Werk

Label: Periodical issue

Jahr: 1958

PURL: https://resolver.sub.uni-goettingen.de/purl?266833020_0070|log26

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

A 82

Postverlagsort Berlin

MATHEMATISCHE ZEITSCHRIFT

UNTER STÄNDIGER MITWIRKUNG VON

E. KAMKE, TÜBINGEN
R. NEVANLINNA, HELSINKI
E. SCHMIDT, BERLIN
F. K. SCHMIDT, HEIDELBERG

HERAUSGEGEBEN VON

H. WIELANDT, TÜBINGEN

WISSENSCHAFTLICHER BEIRAT

W. BLASCHKE L. FEJÉR A. E. INGHAM H. KNESER
W. MAGNUS O. PERRON G. PICKERT

70. BAND, 3. HEFT

(ABGESCHLOSSEN AM 10. DEZEMBER 1958)

BERLIN · GÖTTINGEN · HEIDELBERG
SPRINGER-VERLAG
1958

Niedersächsische Staats- u. Universitätsbibliothek Göttingen

Math. Z.

4186

Die **MATHEMATISCHE ZEITSCHRIFT**

wurde im Jahre 1918 von *L. Lichtenstein* unter der Mitwirkung von *K. Knopp*, *E. Schmidt* und *I. Schur* gegründet und herausgegeben. Nach dem Tode Lichtensteins übernahm *K. Knopp* 1933 die Herausgabe. Die Schriftleitung ergänzte sich 1933 durch *E. Kamke* und *F. K. Schmidt*, 1936 durch *R. Nevanlinna* und 1950 durch *H. Wielandt*, der 1952 die Herausgabe übernahm.

Die Zeitschrift erscheint nach Maßgabe des eingehenden Materials. Der Preis des Bandes beträgt DM 96.—.

Die Mathematische Zeitschrift ist durch jede Buchhandlung zu beziehen.

Die Mathematische Zeitschrift dient der Pflege der reinen Mathematik, doch werden auch Beiträge aus den Gebieten der theoretischen Physik und Astronomie Aufnahme finden, soweit sie mathematisch von Interesse sind. Besprechungen, Aufgaben u. dgl. werden nicht zugelassen.

Es wird ausdrücklich darauf aufmerksam gemacht, daß mit der Annahme des Manuskriptes und seiner Veröffentlichung durch den Verlag das ausschließliche Verlagsrecht für alle Sprachen und Länder an den Verlag übergeht, und zwar bis zum 31. Dezember desjenigen Kalenderjahres, das auf das Jahr des Erscheinens folgt. Hieraus ergibt sich, daß grundsätzlich nur Arbeiten angenommen werden können, die vorher weder im Inland noch im Ausland veröffentlicht worden sind, und die auch nachträglich nicht anderweitig zu veröffentlichen der Autor sich verpflichtet.

Es ist ferner ohne ausdrückliche Genehmigung des Verlages nicht gestattet, photographische Vervielfältigungen, Mikrofilme, Mikrophote u. ä., von den Zeitschriftenheften, von einzelnen Beiträgen oder von Teilen daraus herzustellen.

Die Mitarbeiter erhalten von ihren Arbeiten 75 Sonderdrucke unentgeltlich.

Manuskriptsendungen sind zu richten an die Mitglieder der unterzeichneten Redaktion. Die Herren Mitarbeiter werden im Interesse einer raschen Drucklegung gebeten, die Arbeiten in gut lesbarer Niederschrift einzureichen. Für den Text ist, wenn irgend möglich, Maschinenschrift, für die mathematischen Formeln jedoch nur Handschrift zu verwenden. Etwaige Abbildungen sind auf einem besonderen Blatt zu zeichnen. Die in den Formeln etwa vorkommenden griechischen oder deutschen Buchstaben (Fraktur) sowie andere der Gefahr von Verwechselungen ausgesetzte Zeichen, z.B. die Landauschen Symbole o und O, sind stets besonders (etwa mit verschiedenfarbigen Stiften) zu kennzeichnen. Die Fußnoten sind fortlaufend zu numerieren, bei Zitaten Erscheinungsjahr und Seitenzahlen anzugeben.

