cap \ldots$, en désignant par C_i l'ensemble des points de continuité de la fonction $\pi \to \|\pi(x_i)\|$ dans $\hat{A}$. Il suffit alors d'appliquer le lemme 1, et le fait que $\hat{A}$ est un espace de Baire.

Lemme 2. *Soit A une CCR-algèbre séparable dont le spectre $\hat{A}$ est quasi-compact* (i. e. vérifie l'axiome de Borel—Lebesgue sans être nécessairement séparé). *Alors l'ensemble des points séparés de $\hat{A}$ a un intérieur partout dense dans $\hat{A}$.*

Comme A est une CCR-algèbre, $\hat{A}$ contient une partie ouverte séparée partout dense U. Nous allons montrer que toute partie ouverte non vide V de U contient une partie ouverte non vide dont tous les points sont séparés dans A. Ceci prouvera le lemme.

Comme A est séparable, la topologie de $\hat{A}$ admet une base dénombrable $(U_1, U_2, \ldots)$([5], cor. du th. 3.2). Pour tout $\pi \in V$, $\hat{A} - \{\pi\}$ est ouvert (parce que A est une CCR-algèbre), donc est réunion de certains des U_i. Comme $\hat{A} - V$ est quasi-compact, il existe des indices $i_1, \ldots, i_n$ tels que $U_{i_1}, \ldots, U_{i_n}$ soient contenus dans $\hat{A} - \{\pi\}$ et recouvrent $\hat{A} - V$. Ainsi $\hat{A} - V$ est intersection d'ensembles de la forme $U_{i_1} \cup \cdots \cup U_{i_n}$. La famille de ces ensembles est dénombrable. Leurs complémentaires forment une famille dénombrable de parties fermées dont la réunion est V. Comme $\hat{A}$ est un espace de Baire, l'une de ces parties fermées, soit F, a un intérieur W qui est non vide. Montrons que tout $\pi \in W$ est séparé dans $\hat{A}$. Soit $\pi' \in \hat{A}$ un point distinct de π. Si $\pi' \in F$, on a $\pi \in U$ et $\pi' \in U$, donc π et π' admettent des voisinages (dans U, donc dans $\hat{A}$) qui sont disjoints puisque U est séparé. Si $\pi' \notin F$, W et $\hat{A} - F$ sont des voisinages disjoints de π et π' dans $\hat{A}$.

Proposition 2. *Soit A une C^*-algèbre séparable dont toutes les représentations irréductibles sont de dimension finie. Alors l'ensemble des points séparés de $\hat{A}$ a un intérieur partout dense dans $\hat{A}$.*

Soit B la C^*-algèbre déduite de A par adjonction d'un élément unité. Elle est séparable. Les représentations irréductibles de B sont de dimension finie, donc B est une CCR-algèbre. Puisque B a un élément unité, $\hat{B}$ est quasi-compact. Il existe (lemme 2) une partie ouverte U partout dense de $\hat{B}$ dont les points sont tous séparés dans $\hat{B}$. Or $\hat{A}$ s'identifie au complémentaire d'un point ω de $\hat{B}$. Les points de $U \cap \hat{A}$ sont séparés dans $\hat{A}$. Enfin $U \cap \hat{A}$ est ouvert dans $\hat{A}$, et partout dense dans $\hat{A}$ (parce que $\{\omega\}$ est fermé dans $\hat{B}$).

Proposition 3. *Soit Γ un groupe de Lie nilpotent simplement connexe. L'ensemble des points séparés de $\hat{\Gamma}$ a un intérieur partout dense dans $\hat{\Gamma}$.*

Soient E l'algèbre enveloppante de l'algèbre de Lie de Γ, et Z le centre de E. Pour tout $\pi \in \hat{\Gamma}$, soit χ_π le caractère infinitésimal de π. Soit I l'idéal de Z formé par les éléments classifiants (cf. [1]). Soit Ω l'ensemble des $\pi \in \hat{\Gamma}$ tels que χ_π soit non identiquement nul sur I; on sait ([1], th. 3) que Ω est une partie ouverte localement compacte partout dense de $\hat{\Gamma}$. On va voir que tout point π de Ω est séparé dans $\hat{\Gamma}$. Soit π' un point de $\hat{\Gamma}$ distinct de π. Montrons que π et π' admettent des voisinages disjoints. C'est évident si $\pi' \in \Omega$. Supposons $\pi' \notin \Omega$. Il existe un $a \in I$ tel que $\chi_\pi(a) \neq 0$, et on a $\chi_{\pi'}(a) = 0$. Donc la fonction $\varrho \to \chi_\varrho(a)$ sur $\hat{\Gamma}$ sépare π et π'. Or cette fonction est continue ([1], th. 1), d'où notre assertion.

§ 2. Un exemple de *CCR*-algèbre

On se fixe dans ce paragraphe un espace hilbertien H de dimension infinie, et une famille à un paramètre $t \to U_t$ (t réel) d'opérateurs unitaires dans H possédant les propriétés suivantes: 1) U_t est une fonction fortement continue de t; 2) U_t tend faiblement vers 0 quand $|t| \to +\infty$. (Par exemple, on peut prendre pour H l'espace des fonctions de carré intégrable sur la droite pour la mesure de Lebesgue, et pour U_t l'opérateur défini par la translation $\xi \to \xi + t$). Soit A la C^*-algèbre des opérateurs compacts dans H.

On se fixe également une partie Ω de $[0, 1]$.

Lemme 3. *Soit $t \to T(t)$ une application de R* (ensemble des nombres réels) *dans A, continue au sens de la norme. L'application $t \to U_t T(t) U_t^*$ de R dans A est continue au sens de la norme.*

On se ramène aussitôt au cas où $T(t) = T$ est indépendant de t. Comme tout élément de A est limite en norme d'opérateurs de rang fini, on peut ensuite se limiter au cas où T est de rang fini. Par linéarité, on peut enfin supposer que T est le projecteur sur la droite engendrée par un vecteur $\xi \in H$ de norme 1. Pour tout $\eta \in H$, on a alors

$$U_t T U_t^* \eta - U_{t'} T U_{t'}^* \eta = (U_t^* \eta | \xi) U_t \xi - (U_{t'}^* \eta | \xi) U_{t'} \xi =$$
$$= (\eta | U_t \xi) U_t \xi - (\eta | U_{t'} \xi) U_{t'} \xi$$

donc

$$\| (U_t T U_t^* - U_{t'} T U_{t'}^*) \eta \| \leqq \| (\eta | U_t \xi - U_{t'} \xi) U_t \xi \| + \| (\eta | U_{t'} \xi)(U_t \xi - U_{t'} \xi) \| \leqq$$
$$\leqq 2 \| \eta \| \, \| U_t \xi - U_{t'} \xi \|$$

donc

$$\| U_t T U_t^* - U_{t'} T U_{t'}^* \| \leqq 2 \| U_t \xi - U_{t'} \xi \|$$

ce qui prouve le lemme.

Lemme 4. *Soient $t \to T(t)$, $t \to T'(t)$ deux applications de R dans A, ayant des limites au sens de la norme quand $|t| \to +\infty$. Alors $\|T(t)U_t T'(t)\| \to 0$ et $\|T(t)U_t^* T'(t)\| \to 0$ quand $|t| \to +\infty$.*

On se ramène aussitôt au cas où $T(t) = T$ et $T'(t) = T'$ sont indépendants de t. Puis, comme dans la démonstration du lemme 3, on se ramène au cas où T (resp. T') est le projecteur sur la droite engendrée par un vecteur ξ (resp. ξ') de norme 1. Pour tout $\eta \in H$, on a alors

$$\|TU_t T'\eta\| = \|TU_t(\eta|\xi')\xi'\| = |(\eta|\xi')|\,\|(U_t\xi'|\xi)\xi\| \leqq \|\eta\|\,|(U_t\xi'|\xi)|$$

donc $\|TU_t T'\| \leqq |(U_t\xi'|\xi)|$ et $(U_t\xi'|\xi) \to 0$ quand $|t| \to +\infty$ puisque U_t tend faiblement vers 0. On raisonne de même pour $\|T(t)U_t^* T'(t)\|$.

Lemme 5. *Soit $t \to T(t)$ une application de R dans A, ayant une limite au sens de la norme quand $|t| \to +\infty$. Alors $U_t^* T(t) U_t$ tend fortement vers 0 quand $|t| \to +\infty$.*

On se ramène au cas où $T(t) = T$ est indépendant de t. Soit $\xi \in H$. Quand $|t| \to +\infty$, $U_t\xi$ tend faiblement vers 0, donc $\|U_t^* T(t) U_t \xi\| = \|TU_t\xi\| \to$ puisque T est compact.

Ceci posé, nous introduisons quelques notations.

Soit B l'ensemble des applications $t \to f(t)$ de $[0, 1]$ dans A telles que $\|f\| = \sup_{t \in [0,1]} \|f(t)\| < +\infty$. Cet ensemble est muni naturellement d'une structure de C^*-algèbre. Les $f \in B$ qui sont continues au sens de la norme forment une sous-C^*-algèbre de B que nous désignerons par C. Les représentations irréductibles non nulles de C dans un espace hibertien sont (à une équivalence près) les applications $f \to f(t_0)$, et l'espace topologique $\hat{C}$ s'identifie à l'espace topologique $[0, 1]$ ([6], th. 1.3); la C^*-algèbre C est une CCR-algèbre.

Pour tout $u \in [0, 1]$ et tout $T \in A$, soit $f_{u,T}$ l'élément de B défini de la manière suivante:

$$f_{u,T}(t) = U_{(t-u)^{-1}} T U_{(t-u)^{-1}}^* \quad \text{si} \quad t \neq u$$
$$f_{u,T}(u) = 0.$$

Lemme 6. *Soient $u \in [0, 1]$, $T \in A$, et $g \in C$. Alors $gf_{u,T} \in C$ et $f_{u,T}g \in C$.*

Si $t_0 \neq u$, l'application $t \to f_{u,T}(t)$ est continue en t_0 au sens de la norme d'après de lemme 3, donc il en est de même des applications $t \to (gf_{u,T})(t)$ et $t \to (f_{u,T}g)(t)$. Quand $t \to u$, $\|(gf_{u,T})(t)\| = \|g(t)U_{(t-u)^{-1}} T\| \to 0$ et $\|(f_{u,T}g)(t)\| = \|TU_{(t-u)^{-1}}^* g(t)\| \to 0$ d'après le lemme 4. Or $(f_{u,T}g)(u) = (gf_{u,T})(u) = 0$. D'où le lemme.

Lemme 7. *Soient $u, u' \in [0, 1]$, et $T, T' \in A$. Si $u = u'$, on a $f_{u,T} f_{u',T'} = f_{u,TT'}$. Si $u \neq u'$, on a $f_{u,T} f_{u',T'} \in C$.*

La première assertion est évidente. Si $t_0 \neq u$ et $t_0 \neq u'$ les applications $t \to f_{u,T}(t)$ et $t \to f_{u',T'}(t)$ sont continues en t_0 au sens de la norme (lemme 3), donc il en est de même de l'application $t \to (f_{u,T} f_{u',T'})(t)$. Supposons maintenant $u \neq u'$. Quand $t \to u$, $\|(f_{u,T} f_{u',T'})(t)\| = \|T U^*_{(t-u)^{-1}} f_{u',T'}(t)\| \to 0$ d'après le lemme 4, donc $f_{u,T} f_{u',T'}$ est continu au sens de la norme en u. On voit de même que cette application est continue au sens de la norme en u'. D'où le lemme.

Lemme 8. *Les éléments de B de la forme $g + f_{u_1,T_1} + \cdots + f_{u_n,T_n}$, où $g \in C$, $u_1, \ldots, u_n \in \Omega$ et $T_1, \ldots, T_n \in A$, constituent une sous-algèbre involutive D' de B. Et C est un idéal bilatère fermé de D'.*

Ceci résulte aussitôt des lemmes 6 et 7.

Lemme 9. *Soient $g \in C$, $u_1, \ldots, u_n$ des éléments distincts de Ω, et $T_1, \ldots, T_n \in A$. On a*

$$\|g + f_{u_1,T_1} + \cdots + f_{u_n,T_n}\| \geqq \sup(\|T_1\|, \ldots, \|T_n\|).$$

Quand $t \to u_1$, $U^*_{(t-u_1)^{-1}}[g(t) + f_{u_2,T_2}(t) + \cdots + f_{u_n,T_n}(t)] U_{(t-u_1)^{-1}}$ tend fortement vers 0 d'après le lemme 5. D'autre part, $U^*_{(t-u_1)^{-1}} f_{u_1,T_1}(t) U_{(t-u_1)^{-1}} = T_1$. Donc

$$\|g + f_{u_1,T_1} + \cdots + f_{u_n,T_n}\| \geqq \varlimsup_{t \to u_1} \|g(t) + f_{u_1,T_1}(t) + \cdots + f_{u_n,T_n}(t)\| \geqq \|T_1\|.$$

On raisonne de même pour $T_2, T_3, \ldots, T_n$.

Lemme 10. *Tout élément de D' s'écrit de manière unique sous la forme $g + \sum_{u \in \Omega} f_{u,T_u}$, avec $g \in C$, $T_u \in A$, et $T_u = 0$ sauf pour un nombre fini d'indices $u \in \Omega$.*

L'existence d'une telle représentation résulte de la définition même de D'. Supposons maintenant $g + \sum_{u \in \Omega} f_{u,T_u} = g' + \sum_{u \in \Omega} f_{u,T'_u}$ ($g, g' \in C$, $T_u, T'_u \in A$). On a

$$g - g' + \sum_{u \in \Omega} f_{u,T_u - T'_u} = 0.$$

D'après le lemme 9, ceci entraîne $T_u = T'_u$ pour tout u. On a alors $g = g'$.

Lemme 11. *Considérons la somme directe algébrique $\sum_{u \in \Omega} A_u$, où $A_u = A$ pour tout $u \in \Omega$.*

(i) *L'application $g + \sum_{u \in \Omega} f_{u,T_u} \to (T_u)_{u \in \Omega}$ de D' sur $\sum_{u \in \Omega} A_u$ est un homomorphisme d'algèbres involutives dont le noyau est C.*

(ii) *L'isomorphisme de D'/C sur $\sum_{u \in \Omega} A_u$ qu'on en déduit est isométrique is on munit $\sum_{u \in \Omega} A_u$ de la norme $\|(T_u)_{u \in \Omega}\| = \sup_{u \in \Omega} \|T_u\|$.*

On a

$$\lambda\Big(g+\sum_{u\in\Omega}f_{u,T_u}\Big)+\lambda'\Big(g'+\sum_{u\in\Omega}f_{u,T'_u}\Big)=\lambda g+\lambda' g'+\sum_{u\in\Omega}f_{u,\lambda T_u+\lambda' T'_u}$$

$$\Big(g+\sum_{u\in\Omega}f_{u,T_u}\Big)^*=g^*+\sum_{u\in\Omega}f_{u,T_u^*}$$

et, compte tenu des lemmes 6 et 7

$$\Big(g+\sum_{u\in\Omega}f_{u,T_u}\Big)\Big(g'+\sum_{u\in\Omega}f_{u,T'_u}\Big)\in C+\sum_{u\in\Omega}f_{u,T_u}f_{u,T'_u}=C+\sum_{u\in\Omega}f_{u,T_uT'_u}$$

d'où (i).

Rappelons que l'image canonique de $\sum_{u\in\Omega}f_{u,T_u}$ dans D'/C a pour norme $\inf_{g\in C}\Big\|g+\sum_{u\in\Omega}f_{u,T_u}\Big\|$. Ceci posé, le lemme 9 prouve que l'isomorphisme considéré au lemme 11 (ii) diminue les normes. Pour achever la démonstration, il suffit donc d'établir ceci: soient $u_1,\dots,u_n$ des points distincts de Ω, et $T_1,\dots,T_n\in A$; il existe un élément de D' congru modulo C à $f_{u_1,T_1}+\cdots+f_{u_n,T_n}$ et dont la norme est $\sup(\|T_1\|,\dots,\|T_n\|)$. Or soient $V_1,\dots,V_n$ des voisinages de $u_1,\dots,u_n$ dans $[0,1]$ deux à deux disjoints. Pour $i=1,\dots,n$, soit φ_i une fonction continue sur $[0,1]$, à valeurs dans $[0,1]$, nulle hors de V_i, et égale à 1 dans un voisinage de u_i. Alors $\varphi_i f_{u_i,T_i}-f_{u_i,T_i}\in C$ donc $f_{u_1,T_1}+\cdots+f_{u_n,T_n}$ est congru modulo C à $\varphi_1 f_{u_1,T_1}+\cdots+\varphi_n f_{u_n,T_n}$; cette dernière application est nulle hors de $V_1\cup\cdots\cup V_n$, et égale à $\varphi_i f_{u_i,T_i}$ dans V_i; comme $\|f_{u_i,T_i}(t)\|=\|T_i\|$ pour $t\neq u_i$, on a bien $\|\varphi_1 f_{u_1,T_1}+\cdots+\varphi_n f_{u_n,T_n}\|=\sup(\|T_1\|,\dots,\|T_n\|)$. D'où le lemme.

Comme dernière notation, introduisons l'adhérence D de D' dans B. D'après le lemme 8, D est une sous-C^*-algèbre de B, et C est un idéal bilatère fermé de D. La C^*-algèbre D/C est isomorphe à la C^*-algèbre complétée de D'/C, c'est-à-dire, d'après le lemme 11, à la $C^*(\infty)$-somme des $A_u(u\in\Omega)$.

Cherchons $\hat{D}$. D'abord, $\hat{C}=[0,1]$ s'identifie canoniquement à une partie ouverte de $\hat{D}$ ([6], th. 5. 1), d'une manière qu'il est facile d'expliciter: on sait que toute représentation irréductible non nulle $g\to g(t)$ de C se prolonge de manière unique en une représentation irréductible de D, et cette représentation prolongée est évidemment la représentation π_t: $h\to h(t)$. La différence $\hat{D}-\hat{C}$ est une partie fermée de $\hat{D}$ qui s'identifie canoniquement à $(D/C)\hat{}$. D'après l'alinéa précédent, D/C s'identifie à la $C^*(\infty)$-somme des A_u. Donc $(D/C)\hat{}$ s'identifie à l'ensemble Ω muni de la topologie discrète. Ainsi, chaque point $t\in\Omega$ définit un point $\pi'_t\in\hat{D}-\hat{C}$, tel que

$$\pi'_t\Big(g+\sum_{u\in\Omega}f_{u,T_u}\Big)=T_t$$

pour tout élément $g+\sum_{u\in\Omega} f_{u,T_u}$ de D'. On a ainsi déterminé complètement l'ensemble $\hat{D}$ (et partiellement sa topologie), et prouvé en passant que D est une CCR-algèbre.

Lemme 12. *Si H est séparable et Ω dénombrable, D est séparable.*

Les C^*-algèbres A et C sont séparables si H est séparable. Pour tout $u\in\Omega$, l'ensemble des $f_{u,T}$ ($T\in A$) est séparable. Donc, si de plus Ω est dénombrable, il existe dans D un ensemble total dénombrable, de sorte que D est séparable.

Lemme 13. *Soit $t\in\Omega$. Alors, π_t et π_t' n'admettent pas de voisinages disjoints dans $\hat{D}$.*

Soit $(t_1, t_2, \ldots)$ une suite de points de $[0, 1]$ distincts de t et tendant vers t. Alors π_{t_i} tend vers π_t. On va voir que π_{t_i} tend aussi vers π_t', ce qui démontrera le lemme. Il suffit ([5], cor. du th. 3. 1) de prouver que, pour tout $h\in D$, $U^*_{(t_i-t)^{-1}}\pi_{t_i}(h)U_{(t_i-t)^{-1}}$ tend fortement vers $\pi_t'(h)$ quand t_i tend vers t. Et, par continuité et linéarité, il suffit de vérifier ce point dans les cas suivants:

1. $h=f_{t,T}$ avec un $T\in A$. Alors

$$U^*_{(t_i-t)^{-1}}\pi_{t_i}(h)U_{(t_i-t)^{-1}} = U^*_{(t_i-t)^{-1}}h(t_i)U_{(t_i-t)^{-1}} =$$
$$= U^*_{(t_i-t)^{-1}}U_{(t_i-t)^{-1}}TU^*_{(t_i-t)^{-1}}U_{(t_i-t)^{-1}} = T$$

tend fortement vers $T=\pi_t'(h)$.

2. $h\in C$. Alors, d'après le lemme 5, $U^*_{(t_i-t)^{-1}}\pi_{t_i}(h)U_{(t_i-t)^{-1}}$ tend fortement vers $0=\pi_t'(h)$.

3. $h=f_{u,T}$ avec $u\neq t$ et $T\in A$. Soient φ et ψ deux fonctions continues réelles définies sur $[0, 1]$, telles que $\varphi+\psi=1$, φ étant nulle dans un voisinage de t et égale à 1 dans un voisinage de u. Alors $\pi_{t_i}(\varphi h)$ est nul pour i assez grand, donc aussi $U^*_{(t_i-t)^{-1}}\pi_{t_i}(\varphi h)U_{(t_i-t)^{-1}}$. D'autre part, ψ est nulle dans un voisinage de u, donc $\psi h\in C$ (lemme 3), donc $U^*_{(t_i-t)^{-1}}\pi_{t_i}(\psi h)U_{(t_i-t)^{-1}}$ tend fortement vers 0 d'après le lemme 5. Donc $U_{(t_i-t)^{-1}}\pi_{t_i}(h)U_{(t_i-t)^{-1}}$ tend fortement vers $0=\pi_t'(h)$.

Remarque 1. Le lemme 13 prouve que les points π_t et π_t' ($t\in\Omega$) sont non séparés dans $\hat{D}$. Il est facile de voir que les points $\pi_t (t\notin\Omega)$ sont séparés dans Ω.

Proposition 4. (i) *Il existe des CCR-algèbres dont le spectre ne possède aucun point séparé.*

(ii) *Il existe des CCR-algèbres séparables D telles que l'ensemble des points séparés dans $\hat{D}$ soit d'intérieur vide.*

Pour démontrer (i), il suffit de prendre $\Omega = [0, 1]$ dans la construction précédente. Pour démontrer (ii), il suffit de prendre pour Ω, dans la construction précédente, un ensemble dénombrable partout dense dans $[0, 1]$.

Remarque 2. Il est facile de voir que la C^* algèbre D construite plus haut est, non seulement CCR, mais $UCCR$ au sens de [6].

§ 3. Continuité de la trace

Lemme 14. *Soient H un espace hilbertien de dimension infinie, A une C^*-algèbre irréductible d'opérateurs dans H, et n un entier >0. Il existe dans A des éléments hermitiens positifs $T_1 \neq 0, \ldots, T_n \neq 0$ tels que $T_i T_j = 0$ pour $i \neq j$.*

Soit B une sous-C^*-algèbre abélienne maximale de A. Soient S le spectre de B, et p le nombre d'éléments de S. Si p est fini, il existe des projecteurs minimaux $E_1, \ldots, E_p$ de B tels que $E_1 + \cdots + E_p = 1$. Les opérateurs de $E_1 A E_1$ commutent à $E_1, \ldots, E_p$, donc à B, donc sont dans B, donc sont des multiples scalaires de E_1. Comme A est fortement dense dans l'algèbre A' de tous les opérateurs de H, les opérateurs de $E_1 A' E_1$ sont des multiples scalaires de E_1. Donc E_1 est de rang 1, donc $\dim H = p$, ce qui est contradictoire. Donc p est infini. Donc il existe n fonctions continues positives non nulles $\varphi_1, \ldots, \varphi_n$ sur S telles que $\varphi_i \varphi_j = 0$ pour $i \neq j$. D'où le lemme.

Lemme 15. *Soient H un espace hilbertien, A une C^*-algèbre irréductible d'opérateurs dans H, et T un opérateur positif de A. Soit $T = \int_0^{+\infty} \lambda dE_\lambda$ sa décomposition spectrale. On suppose que T est non compact, de sorte qu'il existe un nombre $\alpha > 0$ tel que $T(1 - E_\alpha)$ soit non compact. Soit n un entier >0. Il existe dans A des éléments positifs $T_1 \neq 0, \ldots, T_n \neq 0$ tels que $T_i T_j = 0$ pour $i \neq j$ et $(1 - E_\alpha) T_j (1 - E_\alpha) = T_j$ pour $j = 1, \ldots, n$.*

Soit $\Sigma \subset [0, +\infty[$ le spectre de T. Nous distinguons deux cas.

1. $\Sigma \cap]\alpha, +\infty[$ contient au moins n points distincts. Alors il existe des fonctions continues positives de variables réelles, $\varphi_1, \ldots, \varphi_n$, nulles sur $]-\infty, \alpha]$, telles que $\varphi_i \varphi_j = 0$ pour $i \neq j$, et telles que chaque φ_i soit non nulle en un point de Σ. Il suffit alors de poser $T_j = \varphi_j(T)$.

2. $\Sigma \cap]\alpha, +\infty[$ contient moins de n points distincts. Alors, l'un de ces points, soit $\beta > \alpha$, est valeur propre isolée de multiplicité infinie. Le projecteur propre E correspondant est de la forme $\varphi(T)$, φ étant une fonction continue de variable réelle. Donc $E \in A$. On a $E \leqq 1 - E_\alpha$. D'autre part,

EAE est une C^*-algèbre irréductible dans $E(H)$. Comme $\dim E(H) = +\infty$, on peut appliquer le lemme 14: il existe $S_1, \dots, S_n \in A$ tels que les ES_jE soient des éléments positifs non nuls de A s'annulant deux à deux. Il suffit donc de poser $T_j = ES_jE$.

Lemme 16. *Soient A une C^*-algèbre à élément unité, π_0 un élément de $\hat{A}$, H l'espace de π_0, E un projecteur dans H. On suppose qu'il existe des éléments positifs non nuls $T_1, \dots, T_n$ de $\pi_0(A)$, tels que $T_iT_j = 0$ pour $i \neq j$, et tels que $ET_iE = T_i$. Il existe alors des éléments positifs $x_1, \dots, x_n$ de A possédant les propriétés suivantes:* 1. $x_1 + \cdots + x_n \leqq 1$; 2. $\|\pi_0(x_j)\| \geqq 1$ *pour* $j = 1, \dots, n$; 3. $E\pi_0(x_j)E = \pi_0(x_j)$ *pour* $j = 1, \dots, n$.

En multipliant les T_j par de scalaires, on peut supposer que j appartient au spectre de T_j. Il existe un élément positif x de A tel que $\pi_0(x) = T_1 + \cdots + T_n$. Soient $\varphi_1, \dots, \varphi_n$ des fonctions continues de variable réelle possédant les propriétés suivantes: 1. $0 \leqq \varphi_j(t) \leqq 1$ pour tout j et tout t; 2. $\varphi_j(j) = 1$; 3. $\varphi_i\varphi_j = 0$ pour $i \neq j$. Soit $x_j = \varphi_j(x) \in A$. Alors les x_j sont positifs. On a $(\varphi_1 + \cdots + \varphi_n)(t) \leqq 1$ pour tout t, donc $x_1 + \cdots + x_n \leqq 1$. D'autre part, $\pi_0(x_j) = \varphi_j(\pi_0(x)) = \varphi_j(T_1 + \cdots + T_n)$. Comme les T_j s'annulent deux à deux, cet opérateur est encore égal à $\varphi_j(T_1) + \cdots + \varphi_j(T_n)$. Il est donc clair que $E\pi_0(x_j)E = \pi_0(x_j)$. Enfin, comme les T_j s'annulent deux à deux, $\varphi_j(T_1) + \cdots + \varphi_j(T_n) \geqq \varphi_j(T_j)$, et le spectre de $\varphi_j(T_j)$ contient $\varphi_j(j) = 1$; donc $\|\pi_0(x_j)\| \geqq 1$.

Proposition 5. *Soient A une C^*-algèbre, x un élément positif de A. La fonction $\pi \to \mathrm{Tr}\,\pi(x)$ est semi-continue inférieurement sur $\hat{A}$.*

On peut supposer que A admet un élément unité. Soit $\pi_0 \in \hat{A}$. Montrons que la fonction considérée est semi-continue inférieurement en π_0. Désignons par H l'espace de π_0. Nous distinguerons plusieurs cas.

1. $\pi_0(x)$ est un projecteur de rang fini n dans H, soit E. Soient $T_1, \dots, T_n$ des projecteurs de rang 1, deux à deux orthogonaux, de somme E. Comme $\pi_0(A)$ est irréductible dans H, l'algèbre $E\pi_0(A)E$ est irréductible dans $E(H)$, donc se compose de tous les opérateurs linéaires T dans H tels que $ETE = T$. En particulier, $T_1, \dots, T_n \in \pi_0(A)$. D'après le lemme 16, il existe des éléments positifs $x_1, \dots, x_n$ de A tels que $x_1 + \cdots + x_n \leqq 1$, $\|\pi_0(x_i)\| \geqq 1$, $E\pi_0(x_i)E = \pi_0(x_i)$. Alors $x \geqq x^{1/2}(x_1 + \cdots + x_n)x^{1/2}$, et

$$\|\pi_0(x^{1/2}x_ix^{1/2})\| = \|E\pi_0(x_i)E\| = \|\pi_0(x_i)\| \geqq 1.$$

Soit $\varepsilon > 0$. Il existe un voisinage V de π_0 dans $\hat{A}$ tel que, pour $\pi \in V$, on ait

$$\|\pi(x^{1/2}x_1x^{1/2})\| \geqq 1 - \varepsilon, \dots, \|\pi(x^{1/2}x_nx^{1/2})\| \geqq 1 - \varepsilon.$$

Pour $\pi \in V$, on a donc

$$\mathrm{Tr}\,\pi(x) \geqq \sum_{j=1}^{n} \mathrm{Tr}\,\pi(x^{1/2}x_j x^{1/2}) \geqq \sum_{j=1}^{n} \|\pi(x^{1/2}x_j x^{1/2})\| \geqq n - n\varepsilon = \mathrm{Tr}\,\pi_0(x) - n\varepsilon$$

d'où notre assertion dans ce cas.

2. $\pi_0(x)$ est de rang fini. Les projecteurs spectraux de $\pi_0(x)$ sont alors de la forme $\varphi(\pi_0(x))$, où φ est une fonction continue positive de variable réelle. Donc il existe des éléments positifs $x_1, \ldots, x_n$ de A et des nombres positifs $\lambda_1, \ldots, \lambda_n$, tels que $x = \lambda_1 x_1 + \cdots + \lambda_n x_n$, et tels que $\pi_0(x_1), \ldots, \pi_0(x_n)$ soient des projecteurs de rang fini. Il suffit alors d'appliquer la partie 1. de la démonstration.