Wenn zu einer bereits gedruckten Arbeit eine Berichtigung nötig wird, wollen die Herren Verfasser dem Herausgeber hiervon unverzüglich Mitteilung machen. Die Berichtigungen sollen dann am Schlusse eines Bandes gesammelt aufgenommen werden.

REDAKTION DER MATHEMATISCHEN ZEITSCHRIFT:

E. Kamke, Tübingen, Frischlinstraße 27,
R. Nevanlinna, Helsinki (Finnland), Mäntytie 5 B
E. Schmidt, Berlin-Steglitz, Sedanstraße 8,
F. K. Schmidt Heidelberg, Mathematisches Institut,
H. Wielandt, Tübingen, Ob dem Viehweidle 21 b.

Springer-Verlag OHG — Berlin-Wilmersdorf, Heidelberger Platz 3 — Heidelberg, Neuenheimer Landstraße 28/30. — Göttingen, Weender Straße 60.

---

70. Band **Inhalt** 3. Heft

Seite

Hofmann, K. H., Topologische Doppelloops 213

Farahat, H. K., and L. Mirsky, Group Membership in Rings of Various Types . 231

Perron, O., Über zwei ausgeartete Heinesche Reihen und einen Kettenbruch von Ramanujan 245

Dekker, J. C. E., The Factorial Function for Isols 250

Kasch, F., Über eine metrische Eigenschaft der S-Zahlen 263

Fan, K., On the Equilibrium Value of a System of Convex and Concave Functions 271

Zaremba, S. K., On Necessary Conditions for the Central Limit Theorem 281

Benz, W., (8_3, 6_4)-Konfigurationen in Laguerre-, Möbius- und weiteren Geometrien 283

HOFMANN, K. H.
Math. Zeitschr. Bd. 70, S. 213–230 (1958)

Topologische Doppelloops

Von
KARL HEINRICH HOFMANN

Diese Arbeit ist eine Fortsetzung der Untersuchung zunächst nicht notwendig assoziativer topologisch-algebraischer Strukturen, die in zwei vorhergegangenen Arbeiten[1]) vorwiegend von Strukturen mit einer Verknüpfung handelte und nun auf Strukturen mit zwei Verknüpfungen vom ring- oder körperartigen Typ ausgedehnt werden soll. Die Terminologie bleibt dieselbe wie in jenen Arbeiten. Die römischen Ziffern I und II bei Hinweisen auf Textstellen beziehen sich auf die erste bzw. die zweite der erwähnten beiden vorausgegangenen Arbeiten.

§ 1. Ringartige Strukturen und Doppelloops

(1.1) Auf den im folgenden betrachteten algebraischen Strukturen K sind stets zwei Verknüpfungen definiert: Erstens eine als Addition bezeichnete Verknüpfung $(x, y) \to x + y$; K sei bezüglich dieser Verknüpfung stets eine Loop; es gibt dann zu x und y immer zwei Elemente u und v mit $x + u = y$ bzw. $v + y = x$, die wir mit $u = -x + y$ bzw. mit $v = x - y$ bezeichnen. Zweitens ist eine als Multiplikation bezeichnete Verknüpfung $(x, y) \to xy$ erklärt; es gelte stets $x0 = 0x = 0$ (wobei mit 0 das neutrale Element der Addition bezeichnet ist), und diese Verknüpfung habe ein beiderseits neutrales Element e. In der Regel werden wir solche Strukturen K betrachten, in denen sogar $K - \{0\}$ bezüglich $(x, y) \to xy$ eine Loop bildet; eine algebraische Struktur dieser Eigenschaft nennen wir mit PICKERT [3], S. 61 eine *Doppelloop*, während wir eine Struktur mit zwei Verknüpfungen ohne diese scharfe Forderung über die Multiplikation eine *ringartige Struktur* nennen. Was unter einer *topologischen ringartigen Struktur* bzw. unter einer *topologischen Doppelloop* zu verstehen sei, geht unmittelbar aus I, (2.1) hervor.