3. $\pi_0(x)$ est compact. Soit $(\varphi_1, \varphi_2, \ldots)$ une suite de fonctions continues positives de variable réelle possédant les propriétés suivantes: a) $\varphi_1 \leqq \varphi_2 \leqq \ldots$; b) $\varphi_n(t)$ tend uniformément vers t sur le spectre de x; c) $\varphi_n(t) = 0$ pour $t \leqq 1/n$. Pour chaque n, $\pi_0(\varphi_n(x)) = \varphi_n(\pi_0(x))$ est de rang fini d'après la propriété c) et le fait que $\pi_0(x)$ est compact. Donc, d'après la partie 2. de la démonstration, la fonction $\pi \to \mathrm{Tr}\,\pi(\varphi_n(x))$ est semi-continue inférieurement en π_0. D'autre part, pour chaque π, $\mathrm{Tr}\,\pi(\varphi_n(x)) = \mathrm{Tr}\,\varphi_n(\pi(x))$ tend en croissant vers $\mathrm{Tr}\,\pi(x)$ d'après les propriétés a) et b) des φ_n. Donc la fonction $\pi \to \mathrm{Tr}\,\pi(x)$ est semi-continue inférieurement en π_0.

4. $\pi_0(x)$ est non compact. Soit $\pi_0(x) = \int_0^{+\infty} \lambda\, dE_\lambda$ la décomposition spectrale de $\pi_0(x)$. Il existe un nombre $\alpha > 0$ tel que $\pi_0(x)(1 - E_\alpha)$ soit non compact. Soit n un entier > 0. Il existe (lemme 15) des éléments positifs $T_1, \ldots, T_n$ de $\pi_0(A)$, avec $T_1, \ldots, T_n \neq 0$, $T_i T_j = 0$ pour $i \neq j$, $(1 - E_\alpha) T_i (1 - E_\alpha) = T_i$. Donc (lemme 16) il existe des éléments positifs $x_1, \ldots, x_n$ de A tels que $x_1 + \cdots + x_n \leqq 1$, $\|\pi_0(x_i)\| \geqq 1$, $(1 - E_\alpha)\pi_0(x_i)(1 - E_\alpha) = \pi_0(x_i)$. Alors $x \geqq x^{1/2} \cdot (x_1 + \cdots + x_n) x^{1/2}$. D'autre part, il existe $\xi \in (1 - E_\alpha)(H)$ tel que $\|\pi_0(x_i)\xi\| \geqq \frac{1}{2}\|\xi\| > 0$; il existe aussi $\eta \in (1 - E_\alpha)(H)$ tel que $\xi = \pi_0(x)^{1/2}\eta$ et $0 < \|\eta\| \leqq \alpha^{-1/2}\|\xi\|$; notons que $\pi_0(x_i)\xi \in (1 - E_\alpha)(H)$, d'où

$$\|\pi_0(x^{1/2}x_i x^{1/2})\eta\| = \|\pi_0(x)^{1/2}\pi_0(x_i)\xi\| \geqq \alpha^{1/2}\|\pi_0(x_i)\xi\| \geqq \tfrac{1}{2}\alpha^{1/2}\|\xi\| \geqq \tfrac{1}{2}\alpha\|\eta\|.$$

Donc $\|\pi_0(x^{1/2}x_i x^{1/2})\| \geqq \frac{1}{2}\alpha$. Par suite il existe un voisinage V de π_0 dans $\hat{A}$ tel que, pour $\pi \in V$, on ait

$$\|\pi(x^{1/2}x_1 x^{1/2})\| \geqq \tfrac{1}{4}\alpha, \ldots, \|\pi(x^{1/2}x_n x^{1/2})\| \geqq \tfrac{1}{4}\alpha.$$

Pour $\pi \in V$, on a donc

$$\mathrm{Tr}\,\pi(x) \geqq \sum_{j=1}^{n} \mathrm{Tr}\,\pi(x^{1/2}x_j x^{1/2}) \geqq \sum_{j=1}^{n} \|\pi(x^{1/2}x_j x^{1/2})\| \geqq \tfrac{1}{4}\alpha n.$$

Vu l'arbitraire de n, ceci prouve que $\mathrm{Tr}\,\pi(x) \to +\infty = \mathrm{Tr}\,\pi_0(x)$ quand $\pi \to \pi_0$. Ceci achève la démonstration de la proposition 5.

Lemme 17. *Soient A une C^*-algèbre, π un point séparé de $\hat{A}$, et e un projecteur de $\pi(A)$. Il existe un élément positif x de A tel que $\pi(x) = e$ et tel que $\pi'(x)$ soit un projecteur pour tous les π' d'un voisinage de π.*

Le raisonnement qui suit est bien connu. Il existe $y \in A$ tel que $\pi(y) = e$. Remplaçant y par y^*y, on peut supposer que $y \geqq 0$. Comme π est séparé, il existe un voisinage V de π tel que, pour $\pi' \in V$, le spectre de $\pi'(y)$ soit contenu dans $]-\frac{1}{4}, \frac{1}{4}[\cup]\frac{3}{4}, \frac{5}{4}[$. Soit φ une fonction continue $\geqq 0$ de variable réelle égale à 0 sur $]-\frac{1}{4}, \frac{1}{4}[$ et à 1 sur $]\frac{3}{4}, \frac{5}{4}[$. Alors $\varphi(y) \geqq 0$, $\pi(\varphi(y)) = \varphi(\pi(y)) = \varphi(e) = e$, et, pour $\pi' \in V$, le spectre de $\pi'(\varphi(y)) = \varphi(\pi'(y))$ est contenu dans $\{0\} \cup \{1\}$, donc $\pi'(\varphi(y))$ est un projecteur.

Lemme 18. *Soient A une C^*-algèbre, π un point séparé de $\hat{A}$, e_1 et e_2 deux projecteurs de rang 1 dans $\pi(A)$. Soient x_1, x_2 deux éléments positifs de A tels que $\pi(x_1) = e_1$, $\pi(x_2) = e_2$ et tels que $\pi'(x_i)$ soit un projecteur pour tous les π' d'un voisinage de π (il existe de tels éléments d'après le lemme 17). Alors $\pi'(x_1)$ et $\pi'(x_2)$ ont même rang pour tous les π' d'un voisinage de π.*

L'algèbre irréductible $\pi(A)$ contient un opérateur compact non nul (par exemple e_1) donc contient tous les opérateurs compacts. Donc il existe un $a \in \pi(A)$ tel que $a^*a = e_1$, $aa^* = e_2$. Il suffit alors d'appliquer mot pour mot le raisonnement de [6], lemme 4.13 (raisonnement qui utilise à deux reprises la continuité de la norme en π).

Soient X un espace topologique, ζ un point de X. Considérons l'ensemble E des fonctions réelles définies dans un voisinage (variable) de ζ. La relation „f_1 et f_2 sont égales dans un voisinage de ζ" est une relation d'équivalence dans E. Rappelons qu'une classe suivant cette relation d'équivalence s'appelle un *germe* de fonction réelle en ζ. Ceci posé, soient A une GCR-algèbre, π un point séparé de $\hat{A}$. Alors $\pi(A)$ contient l'ensemble des opérateurs compacts donc tous les projecteurs de rang 1. Soit e un tel projecteur. Soit x un élément positif de A avec les propriétés du lemme 17. La fonction $\pi' \to \mathrm{rang}\,(\pi'(x))$ définit *un germe de fonction à valeurs entières $\geqq 1$ en π*, et ce germe est, d'après le lemme 18, indépendant des choix de e et de x. Ce germe sera noté γ_π.

Proposition 6. *Soient A une GCR-algèbre, S l'intérieur de l'ensemble des points séparés de $\hat{A}$, et S' l'ensemble des $\pi \in S$ tels que le germe γ_π soit égal au germe de la constante* 1.

(i) *S' est ouvert et partout dense dans S.*

(ii) *Soit $\pi \in S'$. Soit y un élément de A tel que le rang de $\pi'(y)$ soit borné dans un voisinage de π. Alors la fonction $\pi' \to \operatorname{Tr} \pi'(y)$ est continue en π.*

Il est clair que S' est ouvert. D'autre part, soit U une partie ouverte non vide de S. D'après [6], th. 6.2, U contient une partie ouverte non vide U' telle que l'idéal bilatère fermé correspondant I de A soit une C^*-algèbre à trace continue. Pour tout $\pi \in U'$, il existe un élément positif $x \in I$ tel que $\pi'(x)$ soit un projecteur de rang 1 pour tout π' d'un voisinage de π. Donc $U' \subset S'$, ce qui prouve que S' est partout dense dans S.

Soient $\pi \in S'$, et x un élément de A tel que le rang de $\pi'(x)$ soit borné par n dans un voisinage de π. Montrons que la fonction $\pi' \to \operatorname{Tr} \pi'(x)$ est continue en π. Par linéarité, on se ramène au cas où x est hermitien. Il existe alors des éléments $x_1, \ldots, x_n$ de A possédant les propriétés suivantes: 1. $\pi(x_1), \ldots, \pi(x_n)$ sont des projecteurs de rang 1 et $\pi(x) = \sum_{i=1}^{n} \lambda_i \pi(x_i)$ (où les λ_i sont des nombres réels); 2. $\pi'(x_1), \ldots, \pi'(x_n)$ sont des projecteurs dans un voisinage de π. Comme $\gamma_\pi = 1$, le rang de $\pi'(x_1), \ldots, \pi'(x_n)$ est 1 dans un voisinage V de π. On a $\pi\left(x - \sum_{i=1}^{n} \lambda_i x_i\right) = 0$. Donc, pour tout $\varepsilon > 0$, il existe un voisinage V' de π tel que $\left\| \pi'\left(x - \sum_{i=1}^{n} \lambda_i x_i\right) \right\| \leqq \varepsilon$ pour $\pi' \in V'$. Alors, pour $\pi' \in V \cap V'$,

$$|\operatorname{Tr} \pi'(x) - \operatorname{Tr} \pi(x)| =$$

$$= \left| \operatorname{Tr} \pi'(x) - \sum_{i=1}^{n} \lambda_i \right| = \left| \operatorname{Tr} \pi'(x) - \operatorname{Tr} \sum_{i=1}^{n} \lambda_i \pi'(x_i) \right| = \left| \operatorname{Tr} \pi'\left(x - \sum_{i=1}^{n} \lambda_i x_i\right) \right| \leqq n\varepsilon$$

ce qui prouve la proposition.

Remarque 3. La prop. 6 est à rapprocher de [4], th. 2.2, et de [6], lemme 5.15 et th. 6.1. D'ailleurs, tout ce paragraphe s'inspire directement des articles de Fell. Toutefois, la proposition ne semble pas découler directement des résultats cités.

Remarque 4. Prenons pour A la C^*-algèbre du groupe de Lie nilpotent noté Γ_3 dans [2]. On sait que A est une CCR-algèbre. Dans $\hat{A} = \hat{\Gamma}_3$, l'ensemble des points séparés est une partie ouverte partout dense. Il est facile de voir que: 1. avec les notations de la prop. 6, on a $S' = S$; 2. cependant, pour tout $\pi \in S$, il existe des x appartenant à A, et même a $L^1(\Gamma_3)$, tels que la fonction $\pi' \to \operatorname{Tr}(\pi'(x^* x))$ soit discontinue en π.

Par ailleurs, l'exemple suivant le th. 2.2 de [4] prouve que, même pour $\hat{A}$ séparé (donc $\hat{A} = S$), S' peut être distinct de S.

Bibliographie

[1] P. Bernat et J. Dixmier, Sur le dual d'un groupe de Lie, *C. R. Acad. Sci. Paris*, **250** (1960), 1778—1779.

[2] J. Dixmier, Sur les représentations unitaires des groupes de Lie nilpotents. VI, *Canadian J. Math.*, **12** (1960), 324—352.

[3] J. Dixmier, Sur les C^*-algèbres, *Bull. Soc. Math. France*, **88** (1960), 95—112.

[4] J. M. G. Fell, The dual spaces of C^*-algebras, *Transactions Amer. Math. Soc.*, **94** (1960), 365—403.

[5] J. M. G. Fell, C^*-algebras with smooth dual, *Illinois J. Math.*, **4** (1960), 221—230.

[6] J. M. G. Fell, The structure of algebras of operator fields. (A paraître.)

[7] I. Kaplansky, The structure of certain operator algebras, *Transactions Amer. Math. Soc.*, **70** (1951), 219—255.

(Reçu le 7 avril 1960)

Zur Frage der Approximation durch orthonormierte Polynomsysteme

Von LÁSZLÓ LEINDLER in Szeged

In einem vorigen Aufsatz hat Verfasser u. a. Folgendes bewiesen[1]):

Es sei $\{\varphi_n(x)\}$ $(n=1,2,\ldots)$ *ein im Intervall* (a, b) *orthonormiertes Funktionensystem.*[2]) *Dann kann man zu jeder positiven Zahlenfolge* $\{\varepsilon_n\}$ *ein in* (a, b) *orthonormiertes Polynomsystem* $\{P_n(x)\}$ *und eine Folge von meßbaren Mengen* G_n *in* (a, b) *derart angeben, daß*

$$\mu(G_n) \leqq \varepsilon_n \qquad (n=1,2,\ldots)$$

und für jedes $x \in CG_n$[3])

$$|\varphi_n(x)-(-1)^{j_n(x)}P_n(x)| \leqq \varepsilon_n \qquad (\textit{mit } j_n(x)=0 \textit{ oder } 1)$$

gilt $(n=1,2,\ldots)$.

Also können die Absolutbeträge der Glieder eines orthonormierten Funktionensystems, außer einer Menge von beliebig kleinem Maß, mit beliebiger Genauigkeit durch die Absolutbeträge der entsprechenden Glieder eines orthonormierten Polynomsystems approximiert werden.

Wir beweisen nun, daß dieser Satz nicht derart verschärft werden kann, daß die Funktionswerte selbst und nicht nur ihre Absolutbeträge approximiert werden; es gilt nämlich der folgende

Satz. *Es gibt ein im Intervall* $(0, 1)$ *orthonormiertes Funktionensystem* $\{\Phi_n(x)\}$ $(n=1,2,\ldots)$ *und eine positive Zahlenfolge* $\{\varepsilon_n\}$ *derart, daß für kein im Intervall* $(0, 1)$ *orthonormiertes Polynomsystem* $\{P_n(x)\}$ *und für keine Folge*

---

[1]) L. LEINDLER, Über die orthogonalen Polynomsysteme, *Acta Sci. Math.*, **21** (1960), 19—46.

[2]) In dieser Arbeit betrachten wir nur *reellwertige* Funktionen auf einem *endlichen* Intervall (a, b).

[3]) CH bezeichnet immer die Komplementärmenge der Menge H in bezug auf das jeweils betrachtete Grundintervall (a, b). Mit $\mu(H)$ wird das Lebesguesche Maß der Menge H bezeichnet.

von meßbaren Mengen E_n in $(0, 1)$ die Bedingungen

$$\mu(E_n) \leqq \varepsilon_n \qquad (n = 1, 2, \ldots) \tag{1}$$

und

$$|\Phi_n(x) - P_n(x)| \leqq \varepsilon_n \quad \textit{für} \quad x \in CE_n \qquad (n = 1, 2, \ldots) \tag{2}$$

erfüllt sind.

Beweis. Wir definieren ein orthonormiertes Funktionensystem $\{\varphi_n(x)\}$ im Intervall $(-1, 1)$ und eine Indexfolge $\{n_k\}$ folgenderweise:

$$\varphi_n(x) = \begin{cases} 2^{\frac{1}{2}(n+1)} & \text{für } \dfrac{2^{n-1}-1}{2^n} < x < \dfrac{2^n-1}{2^{n+1}}, \\ 0 & \text{sonst,} \end{cases}$$

$n_1 = 1$, und $n_{k+1} - n_k = k$ $(k = 1, 2, \ldots)$.

Dann definieren wir mittels dieses Funktionensystems das Funktionensystem $\{\Phi_n(x)\}$ $(n = 1, 2, \ldots)$ folgenderweise:

$$\Phi_{n_k+m}(x) = \varphi_k(x - (2^{-2} + 2^{-3} + \cdots + 2^{-(m+1)}))$$
$$(0 < x < 1;\ k = 1, 2, \ldots;\ m = 0, 1, \ldots, k-1).$$

Aus der Definition ist es klar, daß die Funktionen $\Phi_n(x)$ $(n = 1, 2, \ldots)$ ein orthonormiertes System im Intervall $(0, 1)$ bilden und die Funktionen $\Phi_{n_k+m}(x)$ $(k = 1, 2, \ldots;\ m = 0, 1, \ldots, k-1)$ im Intervall (c_{n_k+m}, d_{n_k+m}) positiv und sonst gleich Null sind, wobei $c_{n_k+m} = (2^{k-1}-1)2^{-k} + 2^{-2} + 2^{-3} + \cdots + 2^{-(m+1)}$ und $d_{n_k+m} = (2^k-1)2^{-(k+1)} + 2^{-2} + 2^{-3} + \cdots + 2^{-(m+1)}$ ist. Für m fest und $k \to \infty$ konvergieren die Punkte c_{n_k+m} und d_{n_k+m} gegen den Punkt $x_m = (2^{m+1}-1)2^{-(m+1)}$.

Es sei $\{P_n(x)\}$ $(n = 1, 2, \ldots)$ ein beliebiges normiertes (nicht notwendigerweise orthogonales) Polynomsystem in $(0, 1)$ und $\{\varepsilon_n\}$ eine positive Zahlenfolge mit $\varepsilon_n = M_n^{-6}$, wobei $M_n = \max_{0<x<1} \Phi_n(x)$ ist.

Dann gibt es zu jeder natürlichen Zahl l eine von l abhängige Indexfolge $\{n_k(l)\}$ $(k = 1, 2, \ldots)$ derart, daß

$$|\varrho^l_{n_k(l)}| \varepsilon^{-1/3}_{n_k(l)} \to \infty \qquad (k \to \infty) \tag{3}$$

gilt, wobei

$$\varrho^l_n = \int_0^1 P_l(x)\, \Phi_n(x)\, dx$$

ist.

Da $P_l(x)$ nur endlich viele Nullstellen besitzt, so gibt es eine solche natürliche Zahl $m(l)$, für die der Punkt $x_{m(l)} = (2^{m(l)+1}-1)2^{-(m(l)+1)}$ keine Nullstelle des Polynoms $P_l(x)$ ist. Dann gibt es auch eine Umgebung des Punktes $x_{m(l)}$, in der $|P_l(x)| \geqq \alpha_{m(l)} > 0$ ist.

Wir betrachten jetzt die Teilfolge $\{\Phi_{n_k+m(l)}(x)\}$ $(k=m(l)+1, m(l)+2, \ldots)$ unseres Funktionensystems. Für genügend großes k ist das Intervall $(c_{n_k+m(l)}, d_{n_k+m(l)})$ in der genannten Umgebung des Punktes $x_{m(l)}$ enthalten, und so gilt

$$|\varrho^l_{n_k+m(l)}| = \Big|\int_0^1 P_l(x)\,\Phi_{n_k+m(l)}(x)dx\Big| = \Big|\int_{c_{n_k+m(l)}}^{d_{n_k+m(l)}} P_l(x)2^{\frac{1}{2}(k+1)}dx\Big| \geqq \alpha_{m(l)}2^{-\frac{1}{2}(k+1)}.$$

Wir setzen $n_k(l)=n_k+m(l)$. Dann ist

$$|\varrho^l_{n_k(l)}|\varepsilon^{-1/3}_{n_k(l)} \geqq \alpha_{m(l)}2^{-\frac{1}{2}(k+1)}2^{k+1} = \alpha_{m(l)}2^{\frac{1}{2}(k+1)} \to \infty \qquad (k\to\infty).$$

Damit haben wir die Behauptung (3) bewiesen.

Wir nehmen jetzt an, daß es zu unserem Funktionensystem $\{\Phi_n(x)\}$ und zur obigen Folge $\{\varepsilon_n\}$ ein im Intervall $(0, 1)$ orthonormiertes Polynomsystem $\{P_n(x)\}$ und eine Folge von meßbaren Mengen E_n in $(0, 1)$ gibt, für die (1) und (2) erfüllt sind.

Die Behauptung (3) gilt dann auch für dieses orthonormierte Polynomsystem $\{P_n(x)\}$. Andererseits gilt für $l\neq n_k(l)$ $(k=m(l)+1, m(l)+2, \ldots)$:

$$|\varrho^l_{n_k(l)}| = \Big|\int_0^1 P_l(x)\big(\Phi_{n_k(l)}(x)-P_{n_k(l)}(x)\big)dx\Big| \leqq$$

$$\leqq \Big\{\Big(\int_{CE_{n_k(l)}} + \int_{E_{n_k(l)}}\Big)\big(\Phi_{n_k(l)}(x)-P_{n_k(l)}(x)\big)^2dx\Big\}^{1/2} \leqq$$

$$\leqq \varepsilon_{n_k(l)} + \Big\{2\int_{E_{n_k(l)}} \Phi^2_{n_k(l)}(x)dx + 2\int_{E_{n_k(l)}} P^2_{n_k(l)}(x)dx\Big\}^{1/2}.$$

Es gelten ferner die Abschätzungen

$$\int_{E_n} \Phi^2_n(x)dx \leqq \varepsilon_n M_n^2 \quad \text{und} \quad \int_{E_n} P^2_n(x)dx \leqq \varepsilon_n(M_n^2+2).$$

Die erste ist klar und die zweite folgt durch eine einfache Rechnung:

$$\int_{E_n} P^2_n(x)dx = 1-\int_{CE_n} P^2_n(x)dx \leqq 1-\int_{CE_n}(\Phi_n(x)-\varepsilon_n)^2dx+\varepsilon_n^2 < 1-$$

$$-\Big(\int_{CE_n}\Phi^2_n(x)dx - 2\varepsilon_n\int_{CE_n}\Phi_n(x)dx\Big)+\varepsilon_n^2 =$$

$$= 1-\Big(1-\int_{E_n}\Phi^2_n(x)dx-2\varepsilon_n\int_{CE_n}\Phi_n(x)dx\Big)+\varepsilon_n^2 < \varepsilon_n M_n^2+2\varepsilon_n = \varepsilon_n(M_n^2+2).$$

Daraus folgt

$$|\varrho^{l}_{n_{l_k(l)}}| \leqq 5 M^{-2}_{n_{k(l)}} = 5 \varepsilon^{1/3}_{n_{k(l)}},$$

im Widerspruch zu (3).

Aus diesem Wiederspruch folgt die Richtigkeit des Satzes.

(Eingegangen am 16. April 1960)

Bemerkung zu einem Satz von A. N. Kolmogoroff

Von KÁROLY TANDORI in Szeged

Es sei $\{\varphi_n(x)\}$ ein im Grundintervall $[a, b]$ orthonormiertes Funktionensystem und $\{a_n\}$ eine Koeffizientenfolge mit $\sum_{n=0}^{\infty} a_n^2 < \infty$. A. N. KOLMOGOROFF hat den folgenden Satz bewiesen[1]):

Ist die Orthogonalreihe

$$\sum_{n=0}^{\infty} a_n \varphi_n(x) \tag{1}$$

fast überall $(C, 1)$*-summierbar, so ist die Folge* $\{s_{2^n}(x)\}$ *fast überall konvergent, wo* $s_n(x)$ *die n-te Partialsumme der Reihe* (1) *bezeichnet.*

In dieser Note werden wir den folgenden Satz beweisen.

Satz. *Es sei* $N(\geqq 1)$ *eine beliebig angegebene natürliche Zahl. Mit* $\{n_k\}$ *wird die (wachsend angeordnete) Folge derjenigen natürlichen Zahlen bezeichnet, die in der Form* $2^{\nu_1} \pm 2^{\nu_2} \pm \cdots \pm 2^{\nu_r}$ *mit ganzzahligen Exponenten* $\nu_1 > \cdots > \nu_r \geqq 0$ $(1 \leqq r \leqq N)$ *geschrieben werden können. Sind die Bedingungen*

$$c_n \geqq c_{n+1} (> 0) \qquad (n = 0, 1, \ldots), \tag{2}$$

$$\sum_{n=0}^{\infty} c_n^2 < \infty \tag{3}$$

und

$$a_n = O(c_n) \tag{4}$$

erfüllt, und ist die Reihe (1) *fast überall* $(C, 1)$*-summierbar, so konvergiert die Folge* $\{s_{n_k}(x)\}$ *fast überall.*

Beweis. Für $N = 1$ ist die Behauptung auf Grund des erwähnten Satzes von A. N. KOLMOGOROFF richtig.

---

[1]) A. N. KOLMOGOROFF, Une contribution à l'étude de la convergence des séries de Fourier, *Fundamenta Math.*, **5** (1924), 96—97.

Es sei $p(\geqq 1)$ eine natürliche Zahl. Nehmen wir an, daß für $N=p$ die Behauptung schon bewiesen ist; die entsprechende Indexfolge wird mit $\{n_k\}$ bezeichnet $(1=n_0<\cdots<n_k<\cdots)$. Es sei

$$\delta_k^2(x)=\sum_{i=0}^{\log(n_{k+1}-n_k)-1}(s_{n_k+2^i}(x)-s_{n_k}(x))^2 \qquad (k=1,2,\ldots).$$

Auf Grund von (2) und (4) ergibt sich

$$\int_a^b \delta_k^2(x)dx=O(1)\sum_{i=0}^{\log(n_{k+1}-n_k)-1}(c_{n_k+1}^2+\cdots+c_{n_k+2^i}^2)=$$

$$=O(1)c_{n_k}^2\sum_{i=0}^{\log(n_{k+1}-n_k)-1}2^i=O(1)c_{n_k}^2(n_{k+1}-n_k).$$

Da $n_{k+1}\leqq 2n_k$ $(k=1,2,\ldots)$ ist, so gilt nach (2) und (3)

$$\sum_{k=1}^{\infty}\int_a^b \delta_k^2(x)dx=O(1)\sum_{k=1}^{\infty}c_{n_k}^2 n_k=O(1)\sum_{k=0}^{\infty}c_k^2<\infty.$$

Durch Anwendung des Satzes von B. Levi ergibt sich

$$\sum_{k=1}^{\infty}\delta_k^2(x)<\infty$$

fast überall, also gilt fast überall $\delta_k(x)\to 0$. Wegen

$$|s_{n_k+2^i}(x)-s_{n_k}(x)|\leqq\delta_k(x)$$

ergibt sich auf Grund der Induktionsannahme, daß die Folge $\{s_{n_k+2^i}(x)\}$ $(0\leqq i<\log(n_{k+1}-n_k);\ k=1,2,\ldots)$ fast überall konvergiert.

Es sei weiterhin

$$\bar{\delta}_k^2(x)=\sum_{i=0}^{\log(n_{k+1}-n_k)-1}(s_{n_{k+1}}(x)-s_{n_{k+1}-2^i}(x))^2 \qquad (k=0,1,\ldots);$$

Auf Grund von (2) und (4) gilt:

$$\int_a^b \bar{\delta}_k^2(x)dx=O(1)\sum_{i=0}^{\log(n_{k+1}-n_k)-1}(c_{n_{k+1}-2^i+1}^2+\cdots+c_{n_{k+1}}^2)=$$

$$=O(1)c_{n_k}^2\sum_{i=0}^{\log(n_{k+1}-n_k)-1}2^i=O(c_{n_k}^2 n_k),$$

und es ergibt sich wie oben $\bar{\delta}_k(x)\to 0$ fast überall. Da

$$|s_{n_{k+1}}(x)-s_{n_{k+1}-2^i}(x)|\leqq\delta_k(x) \qquad (0\leqq i<\log(n_{k+1}-n_k);\quad k=0,1,\ldots)$$

überall gilt, so ergibt sich, daß die Folge $\{s_{n_{k+1}-2^i}(x)\}$ $(0 \leqq i < \log(n_{k+1}-n_k);$ $k=0,1,\ldots)$ fast überall konvergiert. Also gilt die Behauptung auch für $N=p+1$.

Damit haben wir die Behauptung bewiesen.

(Eingegangen am 23. März 1960)

Verbandstheoretische Betrachtung gewisser idealtheoretischer Fragen

Von O. STEINFELD in Budapest

§ 1. Einleitung

Es ist bekannt, daß die Menge aller Teilringe eines assoziativen Ringes eine multiplikative Halbgruppe und zugleich einen vollständigen Durchschnittshalbverband L bildet, in dem auch gewisse andere Bedingungen gelten. (Siehe (1)—(4).) Dem entsprechend definieren wir eine H-Halbgruppe L als eine multiplikative Halbgruppe und einen vollständigen Durchschnittshalbverband mit den Eigenschaften (1)—(4). Unser Zweck ist Ergebnisse über die H-Halbgruppen zu beweisen, aus denen neue oder bekannte idealtheoretische Sätze folgen.

In unseren Untersuchungen spielen die Absorbenten, die Primabsorbenten, die Halb-Primabsorbenten und die Absorbentenquotienten eine wichtige Rolle. Diese Begriffe kommen durch die Abstraktion der Begriffe des Ideals, des Primideals, des Halb-Primideals und der Idealquotienten zustande.

In § 2 beweisen wir einen Satz über die Absorbenten eines Elementes einer H-Halbgruppe, der eine Verallgemeinerung eines bekannten Satzes über die Ideale eines Ringes ist.

In Lemma 1 geben wir eine Eigenschaft der Primabsorbenten, aus der sich ergibt, daß ein Primideal eines Ringes R nicht nur bezüglich der Ideale von R, sondern auch bezüglich der Ideale der Ideale von R „prim“ ist. Mit Hilfe von Lemma 1 bekommt man leicht das Ergebnis von McCoy, daß der Durchschnitt eines Ideals A und eines Primideals P eines Ringes ein Primideal von A ist.

Über die Absorbentenquotienten beweisen wir einige Sätze, aus denen als Spezialfall die Hauptresultate unserer früheren Arbeit über die Primideale und Idealquotiente folgen.

In § 5 definieren wir eine Radikalklasse in den H-Halbgruppen als einen Durchschnitt gewisser Primabsorbenten. In diese Radikalklasse gehören z. B.

das Brown—McCoysche, Fuchssche, Jacobsonsche und Krull—McCoysche Radikal eines assoziativen Ringes. Wir beweisen eine allgemeine Formel über diese Radikale, die die Bestimmung des Radikals eines Ringes R mit Hilfe des Radikals eines Ideals von R ermöglicht.

§ 2. Grundbegriffe

Es sei $L = \{a, b, \ldots\}$ eine multiplikative Halbgruppe und ein vollständiger Halbverband bezüglich der Durchschnittsoperation $\cap$.

Man kann in L durch

$$a \leqq b \Longleftrightarrow a \cap b = a \qquad (a, b \in L) \tag{1}$$

eine Halbordnungsrelation $\leqq$ definieren. Es gelte

$$a^2 \leqq a \qquad (a \in L), \tag{2}$$

$$\left(\bigcap_{\omega\in\Omega} a_\omega\right) b \leqq \bigcap_{\omega\in\Omega} a_\omega b \quad \text{und} \quad b\left(\bigcap_{\omega\in\Omega} a_\omega\right) \leqq \bigcap_{\omega\in\Omega} b a_\omega \qquad (a_\omega, b \in L), \tag{3}$$

wo Ω eine beliebige Indexmenge bezeichnet. Wir verlangen endlich die Existenz der Elemente 0, $e(\in L)$ mit den Bedingungen

$$0 \leqq x \leqq e \quad \text{und} \quad 0x = x0 = 0 \qquad (x \in L). \tag{4}$$

Eine algebraische Struktur L mit den obigen Eigenschaften wird eine *H-Halbgruppe* genannt. Mit L bezeichnen wir immer eine H-Halbgruppe.