(1.2) Die von den Rechtsmultiplikationen $x \to xa$ $(a \neq 0)$ erzeugte Transformationsgruppe einer ringartigen Struktur $(K, +, .)$ nennen wir gelegentlich $\mathfrak{R}$, die von den Linksmultiplikationen $x \to ax$ $(a \neq 0)$ erzeugte $\mathfrak{L}$ und schließlich die von beiden Typen von Translationen erzeugte Gruppe $\mathfrak{Z}$. Eine ringartige Struktur $(K, +, .)$ nennen wir *rechtsdistributiv*, wenn alle Rechtsmultiplikationen, *linksdistributiv*, wenn alle Linksmultiplikationen und *zweiseitig distributiv* (oder *distributiv* schlechthin) wenn Rechts- und Linksmultiplikation Endomorphismen der additiven Struktur $(K, +)$ darstellen.

Ein Normalteiler J der additiven Struktur $(K, +)$ heißt ein *Rechtsideal*, wenn er von $\mathfrak{R}$, ein *Linksideal*, wenn er von $\mathfrak{L}$ und ein *zweiseitiges Ideal* oder

[1]) Topologische Loops, Math. Z. **70**, 13–37 (1958); Topologische Loops mit schwachen Assoziativitätsforderungen, Math. Z. **70**, 125–155.

Ideal schlechthin, wenn er von $\mathfrak{Z}$ in sich übergeführt wird. *Ein charakteristischer Normalteiler von* $(K, +)$ *in einer rechtsdistributiven ringartigen Struktur* $(K, +, .)$ *ist stets ein Rechtsideal.* Entsprechendes gilt für die Begriffe „links" und „zweiseitig".

In einer Doppelloop $(K, +, .)$ *gibt es außer* $\{0\}$ *und* K *keine Rechts-, Links- oder zweiseitigen echten Ideale:*

Es sei J ein von $\{0\}$ verschiedenes Rechtsideal. x sei ein beliebiger von 0 verschiedener Punkt von K und a ein beliebiger von 0 verschiedener Punkt von J. Es existiert dann genau ein Element $u \in K$, so daß $au = x$. Die Abbildung $y \to yu$ bildet aber J in sich ab. Also liegt x in J und damit K in J.

In einer zweiseitig distributiven ringartigen Struktur $(K, +, .)$ sind die zweiseitigen Ideale J gerade die Kerne von Homomorphismen h von K in eine algebraische Struktur. Es gilt dann nämlich für ein zweiseitiges Ideal $(x+J)(y+J) = (xy+J)$, so daß $(K, +)/J$ mit der Multiplikation $\big((x+J), (y+J)\big) \to (x+J)(y+J)$ zu einem homomorphen Bild von $(K, +, .)$ wird. Es sei umgekehrt h ein auf K definierter Homomorphismus. $J = h^{-1}\big(h(0)\big)$ ist dann ein Ideal: J ist jedenfalls ein $+$-Normalteiler. Jx wird durch h auf $h(Jx) = h(J)\,h(x) = h\big(h^{-1}(h(0))\big)\,h(x) = h(0)$ abgebildet, d.h. Jx liegt in $h^{-1}\big(h(0)\big) = J$. Dieser zweite Teil des Beweises gilt ohne Distributivitätsvoraussetzungen; d.h. jeder Kern eines Homomorphismus ist ein Ideal.

(1.3) $(K, +, .)$ *sei eine topologische Doppelloop. Dann ist* K *entweder zusammenhängend oder nirgends zusammenhängend (also auch insbesondere total unzusammenhängend).*

BEWEIS. $Z'(0)$ sei die Quasikomponente von 0 in K. $Z'(0)$ ist ein charakteristischer $+$-Normalteiler [II, (5.9)]. Die Abbildung $z \to zx$ $(x \neq 0)$ ist eine homöomorphe Abbildung f von $Z'(0)$ in K; das Bild von $Z'(0)$ enthält 0, und umfaßt $Z'(0)$; denn $Z'(0) = \bigcap \{U;\, U \in \mathfrak{U}(0),\, U$ ist abgeschlossen und offen$\}$ und $f\big(Z'(0)\big)$ ist wieder ein Durchschnitt von offenen und abgeschlossenen Mengen der 0 enthält. Ebenso folgt aber auch $f^{-1}\big(Z'(0)\big) = Z'(0)$ und daraus $Z'(0) = f\big(Z'(0)\big)$; es gilt also $Z'(0) = f\big(Z'(0)\big)$. Dann ist aber $Z'(0)$ ein Rechtsideal und stimmt daher mit $\{0\}$ oder K überein.