Aus (1) und (3) folgt:

$$a \leqq b \Longrightarrow ax \leqq bx \quad \text{und} \quad xa \leqq xb \qquad (a, b, x \in L). \tag{5}$$

Wir sagen, daß das Element $b(\in L)$ ein *Absorbent* eines Elementes $a(\in L)$ ist, wenn

$$b \leqq a; \quad ba \leqq b, \quad ab \leqq b \tag{6}$$

bestehen.

Aus (4) sieht man, daß das Element 0 ein Absorbent jedes Elementes von L ist. Wegen (2) ist jedes Element ein Absorbent von sich selbst. Ist b ein Absorbent des Elementes $a(\in L)$, so sind $a \cap b, ab, ba$ und aba Absorbenten von b.

Satz 1. *Die Teilmenge A von L, die aus allen Absorbenten eines Elementes $a(\in L)$ besteht, ist eine H-Teilhalbgruppe von L. Man kann in A derart auch eine Vereinigungsoperation $\cup$ definieren, daß dann A einen vollständigen Verband bezüglich der Verknüpfungen $\cap$ und $\cup$ bildet, in dem auch*

$$b\left(\bigcup_{\omega\in\Omega} a_\omega\right) \geqq \bigcup_{\omega\in\Omega} b a_\omega, \quad \left(\bigcup_{\omega\in\Omega} a_\omega\right) b \geqq \bigcup_{\omega\in\Omega} a_\omega b \qquad (a_\omega, b \in A) \tag{7}$$

und

$$a_1 \cdots a_k \leqq a_1 \cap \cdots \cap a_k \qquad (a_1, \ldots, a_k \in A) \tag{8}$$

gelten.

Beweis. Sind a_1, a_2 zwei Elemente von A, so gilt nach (5), (6)

$$a_1 a_2 \leqq a_1 a \leqq a_1 \leqq a \quad \text{und} \quad a_1 a_2 \leqq a a_2 \leqq a_2 \leqq a. \tag{9}$$

Aus (9) folgt

$$a_1 a_2 \leqq a_1 \cap a_2, \tag{10}$$

woraus man infolge (3) mit vollständiger Induktion

$$(a_1 \cdots a_{k-1}) a_k \leqq (a_1 \cap \cdots \cap a_{k-1}) a_k \leqq a_1 a_k \cap \cdots \cap a_{k-1} a_k \leqq$$
$$\leqq (a_1 \cap a_k) \cap \cdots \cap (a_{k-1} \cap a_k) = a_1 \cap \cdots \cap a_{k-1} \cap a_k$$

bekommt, womit (8) bewiesen ist.

Da

$$(a_1 a_2) a = a_1 (a_2 a) \leqq a_1 a_2 \quad \text{und} \quad a(a_1 a_2) \leqq a_1 a_2$$

gelten, ist $a_1 a_2$ ein Absorbent von a. Das sichert, daß A eine Teilhalbgruppe von L ist. Sind $a_\omega (\omega \in \Omega)$ Elemente von A, so sind $\bigcap\limits_{\omega \in \Omega} a_\omega \leqq a$ und wegen (3), (6)

$$(\bigcap_{\omega \in \Omega} a_\omega) a \leqq \bigcap_{\omega \in \Omega} a_\omega a \leqq \bigcap_{\omega \in \Omega} a_\omega \quad \text{und} \quad a(\bigcap_{\omega \in \Omega} a_\omega) \leqq \bigcap_{\omega \in \Omega} a_\omega \tag{11}$$

richtig. $\bigcap\limits_{\omega \in \Omega} a_\omega$ ist also ein Element von A. Damit ist A ein vollständiger Teilhalbverband von L.

Wegen (4_2) und (2) sind 0 und a Elemente von A und statt (4_1) gilt nach (6_1) für jedes $y (\in A)$

$$0 \leqq y \leqq a \qquad (y \in A). \tag{12}$$

Damit haben wir bewiesen, daß A eine H-Teilhalbgruppe von L ist.

Wir definieren für beliebig viele Elemente a_μ von A eine Vereinigungsoperation $\cup$ durch

$$\bigcup_\mu a_\mu = \bigcap d_\lambda, \tag{13}$$

wo d_λ die in A liegenden gemeinsamen oberen Schranken aller a_μ durchläuft[1]).

Man kann leicht einsehen, daß A bezüglich der in ihm definierten Verknüpfungen $\cap$ und $\cup$ einen vollständigen Verband bildet, in dem auch (7) gültig ist.

Damit ist der Beweis beendet.

---

[1]) Die Verknüpfung $\cup$ in A läßt sich auf eine einzige Art definieren derart, daß hierdurch A zu einem Verband wird. (Siehe Rédei [7] Satz 142.)

Beispiel 1. Es sei R ein assoziativer Ring. Die Menge L_1 aller Teilringe von R bildet eine multiplikative Halbgruppe und einen vollständigen Halbverband bezüglich der Durchschnittsbildung. Es ist leicht einzusehen, daß die Bedingungen (1)—(4) in L_1 gültig sind, somit ist L_1 eine H-Halbgruppe. Die Absorbenten eines Elementes von L_1 sind die Ideale (dieses Elementes d. h.) eines Teilringes von R. Aus Satz 1 ergeben sich wohlbekannte Ergebnisse über die Ideale eines Teilringes. Es ist bekannt, daß (7) sogar auch (7*) für die Ideale eines Teilringes von R erfüllt ist.

Beispiel 2. Ist K eine Halbgruppe mit Nullelement, so bildet die Menge L_2 aller Teilhalbgruppen mit Nullelement von K eine H-Halbgruppe.

Beispiel 3. Bezeichne L_3 die Menge aller (zweiseitigen) Ideale der (zweiseitigen) Ideale eines assoziativen Ringes. Es ist nicht schwer einzusehen, daß L_3 eine H-Halbgruppe ist.

Beispiel 4. In einer Halbgruppe K mit Nullelement bilden alle (zweiseitigen) Ideale mit Nullelement der (zweiseitigen) Ideale mit Nullelement von K eine H-Halbgruppe.

§ 3. Ergebnisse über die Primabsorbenten

Es sei a ein Element von L. Einen Absorbenten p von a nennen wir *prim* (oder einen *Primabsorbenten*), wenn für irgendwelche Absorbenten m, n von a die Regel

$$mn \leqq p \Longrightarrow m \leqq p \quad \text{oder} \quad n \leqq p$$

gilt.

Ein Element $c(\in L)$ wird ein *Subabsorbent* des Elementes $a(\in L)$ genannt, wenn es ein Element $b(\in L)$ gibt, so daß c ein Absorbent von b und b ein Absorbent von a ist.

Betrachten wir den Subabsorbenten c des Elementes a. Die Elemente c, ca, ac, aca sind nach der Definition lauter Absorbenten des Elementes b, deshalb ist das Element $\{c\}_a = c \cup ca \cup ac \cup aca$ nach Satz 1 auch ein Absorbent von b.

Wir machen von jetzt an die sehr wesentliche Voraussetzung:

(7*) $$b\left(\bigcup_{\omega\in\Omega} a_\omega\right) = \bigcup_{\omega\in\Omega} b a_\omega \quad \text{und} \quad \left(\bigcup_{\omega\in\Omega} a_\omega\right) b = \bigcup_{\omega\in\Omega} a_\omega b,$$

wo a_ω und b Absorbenten eines gegebenen Elementes von L sind.

Wegen der Voraussetzung (7*) ist $\{c\}_a$ ein Absorbent des Elementes a.

Lemma 1. *Sind x, y zwei Subabsorbenten und p ein Primabsorbent des Elementes $a(\in L)$, so folgt aus*

$$xy \leqq p$$

entweder $x \leqq p$ oder $y \leqq p$.

Beweis. Nach der Voraussetzung existieren zwei Absorbenten a_1, a_2 von a, so daß x ein Absorbent von a_1 und y ein Absorbent von a_2 ist. Gilt

$$xy \leqq p, \tag{14}$$

so besteht

$$a_1 x a_1 \cdot a_2 y a_2 \leqq xy \leqq p. \tag{15}$$

Da $a_1 x a_1$, $a_2 y a_2$ Absorbenten und p ein Primabsorbent von a sind folgt aus (15)

$$a_1 x a_1 \leqq p \quad \text{oder} \quad a_2 y a_2 \leqq p. \tag{16}$$

Ist z. B. $a_1 x a_1 \leqq p$, so betrachten wir das Produkt $a_1 \{x\}_a a_1$. Infolge der Annahme (7*) besteht

$$a_1\{x\}_a a_1 = a_1(x \cup xa \cup ax \cup axa)a_1 = a_1 x a_1 \cup a_1 x a a_1 \cup a_1 a x a_1 \cup a_1 a x a a_1 = a_1 x a_1 \leqq p,$$

deshalb gilt entweder $a_1 \leqq p$ oder $\{x\}_a \leqq p$, woraus in beiden Fällen $x \leqq p$ folgt.

Damit ist Lemma 1 bewiesen.

Aus Lemma 1 sieht man, daß aus der „Primeigenschaft" bezüglich der Absorbenten die „Primeigenschaft" bezüglich der Subabsorbenten folgt.

Wir sagen, daß $p(\in L)$ ein *Primelement* in L ist, wenn für beliebige Elemente $x, y(\in L)$ aus

$$xy \leqq p$$

$x \leqq p$ oder $y \leqq p$ folgt.

Aus Lemma 1 bekommt man unmittelbar:

Korollar 1. *Ist jedes Element von L ein Subabsorbent von e, so ist ein Primabsorbent von e ein Primelement in L.*

Lemma 1 besagt für Ringe folgendes: Es bezeichnen A, B zwei Ideale und P ein Primideal[2]) eines assoziativen Ringes R. Besteht für das Ideal X von A und für das Ideal Y von B die Bedingung

$$XY \subseteq P,$$

so gilt $X \subseteq P$ oder $Y \subseteq P$.

Man sieht, daß Korollar 1 auf die H-Halbgruppen L_3 (s. Beispiel 3) und L_4 (s. Beispiel 4) anwendbar ist.

Lemma 2. *Ist b ein Absorbent und p ein Primabsorbent des Elementes $a(\in L)$, so ist $b \cap p$ ein Primabsorbent von b.*

---

[2]) Ein Ideal P eines assoziativen Ringes R nennen wir ein *Primideal*, wenn für irgendwelche Ideale A, B von R die Regel

$$AB \subseteq P \Rightarrow A \subseteq P \quad \text{oder} \quad B \subseteq P$$

gilt.

Ein Ideal S von R heißt nach NAGATA [6] *Halb-Primideal*, wenn S ein Durchschnitt von Primidealen ist.

Beweis. $b \cap p = b'$ ist offenbar ein Absorbent von b. Sind x, y zwei Absorbenten von b mit

$$xy \leqq p' = b \cap p \leqq p,$$

so gilt nach Lemma 1 entweder $x \leqq p$ oder $y \leqq p$. Dies bedeutet wegen $x \leqq b$ und $y \leqq b$, daß $x \leqq p'$ oder $y \leqq p'$ gilt, womit unser Beweis beendet ist.

Ein Element $s(\in L)$ heißt *Halb-Primabsorbent* des Elementes $a(\in L)$, wenn s ein Durchschnitt von Primabsorbenten von a ist.

Aus Lemma 2 folgt unmittelbar

Lemma 2'. *Ist b ein Absorbent und s ein Halb-Primabsorbent des Elementes $a(\in L)$, so ist $b \cap s$ ein Halb-Primabsorbent von b.*

Lemma 3. *Ist b ein Absorbent des Elementes $a(\in L)$ und s ein Halb-Primabsorbent von b, so ist s ein Absorbent von a.*

Beweis. Im Falle $s = b$ ist die Behauptung trivial. Offenbar ist es genug zu zeigen, daß ein Primabsorbent $p(\neq b)$ von b ein Absorbent von a ist. Da $bap \leqq p$ und $b \not\leqq p$ gilt, muß $ap \leqq p$ bestehen. Ebenso bekommt man: $pa \leqq p$, womit Lemma 3 bewiesen ist.

Aus Lemma 2 bzw. Lemma 3 bekommt man als einen speziellen Fall die folgenden bekannten Ergebnisse:

Ist A ein Ideal und P ein Primideal eines assoziativen Ringes R, so ist $A \cap P$ ein Primideal von A. (McCoy [5] Lemma 2.)

Ist A ein Ideal eines assoziativen Ringes R und S ein Halb-Primideal von A, so ist S ein Ideal von R. (Nagata [6] Remark 2.)

§ 4. Über die Absorbentenquotienten

Betrachten wir zwei Absorbenten a, b des Elementes $e(\in L)$. Die Vereinigung der Absorbenten x von e, welche die Bedingung

$$xa \leqq b \tag{17}$$

befriedigen, heißt ein *linksseitiger Absorbentenquotient* und wird durch $(b:a)_l$ bezeichnet.

Wegen $ba \leqq be \leqq b$ befriedigt das Element b die Bedingung (17), woraus

$$b \leqq (b:a)_l \tag{18}$$

folgt. Nach Satz 1 ist $(b:a)_l$ ein Absorbent von e und wegen (17), (7*) gilt[3])

$$(b:a)_l a \leqq b. \tag{19}$$

[3]) Aus der Definition und (19) sieht man, daß $(b:a)_l$ der größte Absorbent von e ist, der die Bedingung (17) befriedigt.

Ähnlich heißt der *rechtsseitige Absorbentenquotient* $(b:a)_r$ die Vereinigung der Absorbenten x von e, die die Bedingung

(17′) $$ax \leqq b$$

befriedigen.

Die Vereinigung der Absorbenten x von e, die die Bedingungen (17) und (17′) gleichzeitig befriedigen, wird *Absorbentenquotient* genannt und durch $b:a$ bezeichnet.

Natürlich gelten auch

(18′) $$b \leqq (b:a)_r, \quad b \leqq b:a$$

und

(19′) $$a(b:a)_r \leqq b; \quad (b:a)a \leqq b, \quad a(b:a) \leqq b.$$

Es ist leicht die folgenden wichtigen Formeln

(20) $$((\bigcap_{\omega\in\Omega} b_\omega):a)_l = \bigcap_{\omega\in\Omega}(b_\omega:a)_l; \quad ((\bigcap_{\omega\in\Omega} b_\omega):a)_r = \bigcap_{\omega\in\Omega}(b_\omega:a)_r; \quad (\bigcap_{\omega\in\Omega} b_\omega):a = \bigcap_{\omega\in\Omega}(b_\omega:a)$$

nachzuweisen, wo b_ω, a Absorbenten des Elementes e sind.

Einerseits gilt nämlich nach (19)

$$((\bigcap_{\omega\in\Omega} b_\omega):a)_l a \leqq \bigcap_{\omega\in\Omega} b_\omega \leqq b_\omega \qquad (\omega \in \Omega),$$

woraus

(21) $$((\bigcap_{\omega\in\Omega} b_\omega):a)_l \leqq \bigcap_{\omega\in\Omega}(b_\omega:a)_l$$

folgt.

Anderseits gilt nach (3_1) und (19)

$$(\bigcap_{\omega\in\Omega}(b_\omega:a)_l)a \leqq \bigcap_{\omega\in\Omega}((b_\omega:a)_l a) \leqq \bigcap b_\omega,$$

woraus man

(21′) $$\bigcap_{\omega\in\Omega}(b_\omega:a)_l \leqq ((\bigcap_{\omega\in\Omega} b_\omega):a)_l$$

bekommt.

(21) und (21′) zeigen die Gültigkeit von (20_1). Ähnlich sieht man auch (20_2) und (20_3) ein.

Satz 2. *Es sei a ein Absorbent des Elementes $e(\in L)$ und p ein Primabsorbent von a. Der Absorbentenquotient $p:a$ ist dann ein Primabsorbent von e, ferner gelten*

(22) $$(p:a) \cap a = p$$

und

(23) $$p:a = (p:a)_l = (p:a)_r.$$

Im Fall $p \neq a$ ist $p:a$ der einzige Primabsorbent von e, deren Durchschnitt

mit a das Element p ist, ferner ist dieses dann und nur dann ein Primabsorbent von e, wenn $p:a=p$ gilt[4]).

Beweis. Nach Lemma 3 ist p ein Absorbent von e, deshalb existieren die in (23) erwähnten Absorbentenquotienten.

Ist $p=a$, so gilt $(a:a)_l=(a:a)_r=a:a=e$, ferner gilt auch (22).

Setzen wir nachher $p\neq a$ voraus. Wir zeigen zuerst, daß $(p:a)_l$ ein Primabsorbent von e ist. Gilt für die Absorbenten m, n von e die Bedingung $mn\leqq(p:a)_l$, so besteht

$$am\cdot na\leqq mna\leqq p. \tag{24}$$

Da am und na zwei Absorbenten von a sind, muß wegen (24) $am\leqq p$ oder $na\leqq p$ bestehen.

Im Fall $na\leqq p$ ist $n\leqq(p:a)_l$.

Wenn $am\leqq p$ gilt, gilt auch $a\cdot ma\leqq p$, woraus wegen $a\not\leqq p$ die Relation $ma\leqq p$ d. h. $m\leqq(p:a)_l$ folgt.

Jetzt zeigen wir

$$(p:a)_l=(p:a)_r. \tag{25}$$

Nach der Definition besteht

$$a(p:a)_l\cdot a\leqq(p:a)_l a\leqq p \quad \text{und} \quad a\not\leqq p,$$

woraus $a(p:a)_l\leqq p$ folgt. Es gilt also $(p:a)_l\leqq(p:a)_r$. Ebenso sieht man ein, daß $(p:a)_r\leqq(p:a)_l$ ist. Damit haben wir (25) und zugleich (23) bewiesen.

Da wegen (3) und (19)

$$((p:a)_l\cap a)a\leqq(p:a)_l a\cap a^2\leqq p\cap a^2\leqq p \quad \text{und} \quad a\not\leqq p$$

bestehen und $(p:a)_l\cap a$ ein Absorbent von a ist, muß $(p:a)_l\cap a\leqq p$ sein. Offenbar gilt auch $p\leqq(p:a)_l\cap a$, weshalb (22) infolge (23) bewiesen ist.

Ist r ein Primabsorbent von e mit der Eigenschaft

$$r\cap a=p \qquad (a\not\leqq p), \tag{26}$$

so besteht wegen (26) und (8)

$$ra\leqq r\cap a=p,$$

woraus $r\leqq(p:a)_l$ folgt. Umgekehrt muß wegen $(p:a)_l a\leqq p\leqq r$ und $a\leqq r$ die Bedingung $(p:a)_l\leqq r$ erfüllt sein, womit $r=(p:a)_l=p:a$ bewiesen ist.

---

[4]) Es wäre möglich die Absorbentenquotienten nicht bezüglich e, sondern bezüglich eines beliebigen festgewählten Elementes von L zu definieren und Satz 2 in diesem allgemeinerem Fall zu beweisen. Der Einfachkeit halber beschäftigen wir uns nur mit dem obigen Falle.

Wenn $p = p:a$ gilt, so ist p, wie wir oben bewiesen haben, ein Primabsorbent von e.

Umgekehrt wenn $(p:a)_l = p:a \neq p$, folglich $(p:a)_l \not\equiv p$ gilt, so bekommt man aus

$$(p:a)_l a \leqq p \qquad (a \not\equiv p),$$

daß p kein Primabsorbent von e ist. Somit ist der Beweis von Satz 2 vollendet.

Das *Intervall* $[a, b]$ $(a, b \in L)$ besteht aus den Elementen $x(\in L)$ mit $a \leqq x \leqq b$.

Einen Absorbenten b des Elementes $a(\in L)$ nennen wir *eigentlich*, wenn $b \neq a$ gilt.

Korollar 2. *Ist a ein Absorbent des Elementes e, so besitzt e dann und nur dann einen eigentlichen Primabsorbenten, wenn entweder a einen eigentlichen Primabsorbenten hat oder in dem Intervall $[a, e]$ ein eigentlicher Primabsorbent von e existiert.*

Beweis. Es sei q ein eigentlicher Primabsorbent von e. Dann gilt entweder $q \cap a = a$ oder $q \cap a < a$. Im ersten Falle liegt q in dem Intervall $[a, e]$; im zweiten Fall ist $q \cap a$ nach Lemma 2 ein eigentlicher Primabsorbent von a.

Ist p ein eigentlicher Primabsorbent des Elementes a, so ist der Absorbentenquotient $p:a$ nach Satz 2 ein eigentlicher Primabsorbent von e.

Aus Satz 2 und Korollar 2 ergibt sich:

Korollar 3. *Mit Hilfe eines Absorbenten a des Elementes e läßt sich die Menge aller eigentlichen Primabsorbenten von e folgenderweise überblicken: Man bilde die Absorbentenquotienten $p_\alpha:a$ für alle eigentlichen Primabsorbenten p_α von a: So entstehen alle eigentlichen Primabsorbenten q_α von e mit $a \not\equiv q_\alpha$. Die übrigen Primabsorbenten von e liegen im Intervall $[a, e]$*[5]).

Über die Halb-Primabsorbenten beweisen wir folgendes

Lemma 4. *Es sei a ein Absorbent und v ein Halb-Primabsorbent des Elementes $e(\in L)$. Man betrachte eine gegebene Darstellung*

$$v = \bigcap_{\lambda \in \Lambda} p_\lambda$$

von v mit Hilfe von Primabsorbenten p_λ von e, unter welchen auch $p_{\lambda_0} = e$ vorkommt. Dann gilt die Formel

$$v = (v:a) \cap \bar{v},$$

wo $\bar{v} = \bigcap_{a \leqq p_\lambda} p_\lambda$ ist.

[5]) Man kann in L auch Primärabsorbenten definieren, für die dann die vorigen Ergebnisse unter geeigneten Voraussetzungen gültig bleiben.

Beweis. Gilt für jedes p_λ die Bedingung $a \leqq p_\lambda$, so besteht wegen $a \leqq v$ auch

$$v:a = e,$$

woraus die Behauptung $v = (v:a) \cap \bar{v} = e \cap \bar{v} = \bar{v}$ folgt.

Existiert mindestens ein Primabsorbent $p_{\lambda'}$ mit $a \not\leqq p_{\lambda'}$, so besteht

$$v = \Big(\bigcap_{a \not\leqq p_{\lambda'}} p_{\lambda'}\Big) \cap \Big(\bigcap_{a \leqq p_{\lambda''}} p_{\lambda''}\Big) = v_1 \cap v_2.$$

Da nach der Definition $\bar{v} = v_2$ gibt, bleibt nur

$$v_1 = \bigcap_{a \not\leqq p_{\lambda'}} p_{\lambda'} = v:a$$

zu beweisen. Wegen (20_3) und $a \leqq v_2$ ergibt sich

$$v:a = (v_1 \cap v_2):a = (v_1:a) \cap (v_2:a) = (v_1:a) \cap e = v_1:a.$$

So haben wir

$$v_1 = v_1:a$$

zu zeigen. Nach $(18_2')$ gilt einerseits $v_1 \leqq v_1:a$. Anderseits besteht nach (19′)

$$(v_1:a)a \leqq v_1 = \bigcap_{a \not\leqq p_{\lambda'}} p_{\lambda'},$$

woraus $(v_1:a)a \leqq p_{\lambda'}$ folgt. Wegen der Voraussetzung $a \not\leqq p_{\lambda'}$ muß für jedes $p_{\lambda'}$

$$v_1:a \leqq p_{\lambda'} \Rightarrow v_1:a \leqq \bigcap_{a \not\leqq p_{\lambda'}} p_{\lambda'} = v_1$$

bestehen.

Damit ist $v_1 = v_1:a$ bewiesen, wodurch der Beweis von Lemma 4 beendet ist.

Satz 2′. *Es sei a ein Absorbent des Elementes $e(\in L)$ und bezeichne s einen Halb-Primabsorbenten von a. Der Absorbentenquotient $s:a$ ist dann ein Halb-Primabsorbent von e, ferner gelten*

(27) $$(s:a) \cap a = s$$

und

(28) $$s:a = (s:a)_l = (s:a)_r.$$

Im Falle $s \neq a$ ist jeder Halb-Primabsorbent t von e, deren Durchschnitt mit a das Element s ist, in der Form

(29) $$t = (s:a) \cap u$$

darstellbar, wo u ein beliebiger Halb-Primabsorbent von e mit $a \leqq u$ bezeichnet. $s(\neq a)$ ist dann und nur dann ein Halb-Primabsorbent von e, wenn $s = t$ gilt.

Beweis. Nach Lemma 3 ist s ein Absorbent von e, also existieren die in (28) erwähnten Absorbentenquotienten.

Es sei $s=\bigcap_{\omega\in\Omega} p_\omega$, wobei die p_ω Primabsorbenten von a sind. Wegen (20_3) besteht

$$s:a=(\bigcap_{\omega\in\Omega} p_\omega):a=\bigcap_{\omega\in\Omega}(p_\omega:a). \tag{30}$$

Die Absorbentenquotienten $p_\omega:a$ sind nach Satz 2 Primabsorbenten von e, folglich ist $s:a$ ein Halb-Primabsorbent von e. Nach (30) und (22) gilt:

$$(s:a)\cap a=(\bigcap_{\omega\in\Omega}(p_\omega:a))\cap a=\bigcap_{\omega\in\Omega}((p_\omega:a)\cap a)=\bigcap_{\omega\in\Omega} p_\omega=s,$$

wodurch (27) nachgewiesen ist. Aus (30), (23) und (20) bekommt man die Behauptung (28).

Um (29) zu zeigen, bezeichne $t=\bigcap_{\lambda\in\Lambda} q_\lambda$ $(q_{\lambda_0}=e)$ einen Halb-Primabsorbenten von e mit

$$s=t\cap a=\bigcap_{\lambda\in\Lambda}(q_\lambda\cap a)<a. \tag{31}$$

Infolge Lemma 4 besteht

$$t=(t:a)\cap\bar{t}, \tag{32}$$

wobei $\bar{t}=\bigcap_{a\leqq q_\lambda} q_\lambda$ ist. Wir haben nur

$$t:a=s:a \tag{33}$$

zu beweisen. Nach (31) und (20_3) gilt

$$s:a=(t\cap a):a=(t:a)\cap(a:a)=t:a, \tag{34}$$

was die Behauptung (33) nachweist.

Gilt $s=t$, so ist s ein Halb-Primabsorbent von e. Ist umgekehrt s ein Halb-Primabsorbent von e, so ist s wegen $s\cap a=s$ in der Form $s=t=(s:a)\cap u$ darstellbar. Somit ist der Beweis beendet.

Die Begriffe der verschiedenen Absorbentenquotienten stimmen in Ringen (Halbgruppen) mit den Begriffen der ein- und zweiseitigen Idealquotienten überein[6]).

Aus Satz 2, Korollar 2 und 3 bekommt man durch eine Spezialisierung den Satz 1, das Korollar 1 und die Bemerkung 5 unserer Arbeit [8].

So besagt Satz 2′ z. B. für Ringe den folgenden:

Satz 3. *Es sei A ein Ideal eines assoziativen Ringes R und bezeichne S ein Halb-Primideal von A. Der Idealquotient $S:A$ ist ein Halb-Primideal von R und es gilt:*

$$(S:A)\cap A=S,\quad S:A=(S:A)_l=(S:A)_r.$$

[6]) Sind A und B zwei Ideale eines assoziativen Ringes R, so besteht z. B. der *linksseitige Idealquotient* $(B:A)_l$ aus den Elementen $x(\in R)$, die die Bedingung

$$xA\subseteq B$$

befriedigen. In den Halbgruppen definiert man diesen Begriff ähnlich.

Im Fall $S \neq A$ ist jedes Halb-Primideal T von R, deren Durchschnitt mit A das Ideal S ist, in der Form

$$T = (S:A) \cap U$$

darstellbar, wo U ein beliebiges Halb-Primideal von R mit $A \subseteq U$ bezeichnet. $S \neq A$ ist dann und nur dann ein Halb-Primideal von R, wenn $S = T$ gilt.

§ 5. Ergebnisse über gewisse Radikale

Es seien $a, b (a < b)$ zwei Absorbenten des Elementes $e (\in L)$. Den (nichtleeren) Durchschnitt aller Primabsorbenten von b, die im Intervall $[a, b]$ liegen und eine gegebene Eigenschaft (T) haben, nennen wir das *T-Radikal des Intervalls* $[a, b]$ und bezeichnen dieses mit $T[a, b]$. Hat aber das Element b keinen Primabsorbenten mit der Eigenschaft (T) im Intervall $[a, b]$, so werde $T[a, b] = b$ gesetzt.

Aus Lemma 4 bekommt man unmittelbar

Satz 4. *Ist a ein Absorbent des Elements $e (\in L)$, so gilt die Formel*

$$T[0, e] = (T[0, e] : a) \cap T[a, e]. \tag{35}$$

Aus Satz 4 ergibt sich leicht das folgende

Korollar. *Es sei a ein Absorbent des Elementes e. Besteht für das T-Radikal $T[0, a]$ des Intervalls $[0, a]$ die Bedingung*

$$T[0, a] = T[0, e] \cap a, \tag{36}$$

so gilt

$$T[0, e] = (T[0, a] : a) \cap T[a, e]. \tag{37}$$

Beweis. Wegen (36) und (20) besteht

$$T[0, a] : a = (T[0, e] \cap a) : a = (T[0, e] : a) \cap (a:a) = T[0, e] : a,$$

woraus nach (35) die Behauptung (37) folgt.

Satz 4 und Korollar 4 wollen wir auf gewisse Radikale eines assoziativen Ringes R anwenden. Zu diesem Zweck bezeichne L nun die H-Halbgruppe aller Teilringe eines assoziativen Ringes R. Sind $A, B (A \subset B)$ zwei Ideale des Ringes R, so nennen wir den nichtleeren Durchschnitt aller Primideale des Teilringes B, die das Ideal A enthalten und eine gegebene Eigenschaft (T) haben, das *T-Radikal von B über A*, und wir bezeichnen es mit $T[A, B]$. Hat der Teilring B kein das Ideal A enthaltendes Primideal mit der Eigenschaft (T), so gelte $T[A, B] = B$.

Jetzt geben wir die Definitionen gewisser bekannter Radikale an, die sich als lauter T-Radikale erweisen.

Das *Brown—McCoysche Radikal* eines Ringes R ist der nichtleere Durchschnitt aller Ideale M von R, für die der Faktorring R/M einfach und mit Einselement ist. (Siehe BROWN—MCCOY [1].) Es ist bekannt, daß die Ideale M mit der obigen Eigenschaft Primideale von R sind. (Siehe z. B. RÉDEI [7], Satz 186.)

Das *M-Radikal* bei NAGATA [6] ist der nichtleere Durchschnitt aller Primideale P des Ringes R, für die der Faktorring R/P einfach ist.

Das *Fuchssche Radikal* eines Ringes R ist der nichtleere Durchschnitt aller Z-maximalen Ideale von R und jedes Z-maximale Ideal ist ein Primideal von R. (Siehe FUCHS [2] und [2a].)

Das *Krull—McCoysche Radikal* eines Ringes R ist der nichtleere Durchschnitt aller Primideale von R. (Siehe MCCOY [5] und NAGATA [6].)