(1.4) *In einer topologischen ringartigen Struktur sind die Zusammenhangskomponente* $Z(0)$ *und die Quasikomponente* $Z'(0)$ *des Punktes* 0 *zweiseitige Ideale.*

BEWEIS. Wie unter (1.3).

(1.5) $(K, +, .)$ sei eine lokalkompakte Doppelloop. Dann ist K nicht kompakt. Die Abbildung $x \to x\backslash e$ hat eine eindeutige Fortsetzung zu einem Homöomorphismus g der Einpunktkompaktifizierung $K \cup \{a\}$ auf sich mit $g(0) = a$ und $g(a) = 0$.

BEWEIS. $\mathfrak{U}'(0)$ bestehe aus den Mengen $U - \{0\}$ mit $U \in \mathfrak{U}(0)$. Das Bild von $\mathfrak{U}'(0)$ bei $x \to x\backslash d$ (mit beliebigem $d \neq 0$ aus K) hat keine Adhärenzpunkte in K; denn für jede gegen 0 konvergierende Filterbasis $\mathfrak{B}$ mit $\lim_{\mathfrak{B}} x\backslash d = k$ gilt $d = \lim_{\mathfrak{B}} x\,(x\backslash d) = \lim_{\mathfrak{B}} x \lim_{\mathfrak{B}} x\backslash d = 0 \cdot k = 0$ im Widerspruch zur Wahl von d.

Nun sei $K\cup\{a\}$ die Einpunktkompaktifizierung von K. Das Bild von $\mathfrak{U}'(0)$ bei $x\to x\backslash d$ hat keinen Adhärenzpunkt in K, muß aber in dem kompakten Raum $K\cup\{a\}$ wenigstens einen solchen besitzen; dieses Bild konvergiert also gegen a. In derselben Weise konvergiert das Bild von $\mathfrak{U}'(0)$ bei $x\to d/x$ (mit beliebigem $d\neq 0$ aus K) gegen a. Die beiden Abbildungen

$$x\to g(x)=\begin{cases} a & \text{für } x=0\\ x\backslash e & \text{für } x\in K-\{0\}\\ 0 & \text{für } x=a,\end{cases}\quad\text{und}$$

$$x\to \bar{g}(x)=\begin{cases} a & \text{für } x=0\\ e/x & \text{für } x\in K-\{0\}\\ 0 & \text{für } x=\mathrm{a}\end{cases}\quad\text{sind}$$

eineindeutige und auf K stetige Abbildungen von $K\cup\{a\}$ auf sich, und die eine ist die Umkehrabbildungen der anderen. Da $\bar{g}$ in 0 stetig ist, gibt es zu jeder offenen Umgebung U von a in $K\cup\{a\}$ mit $0\notin\overline{U}$ eine Umgebung V von 0, so daß $V\subseteq g(U)$; d.h. g ist in a offen und bildet U eineindeutig und offen in $K\cup\{a\}$ ab. Ist $\overline{U}$ kompakt, so wird $\overline{U}_0=\overline{U}\cup\{0\}$ durch g eineindeutig relativ offen, also homöomorph auf $g(\overline{U})\in\mathfrak{U}(0)$ abgebildet, denn $g(\overline{U}_0)=g(\overline{U}-\{a\})\cup\{0\}\cup\{a\}$ ist abgeschlossen (und daher kompakt), weil g auf $K-\{0\}$ einen Homöomorphismus auf sich darstellt. g und dann auch $\bar{g}$ sind also überall stetige und sogar homöomorphe Abbildungen von $K\cup\{a\}$ auf sich.