Das *Jacobsonsche Radikal* eines Ringes R ist der nichtleere Durchschnitt aller primitiven Ideale von R. (Siehe JACOBSON [3], [4] und Nagata [6].) Es ist bekannt, daß jedes primitive Ideal ein Primideal von R ist. (Siehe z. B. NAGATA [6].)

Aus Satz 4 bekommt man den

Satz 5. *Ist A ein Ideal eines assoziativen Ringes R, so gilt die Formel*

$$T[0, R] = (T[0, R]:A) \cap T[A, B]. \tag{38}$$

Unter den oben erwähnten Radikalen haben das Brown—McCoysche, Jacobsonsche und Krull—McCoysche Radikal auch die Eigenschaft:

$$T[0, A] = T[0, R] \cap A \tag{39}$$

für jedes Ideal A von R.

Wir nennen ein T-Radikal, welches auch die Bedingung (39) befriedigt, *T^*-Radikal*, und bezeichnen es mit $T^*[A, B]$. Nach Korollar 4 gilt

Korollar 5. *Ist A ein Ideal des Ringes R, so besteht die Formel*[7])

$$T^*[0, R] = (T^*[0, A]:A) \cap T^*[A, R]. \tag{40}$$

[7]) J. SZENDREI [9] hat ein ähnliches Ergebnis über das Jacobsonsche Radikal eines Ringes bewiesen.

Literaturverzeichnis

[1] B. Brown—N. H. McCoy, Radicals and subdirect sums, *American Journal of Math.*, **69** (1947), 46—58.
[2] Fuchs László, A radikálnak egy új definíciója, *Első Magyar Matematikai Kongresszus Közl.* (1952), 435—443.
[2a] L. Fuchs, On a new type of radical, *Acta Sci. Math.*, **16** (1955), 43—53.
[3] N. Jacobson, The radical and semi-simplicity for arbitrary rings, *American Journal of Math.*, **67** (1945), 300—320.
[4] N. Jacobson, *Structure of rings* (New York, 1956).
5] N. H. McCoy, Prime ideals in general rings, *American Journal of Math.*, **71** (1949), 823—833.
[6] M. Nagata, On the theory of radicals in a ring, *Journal Math. Soc. Japan*, **3** (1951), 330—344.
[7] L. Rédei, *Algebra* I (Leipzig, 1959).
[8] O. Steinfeld, On ideal-quotients and prime ideals, *Acta Math. Acad. Sci. Hung.*, **4** (1953), 289—298.
[9] J. Szendrei, On the Jacobson radical of a ring, *Publ. Math. Debrecen*, **4** (1955), 93—97.

(Eingegangen am 6. August 1960)

Bibliographie

Paul B. Fischer †, Arithmetik, 3. Auflage (Sammlung Göschen, Band 147), 152 Seiten, Berlin, Walter de Gruyter & Co., 1958.

Obwohl die erste Auflage dieses Büchleins 1938 erschienen ist, ist es auch noch heute ein nützliches Lehrbuch, welches u. a. einen Überblick über die Geschichte und eine systematische Entwicklung der Zahlenbegriffe gibt, die Quaternionen mit inbegriffen. In einem Anhang werden die arithmetischen und geometrischen Reihen, die Zinseszins- und Rentenrechnung, und die Elemente der Kombinatorik behandelt.

J. Szendrei (Szeged)

C. Berge, Théorie des graphes et ses applications (Collection Universitaire de Mathématiques, II), VIII+277 pages, Paris, Dunod, 1958.

The present book is the first attempt since the classical work of D. König[1]) to give a survey of some important branches of graph theory. The author does not treat again in detail all the results presented in König's book, but he turns his attention to the more recent investigations, in particular to topics which resulted in connection with (more or less practical) applications.

The book consists of 21 chapters and 5 appendices (Appendix 5 is due to J. Riguet), there are about 150 bibliographical references grouped according to the chapters.

Ch. 1 (Définitions générales) introduces the most fundamental concepts about sets, mappings, non-oriented and oriented graphs. Ch. 2 (Étude préliminaire de la descendance) studies the bases of an oriented graph, the inductive graphs, the classification of points introduced by the mutual preceding relation. In Ch. 3 (Fonction ordinale et fonction de Grundy sur un graphe infini) the functions mentioned in the title of the chapter are discussed, and a criterion is stated in order that an ordinal function can be defined. There are defined two manners of multiplication for a finite number of graphs. Ch. 4 (Les nombres fondamentaux de la théorie des graphes) investigates cyclomatic numbers, chromatic numbers, the point sets of internal resp. external stability. Ch. 5 (Noyaux d'un graphe) studies the sets of points being both internally and externally stable. Ch. 6 (Jeux sur un graphe) treats the game "Nim", the general concept of a game (with complete information), and the notion of strategy; there is exposed the theorem of Zermelo and von Neumann. Ch. 7 (Le problème du plus court chemin) presents algorithms for the solution of the labyrinth problem and some related ones. Ch. 8 (Réseaux de transport) reports chiefly on the researches of Ford and Fulkerson concerning the maximal flow through a transportation network. The main result of Ch. 9 (Théorème des demi-degrés) gives a criterion for the existence of an oriented graph if the collection of the semi-degrees of the points is prescribed. In Ch. 10 (Couplage d'un graphe simple) the even graphs are studied from

[1]) See the review in *Acta Sci. Math.*, 9 (1938), 66—68.

that point of view, what is the maximal number of elements in the sets of pairwise non-adjacent edges. It is proved the famous equivalence theorem of BERNSTEIN. There is given an application in matrix theory. Ch. 11 (Facteurs) introduces the notions of Hamiltonian circuit, factor and dissection. (Dissection is a collection of chains such that any point is contained in exactly one chain). A criterion is proved for the existence of a factor, and the determination of a partial graph having prescribed semi-degrees is studied. Ch. 12 (Centres d'un graphe) investigates the distance of points, the centre and the radius of a graph. Ch. 13 (Diamètre d'un graphe fortement connexe) presents some theorems in connection with the diameter of oriented graphs in which to any ordered pair of points there exists a chain from the first point to the second one. Ch. 14 (Matrice associée à un graphe) introduces matrices which show for each pair of points whether they are connected by an edge or not. It is given a method in order to determine the number of circuits consisting of three edges. There are defined (and graph-theoretically interpreted) the Boolean operations between these matrices. Ch. 15 (Matrices d'incidence) presents some theorems about incidence matrices, among others the criterion of POINCARÉ—VEBLEN—ALEXANDER for a set of edges of an antisymmetric (oriented) graph to be a sum of cycles. Ch. 16 (Arbres et arborescences) gives several characterizations of trees, methods for determining the number of subgraphs of a graph being trees resp. "arborescences", an algorithm for searching a subtree, satisfying a certain minimum property, of a graph. Ch. 17 (Le problème d'Euler) studies the questions of existence, determination and number of the Eulerian cycles. Ch. 18 (Couplage d'un graphe quelconque) discusses various questions starting with the classification of the edges of a graph into two classes. In Ch. 19 (Semi-facteurs) there are exposed among others the theorems of PETERSEN and TUTTE about the existence of semi-factors. Ch. 20 (Connectivité d'un graphe) constains results about the articulation points and the connectivity number. Ch. 21 (Graphes planaires) presents the well-known theorems characterizing the planar graphs (due to KURATOWSKI) resp. asserting the colorability of a planar graph by five colours.

Appendix 1 (Notice sur la théorie générale des jeux) presents the abstract definition of the game between two players, introduces the notions of combined strategy, hope and balance point, exposes the theorems of VON NEUMANN—NASH and KUHN—BIRCH. Appendices 2 and 3 (Notice sur les problèmes de transport; Notice sur l'utilisation de la notion de potentiel pour les réseaux de transport) investigate the so called Hungarian method resp. the problems of DIRICHLET and KOOPMANS concerning transportation questions. Appendix 4 (Problèmes non résolus et conjectures improuvées) enumerates fourteen open problems. Appendix 5 (Notice sur quelques principes fondamentaux d'énumération), written by J. RIGUET, investigates enumeration questions in connection with permutation groups (especially transitivity classes, fixed elements) and words (non-abelian and abelian ones) over a finite set.

A. Ádám (Szeged)

H. R. Pitt, Tauberian Theorems, X+174 Seiten, London, Oxford University Press, 1958.

Dieses Buch beschäftigt sich mit der Theorie der sog. Tauberschen Sätze, die auf die Grundideen von HARDY, LITTLEWOOD und WIENER aufgebaut ist, und gibt eine kurze Einführung in die wichtigsten Teile dieser Theorie.

Kapitel I ist eine Einführung, wo u. a. das Grundproblem allgemein abgefaßt ist. Man betrachtet eine Transformation

$$g(u) = \int_{-\infty}^{\infty} k(u, v)\, s(v)\, dv$$

mit gegebenem Kern; die Sätze von Tauberschem Charakter folgern gewisse Eigenschaften von $s(u)$ aus den Eigenschaften von $g(u)$. Das erste solche Resultat stammt von TAUBER; er hat bewiesen, daß die Konvergenz der Reihe $\sum_{n=0}^{\infty} a_n$ aus ihrer Abel-Summierbarkeit neben der Bedingung $a_n = o(n^{-1})$ folgt. Später hat LITTLEWOOD diese Behauptung anstatt „o" mit „O" bewiesen. In den Kapiteln II und III werden die elementaren Tauberschen „o"- und „O"- Sätze, u. a. die klassischen „O"- Sätze von HARDY und LITTLEWOOD betrachtet. Kapitel IV beschäftigt sich mit der Wienerschen Theorie und mit ihren Anwendungen auf die Verfahren von CESÀRO, RIESZ, LAMBERT, RIEMANN, HAUSDORFF, EULER, BOREL und ABEL. Im Kapitel V werden die Mercerschen Sätze mit Anwendungen auf die Integrodifferentialgleichungen kurz zusammengefaßt.

Die Tauberschen Sätze können auch in der analytischen Zahlentheorie angewendet werden. Alle Beweise des klassischen Primzahltheorems von HADAMARD und DE LA VALLÉE POUSSIN haben nämlich einen Tauberschen Charakter. In dem letzten Kapitel vergleicht Verfasser die verschiedenen Beweise dieses Satzes, die mit Anwendung des Satzes von LANDAU—IKEHARA, des Tauberschen Satzes von LAMBERT bzw. mit der Methode von INGHAM und SELBERG gezeigt werden können.

K. Tandori (Szeged)

Karl Zeller, Theorie der Limitierungsverfahren (Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 15), VIII + 242 Seiten, Berlin—Göttingen—Heidelberg, Springer-Verlag, 1958.

Die Limitierungstheorie ist heute schon so weit verzweigt und ihre Literatur ist so umfangreich, daß es im Rahmen eines solchen Buches unmöglich ist, eine abgeschlossene Darstellung der Ergebnisse dieser Theorie mit ausführlichen Beweisen darzubieten. Dieses Buch hat nur die Absicht, einen Überblick über die Theorie der Limitierung und ihre Methoden anzugeben und in die Literatur hineinzuführen. Dieser Zielsetzung entsprechend, werden die Definitionen und Erläuterungen knapp gefaßt, nur typische und leicht verständliche Sätze formuliert und von den Beweisen nur die Grundzüge wiedergegeben. Über die Verschärfungen, Verallgemeinerungen und vollständigen Beweise gibt das Buch nur Hinweise auf die entsprechende Literatur. Das Literaturverzeichnis (64 Seiten) ist nach Jahren angeordnet; neben den einzelnen zitierten Arbeiten findet man auch Hinweise auf die entsprechenden Referate in den referierenden Zeitschriften. Das Literaturverzeichnis ist im Rahmen der Stoffabgrenzung des Buches vollständig.

Die ersten 4 Kapitel des Buches behandeln die allgemeine Theorie der Matrixverfahren. Fragen über absolute und starke Limitierung, Mehrfachfolgen, Integraltransformationen und Anwendungen werden nur kurz gestreift. Nach einer kurzen geschichtlichen Übersicht werden die Grundbegriffe bzw. die Hauptprobleme definiert bzw. formuliert, dann werden die verwendeten Hilfsmittel aus der Funktionalanalysis angeführt. Anschließend wird die Strukturtheorie von Wirkfeldern behandelt. In dieser Theorie, die mit den Arbeiten von BANACH, MAZUR und ORLICZ beginnt, wird in die Wirkfelder eine Topologie eingeführt, wodurch funktionalanalytische Überlegungen zur Anwendung kommen können. Im Rahmen dieser Theorie werden z. B. die perfekten Verfahren, die Abschnittkonvergenz, allgemeine Limitierbarkeitskriterien, Einfolgenverfahren, Existenz eines Matrixverfahrens mit vorgeschriebenem Wirkfeld und Inäquivalenzsätze behandelt. Endlich folgt die Erörterung der direkten Sätze der Limitierungstheorie, insbesondere Einschließungssätze, Kernsätze, Sätze über Konvergenzfaktoren, Vergleichssätze, Multiplikationssätze, ferner Sätze über Verträglichkeit, Translation und Umordnung.

Im fünften Kapitel werden in größter Kürze Umkehrsätze behandelt. Zunächst werden konvergenzgleiche Verfahren und Mercer-Sätze, Lückensätze, gewisse elementare und tiefliegende Umkehrsätze, die Methoden von LITTLEWOOD, WIENER, KARAMATA und SCHMIDT, WIENERS Hauptsatz und gewisse funktionentheoretische Umkehrsätze betrachtet. Die letzten drei Kapitel beschäftigen sich mit speziellen Verfahren, analytischer Fortsetzung und Anwendungen. Als Verfahren vom Cesàro-Abel-Typ werden die Verfahren von CESÀRO, HÖLDER, ABEL, RIESZ und DIRICHLET erwähnt. Dann sind die Verfahren funktionentheoretischen Typs erörtert: z. B. Zweierverfahren, definiert mit der Transformation $t_l=(1-a)s_{l-1}+as_l$ $(l=0,1,\ldots)$. Verfahren von NÖRLUND, EULER—KNOPP, BOREL, allgemeine Euler-Verfahren, Kreisverfahren von TAYLOR und VALIRON. Endlich werden weitere Verfahren, z. B. die von HAUSDORFF, DE LA VALLÉE POUSSIN, GRONWALL, ROGOSINSKI—BERNSTEIN, RIEMANN, WIENER und die zahlentheoretischen Verfahren von LAMBERT und INGHAM betrachtet.

K. Tandori (Szeged)

Gustav Doetsch, Einführung in Theorie und Anwendung der Laplace-Transformation. Ein Lehrbuch für Studierende der Mathematik, Physik und Ingenieurwissenschaft (Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften, Mathematische Reihe, Band 24), 304 Seiten, 40 Figuren, Basel und Stuttgart, Birkhäuser Verlag, 1958.

Verf. hat sich das Ziel gesetzt, ein Lehrbuch über die Laplace-Transformation zu schreiben, welches — im Gegensatz zu den üblichen „Operatorenkalküln" — alles in der Theorie und in deren Anwendungen unbedingt Benötigte in voller Allgemeinheit und mit exakten Beweisen darbietet, — ein Buch, durch dessen Durcharbeiten ein Mathematiker oder Ingenieur, der die Laplace-Transformation in der täglichen Forschungsarbeit brauchen will, den dazu benötigten Stoff beherrschen wird. — Die berühmte dreibändige Monographie des Verfassers, das „Handbuch der Laplace-Transformation", konnte diese Aufgabe prinzipiell nicht lösen; dementsprechend ist das referierte Werk kein Auszug jenes größeren, sondern wurde es nach gut bewahrten didaktischen Erfahrungen neu aufgebaut. Das in der Theorie erreichte wird immer gleich zu Anwendungen ausgenutzt, aus jedem Anwendungsgebiet werden spezielle Beispiele gebracht. Einige Abschnitte sind anders dargestellt wie im „Handbuch"; manches Neue ist auch hinzugekommen.

Das Buch besteht aus 28 Paragraphen. §§ 1—11 behandeln die Grundbegriffe und die „Anwendungsregeln" der Laplace-Transformation. Das Laplace-Integral wird von physikalischen Gesichtspunkten aus mittels gewisser Fourier-Integrale eingeführt. Eine Einführung von rein mathematischem Charakter, die aus dem Begriff der Potenzreihen und Dirichletschen Reihen ausgeht, wird auch gegeben. Die Analogie mit den Potenzreihen wird im ganzen Werk oft ausgenützt. Nach den Konvergenzproblemen des Laplace-Integrals werden die Laplace-Transformation als linearer Integraloperator und die diesbezüglichen Begriffe wie Originalfunktion, Bildfunktion und Abbildung eingeführt, und die Frage der Umkehrbarkeit behandelt. §§ 12—15 sind dem Anfangswertproblem der gewöhnlichen Differentialgleichungen (nebst regelungstechnischen Fragen), der Behandlung der Systemen von Differentialgleichungen, und dem Anfangswertproblem von Differenzengleichungen gewidmet. In § 13 führt Verf. den Begriff der Diracschen Funktion (auch Impulsfunktion genannt) ein, und gibt mehrere Methoden, mit denen diesbezügliche praktisch wichtige Fälle behandelt werden können. Auf die Distributionstheorie wirdes nicht eingegangen. — §§ 16—23 beschäftigen sich wieder mit Fragen rein mathematischer Natur, u. a. mit dem Verhalten der Laplace-Transformierten im Unendlichen, mit der komplexen Umkehrformel, mit der Auswertung des komplexen Umkehrintegrals durch Residuenrechnung, ferner mit dem Problem

der Darstellbarkeit einer Funktion als Laplace-Transformierte, und mit der für die Praxis so wichtigen Aufgabe der Bestimmung der Originaltunktion durch Reihenentwicklung der Bildfunktion. §§ 24—25 behandeln u. a. das asymptotische Verhalten der Bildfunktion (Originalfunktion) im Unendlichen. In § 26 sind gewöhnliche Differentialgleichungen mit Polynomkoeffizienten durch Anwendung der Resultate der früheren Abschnitte betrachtet. § 28 beschäftigt sich mit Rand- und Anfangswertproblemen gewisser partieller Differentialgleichungen (Wärmeleitung- und Telegraphengleichung), mittels der Laplace-Transformation. § 28 behandelt mit denselben Hilfsmitteln Volterrasche Integralgleichungen erster und zweiter Art vom Faltungstypus.

Das Buch hat einen anziehenden Stil, ist methodisch ausgezeichnet aufgebaut und sehr gut lesbar. Der organische Zusammenhang zwischen den einzelnen Paragraphen wird immer angedeutet. Neben dem Hauptthema wird der Leser über viele Begriffe, Ideen und Resultate der klassischen Analysis unterrichtet, so daß dadurch eventuelle umfangreichere Vorstudien wohl vermieden werden können; auch der Kenner wird durch das Studium des Werkes viele Einzelheiten z. B. in der komplexen Funktionentheorie in neueren Beziehungen kennen lernen. Die behandelten Anwendungen sind lehrreich. Einige interessante mathematische Themen bzw. oben nicht erwähnte Anwendungsgebiete, die im Buche beiläufig berührt sind, mögen erwähnt werden: Diskontinuierliche Faktoren; Eigenschaften von speziellen Funktionen und elegante Formeln dafür: Fourier-Transformation; Neumannsche Reihe; Thomésche Normalreihe; Partialbruchzerlegung meromorpher Funktionen; Integration nichtganzer Ordnung: Abstimmung eines Empfängers; bremsende Kupplung eines Schwungrads; elektrische Schwingungprobleme; Bewegung eines Pendels unter Stoßeinwirkung; Rückkoppelungsprobleme; Übergangsfunktionen und Frequenzcharakteristiken; Verzerrung eines Signals; Wellengleichung. Als Neues schließen sich an diese z. B. die Themen: exakter Beweis für die Berechnung der Übergangsfunktion aus den Komponenten des Frequenzgangs; Untersuchung der Eigenschaften des komplexen Umkehrintegrals mit winkelförmigem Weg: asymptotische Entwicklung der Lösungen von partiellen Differentialgleichungen.

Das Buch bildet ein wertvolles Hilfsmittel für die Studierenden, sowie für die auf anderen Gebieten arbeitenden Experten.

P. Medgyessy (Budapest)

J. Kuntzmann, Méthodes numériques. Interpolation—Dérivées, XVIII + 254 pages, Paris, Dunod, 1959.

En connexion avec la croissance, pendant les derniers dizaines d'années, de l'importance du calcul numérique pour la technique et la science modernes, en premier lieu en relation avec le développement des machines à calculer, avait lieu aussi un développement des méthodes numériques si rapide, qu'à jour s'est fait très difficile à écrire une monographie sur le calcul en tout. Ce domaine se met à se différencier, comme c'était arrivé plus tôt à des autres branches de la mathématique. La théorie qui donne, en commun avec le calcul des erreurs, le fondement pour toutes les autres théories provenant de cette différentiation, c'est celle de l'interpolation. L'auteur donne une vue d'ensemble moderne de cette théorie. Il réalise deux buts: d'une part il traite de l'exécution pratique des calculs d'une manière bien approfondie, avec un regard spécial pour les machines à programme, d'autre part il s'efforce de rendre ses Cours plus théoriques comme d'usage. Tout de même, en ce qui concerne cette deuxième tendance, il nous semble que l'étude de l'expression en forme d'intégrale de l'erreur des formules d'interpolation (pp. 44—49), bien qu'intéressante théoriquement, est peu conforme à l'esprit du livre, parce que les résultats obtenus ont peu de chance à être employés dans la pratique.

Dans le premier chapitre l'auteur présente les méthodes du calcul de la valeur d'un polynôme de degré n, donné par $n+1$ valeurs, y compris le procédé d'AITKEN et ses variantes. Le second et le troisième chapitre développent la théorie de l'interpolation par tels polynômes et l'application de cette théorie pour les tables, avec une étude détaillée des erreurs. Après, on étudie la dérivation approchée, l'interpolation dans le cas où parmi les données on a aussi des valeurs des dérivées, l'interpolation pour des fonctions d'une variable complexe et des fonctions de plusieurs variables, et enfin on donne une vue d'ensemble de la théorie générale de l'interpolation.

G. Pollák (Szeged)

Frédéric Riesz, Oeuvres complètes, Publiées sur l'ordre de l'Académie des Sciences de Hongrie par ÁKOS CSÁSZÁR, docteur des sciences mathématiques. En deux volumes, 1601 pages, Budapest, Akadémiai Kiadó, 1960.

Peu après les *Oeuvres complètes* d'ALFRED HAAR, l'Académie des Sciences de Hongrie vient de faire apparaître aussi les *Oeuvres complètes* de F. RIESZ, et de cette façon les deux illustres fondateurs des *Acta* de Szeged ont reçu l'hommage de l'Académie des Sciences de Hongrie dont ils étaient des membres, et les savants de tous les pays ont obtenu un accès commode à l'oeuvre de ces deux maîtres des sciences mathématiques du XXième siecle.

M. ÁKOS CSÁSZÁR, qui a entrepris le travail de rédiger les *Oeuvres complètes* de F. RIESZ, commence par une courte notice biographique (F. RIESZ naquit le 22 janvier 1880 à Győr et décéda le 28 janvier 1956 à Budapest). Après, il suit une liste des travaux scientifiques de F. RIESZ, en ordre chronologique, embrassant 95 titres. Tous ces travaux ont été reproduits dans les deux volumes sauf un: les *Leçons d'analyse fonctionnelle* de F. RIESZ et B. SZ.-NAGY. En particulier, on trouve inséré aussi le livre, devenu classique, *Les systèmes d'équations linéaires à une infinité d'inconnues* (1913).

La reproduction est faite par une voie photographique. Les travaux sont groupés selon leur sujet dans les groupes suivants: Topologie — Théorie des fonctions réelles — Espaces fonctionnelles — Fonctions analytiques — Fonctions harmoniques et sousharmoniques — Analyse fonctionnelle — Théorie ergodique — Géométrie — Questions diverses.

Certains des travaux de F. RIESZ étaient rédigés et publiés en deux variantes: en hongrois et en une autre langue; on trouve ici reproduites toutes les deux. Quelques de ses ouvrages n'étaient publiés originalement qu'en hongrois: on les trouve ici dans leur forme originale et, dans l'appendice, aussi en traduction française. Parmi ces ouvrages, qui de cette façon deviennent pour la première fois accessibles aussi à ceux qui ne comprennent pas le hongrois, on trouve une Note sur les valeurs à la frontière des fonctions analytiques par F. RIESZ et G. SZEGŐ et, ce qui sera peut-être le plus surprenant à ceux qui ne connaissaient F. RIESZ que de ses travaux sur l'analyse mathématique et la topologie, on y trouve la traduction de ses travaux de sujet de géométrie projective (en particulier sa Thèse: *Étude des configurations ponctuelles sur les courbes gauches de première espèce du quatrième ordre par la méthode synthétique de la géométrie projective* (1902)). On y trouve aussi la traduction d'un discours, prononcé par RIESZ comme recteur de l'Université de Szeged en 1925, sur les *„méthodes élémentaires dans les mathématiques supérieures"*. On a inséré en appendice aussi un article de T. RADÓ embrassant entre autres la démonstration simple du théorème de RIEMANN sur les représentations conformes, due à F. RIESZ et L. FEJÉR.

A la fin des *Oeuvres complètes* on trouve une liste des *errata*, très soigneusement rédigée, contenant même des remarques critiques qui vont souvent nettement au delà la

correction des fautes d'impression. On doit remercier M. Ákos Császár et ses collaborateurs MM. J. Bognár, J. Czipszer, F. Kárteszi et D. Králik d'avoir entrepris la tâche de revoir très attentivement les travaux originaux. Par la rédaction de ces *errata* ils ont contribué essentiellement à la valeur de cette édition des *Oeuvres complètes* du Maître.

Béla Sz.-Nagy (Szeged)

F. G. Tricomi, Fonctions hypergéométriques confluentes (Mémorial des Sciences Mathématiques, Fasc. CXL), 86 pages, Paris, Gauthier-Villars, 1960.

La classe des fonctions en question — celle des solutions de l'*équation hypergéométrique confluente* $xy'' + (c-x)y' - ay = 0$ (*) — figure parmi les famillies de fonctions spéciales les plus importantes et récemment aussi le plus souvent considérées dans la littérature. Mais tandis que les monographies précédantes (p. ex. le livre de même sujet de Buchholz [1953] ou „L'analyse moderne" de Whittaker et Watson) portent sur l'*équation de Whittaker* qui découle par une transformation convenable de (*), et sur les deux solutions fondamentales $M_{\varkappa,\mu}(x)$, $W_{\varkappa,\mu}(x)$ de celle-ci, l'auteur préfère ici (comme dans un ouvrage en langue italienne de 1954) d'envisager l'intégrale principale de (*) (due à Kummer)

$$\Phi(a, c; x) = \sum_{n=0}^{\infty} \frac{a(a+1)\dots(a+n-1)}{c(c+1)\dots(e+n-1)} \frac{x^n}{n!} \qquad (c \text{ non-entier}),$$

ainsi que la seconde solution particulière $\Psi(a, c; x) = \Gamma(1-c)\Gamma(a-c+1)^{-1}\Phi(a, c; x) + + \Gamma(c-1)\Gamma(a)^{-1}\Phi(a-c+1, 2-c; x)$, définie immédiatement par une intégrale à lacet. Cette discussion a l'avantage que $\Phi(a, c; x)$ est une fonction *entière* de x et on obtient pour Φ et Ψ des formules qui dépassent en simplicité presque toujours les relations correspondantes pour $M_{\varkappa,\mu}$, $W_{\varkappa,\mu}$.

Après une courte introduction on trouve la discussion de l'équation différentielle (*) et les propriétés les plus essentielles des solutions que nous venons d'indiquer, en particulier le développement (due à Tricomi) de $\Gamma(c)^{-1}\Phi(a, c; x)$ en série de fonctions de Bessel. Chapitre III porte sur le comportement asymptotique, les zéros etc. de $\Phi(a, c; x)$ et $\Psi(a, c; x)$, prenant surtout le champ réel en considération. Chapitre IV est destiné aux applications de la théorie générale. On considère ici de nombreux cas particuliers (fonctions de Bessel, de Laguerre, celles du cylindre parabolique et fonctions gamma incomplètes) et certains problèmes remarquables de la physique mathématique. La descpriction des deux fdnctions gamma incomplètes (liées au sinus intégral, à l'intégrale d'erreur, au logarithme intégral etc.) est naturellement prépondérante. — Une bibliographie sommaire sur les dernières pages contient 33 ouvrages.

L'exposé reste partout clair et un nombre de figures et tables — en partie originalement illustrées — est inséré. Le livre atteindra sans doute son but chez les analystes, donnant dans le cadre d'une théorie intéressante une vue d'ensemble de la plupart des fonctions spéciales qui présentent un intérêt pratique.

M. Mikolás (Budapest)

ERRATUM

Page 155, ligne 21:

au lieu de 28 janvier 1956

lire 28 février 1956

INDEX — TARTALOM

Benado, M. Sur une propriété d'interpolation remarquable dans la théorie des ensembles partiellement ordonnés 1
Bruck, R. H. Sums of normal endomorphisms. II 6
Daróczy, Z. Notwendige und hinreichende Bedingungen für die Existenz von nichtkonstanten Lösungen linearer Funktionalgleichungen 31
Fuchs, L. On the ordering of quotient rings and quotient semigroups 42
Huppert, B. Subnormale Untergruppen und p-Sylowgruppen 46
Pollák, G. Über die Struktur kommutativer Hauptidealringe 62
Rényi, A. On random generating elements of a finite Boolean algebra 75
Steinfeld, O. Die einstufig nichtregulären bzw. nichtprimen Ringe 82
Surányi, J. Über zerteilte Parallelogramme 85
Weinert, H. J. Über die Einbettung von Ringen in Oberringe mit Einselement 91
Brehmer, S. Über vertauschbare Kontraktionen des Hilbertschen Raumes 106
Sz.-Nagy, B. Bemerkungen zur vorstehenden Arbeit des Herrn S. Brehmer 112
Dixmier, J. Points séparés dans le spectre d'une C^*-algèbre 115
Leindler, L. Zur Frage der Approximation durch orthonormierte Polynomsysteme . . 129
Tandori, K. Bemerkung zu einem Satz von A. N. Kolmogoroff 133
Steinfeld, O. Verbandstheoretische Betrachtung gewisser idealtheoretischer Fragen . . 136
Bibliographie 150

ACTA SCIENTIARUM MATHEMATICARUM
SZEGED (HUNGARIA), ARADI VÉRTANÚK TERE 1

Prix d'abonnement pour l'étranger $ 8.50. On peut s'abonner à l'entreprise de commerce des livres et journaux „Kultúra" (Budapest, VI., Népköztársaság útja 21).

61-56 Szegedi Nyomda Vállalat
Tankönyvkiadó Vállalat
A kiadásért felel: Vágvölgyi Tibor igazgató
Felelős szerkesztő: Szőkefalvi-Nagy Béla
Műszaki vezető: Horváth János
Műszaki szerkesztő: Vízkelety József
A kézirat nyomdaba érkezett: 1961. január. Megjelenés: 1961. május.
Példányszám 750. Terjedelem 13,6 (A/5) ív
Készült kéziszedéssel, íves magasnyomással az MSZ 5601-54 és az MSZ 5602-55 szabvány szerint
Azonossági szám: 6446