(1.6) *Eine lokalkompakte, zusammenhängende Doppelloop ist lokalzusammenhängend.*

Beweis. $(K,+,.,\mathfrak{O}(K))$ erlaubt eine Verfeinerung der Topologie $\mathfrak{O}(K)$ zu $\mathfrak{O}'(K)$ derart, daß $(K,+,.,\mathfrak{O}'(K))$ eine lokalkompakte, lokalzusammenhängende und wegen (1.3) zusammenhängende Doppelloop bildet [I, (5.15)]. U sei eine kompakte Umgebung von 0 in der alten Topologie; in der neuen Topologie ist U eine Vereinigung $\cup\{U_i;\,i\in I\}$ von kompakten punktfremden Umgebungen U_i. Angenommen $\mathfrak{U}(0)$ würde die Zusammenhangskomponente U_{i_0} von 0 in U nicht enthalten. Dann enthielte jedes $V\in\mathfrak{U}(0)$ ein x_{i_V} aus einem $U_{i_V}\neq U_{i_0}$. Die Menge $I'=(i_V;\,V\in\mathfrak{U}(0))$ ist durch $\leqq$ gefiltert gemäß der Angabe, daß $i_V\leqq i_{V'}$ genau gilt, wenn $V\subseteq V'$ gilt. Wir haben $\lim\limits_{i\in I} x_i=0$ in der alten Topologie; in der neuen kann $(x_i)_{i\in I}$ kein konvergentes Unternetz $(x_i)_{i\in I}$ besitzen; denn in der neuen Topologie ist der Teilraum $\{x_i;\,i\in I\}$ diskret, da jedes x_i in einer offenen Menge U_i liegt, die kein Element x_j mit $j\neq i$ enthält. Es gilt also $\lim\limits_{i\in I'} x_i=a$, wenn $K\cup\{a\}$ die Kompaktifizierung von K in der neuen Topologie bezeichnet. Daraus folgt aber $\lim\limits_{i\in I} x_i\backslash e=0$ in der neuen Topologie und erst recht in der alten. Dies ist aber ein Widerspruch zu der Gültigkeit von $\lim\limits_{i\in I'} x_i=0$ in der alten Topologie. Demnach muß U_{i_0} eine Umgebung von 0 sein, und da U beliebig gewählt war, besitzt $\mathfrak{U}(0)$ eine Basis aus zusammenhängenden Umgebungen.

(1.7) $(K, +, .)$ sei eine ringartige Struktur. Unter dem *Ringzentrum* H von K verstehen wir diejenige Menge von Elementen $x \in K$, die aus der Null und allen x besteht, die im Zentrum von $(K, +)$ liegen und für alle $(a, b) \in K \times K$ die Identitäten $xa = ax$, $(ab)x = a(bx) = (ax)b$ erfüllen. Das Ringzentrum ist eine Unterstruktur und ein $+$-Normalteiler. Ist K eine Doppelloop, so ist $(H - \{0\}, .)$ das Zentrum von $(K - \{0\}, .)$.

(1.8) *$(K, +, .)$ sei eine zusammenhängende ringartige Struktur. H sei ein total unzusammenhängendes Ideal. Dann liegt H im Ringzentrum von K.*

BEWEIS. H ist ein $+$-Normalteiler. Es sei $a \in H$. Dann ist $x \to xa - ax$ eine stetige Abbildung von K in H; das Bild ist zusammenhängend und enthält 0, ist also gleich $\{0\}$. Daher gilt $xa = ax$ für alle $x \in K$. Ebenso beweist man die übrigen Identitäten.

(1.9) H sei ein total unzusammenhängendes Ideal einer zusammenhängenden ringartigen Struktur. Für alle $a, b \in H$ und alle $x \in K$ gilt dann $(a+b)x = (ax + bx)$, $x(a+b) = (xa + xb)$; d.h. $\mathfrak{Z}$ ist eine Endomorphismengruppe auf H. Insbesondere folgt, daß jedes total unzusammenhängende Ideal in K ein kommutativer Unterring ist.

BEWEIS. Die Abbildung $x \to (a+b)x - (ax + bx)$ ist eine stetige Abbildung von K in H; das Bild ist zusammenhängend und enthält 0; da e auf 0 abgebildet wird. Dieses Bild muß also mit $\{0\}$ übereinstimmen, woraus die eine der Identitäten folgt. Die andere beweist man analog.

(1.10) *$(K, +, .)$ sei eine ringartige Struktur; sie sei zusammenhängend, lokalzusammenhängend. $(\tilde{K}, +, ., f)$ sei eine einfach zusammenhängende Überlagerungsstruktur von K. Dann enthält das Zentrum von $\tilde{K}$ ein diskretes Ideal $\tilde{H}$, das einen Ring bildet, dessen additive Gruppe der Poincaré-Gruppe von K isomorph ist, und in dem sämtliche Produkte null sind.*

BEWEIS. $(\tilde{K}, +, ., f)$ sei die einfach zusammenhängende Überlagerungsstruktur von K. Dann ist $(\tilde{K}, +)$ eine Loop mit neutralem Element $\tilde{0}$. Ferner bildet $(\tilde{K}, .)$ eine Struktur mit der Verknüpfung $(\tilde{x}, \tilde{y}) \to \tilde{x}\tilde{y}$. Es gibt ein Element $\tilde{e} \in f^{-1}(e)$, so daß $\tilde{x}\tilde{e} = \tilde{e}\tilde{x} = \tilde{x}$. Die Abbildung $\tilde{x} \to \tilde{0}\tilde{x}$ bildet den zusammenhängenden Raum $\tilde{K}$ in den diskreten Raum $\tilde{H} = f^{-1}(0)$ ab und ist daher konstant: $\tilde{0}\tilde{x} = \tilde{c}$. Wie im Beweis von (1.9) überlegt man, daß für alle $\tilde{a}$ und $\tilde{b}$ aus $\tilde{H}$ und alle $\tilde{x}$ aus $\tilde{K}$ stets $(\tilde{a} + \tilde{b})\tilde{x} = \tilde{a}\tilde{x} + \tilde{b}\tilde{x}$ gilt. Mit $\tilde{a} = \tilde{b} = \tilde{0}$ folgt daraus insbesondere $\tilde{c} + \tilde{c} = \tilde{c}$, was aber $\tilde{c} = \tilde{0}$ nach sich zieht. Ebenso beweist man $\tilde{x}\tilde{0} = \tilde{0}$. Nun ist also $(\tilde{K}, +, .)$ eine ringartige Struktur, und f ein Homomorphismus von $\tilde{K}$ auf K. Der Kern $\tilde{H} = f^{-1}(0)$ ist ein im Ringzentrum gelegenes diskretes Ideal. Es sei $a \in H$. Dann gilt für alle $\tilde{x}$ stets $f(\tilde{x}\tilde{a}) = 0$ und überdies ist $\tilde{0} \cdot \tilde{a} = \tilde{0}$. Die Abbildungen $\tilde{x} \to \tilde{0}$ und $\tilde{x} \to \tilde{x}\tilde{a}$ von $\tilde{K}$ in $\tilde{K}$ haben dieselben im Sinne von I, (6.2) eindeutig kennzeichnenden Eigenschaften und stimmen daher überein. (Derselbe Schluß wurde in I, § 6 wiederholt angewandt.)

(1.11) Nun erfülle $(K, +, .)$ die Voraussetzungen von (1.10) und sei überdies eine Doppelloop. Dann ist für jedes $\tilde{a} \notin \tilde{H}$ die Abbildung $\tilde{x} \to \tilde{x}\,\tilde{a}$ eine eineindeutige Abbildung „auf".

BEWEIS. Zu jedem $\tilde{a} \notin \tilde{H}$ existiert eine Abbildung $\tilde{x} \to \tilde{x}/\tilde{a}$ von $\tilde{K}$ in sich derart, daß $f(\tilde{x}/\tilde{a}) = f(\tilde{x})/f(\tilde{a})$, daß $\tilde{a}/\tilde{a} = \tilde{e}$ und daß $(\tilde{x}/\tilde{a})\tilde{a} = \tilde{x}$ gilt (in der Tat: $\bar{x} \to (\tilde{x}/\tilde{a})\,\tilde{a}$ hat die Eigenschaft, daß $f((\tilde{x}/\tilde{a})\,\tilde{a}) = f(\tilde{x})$ und $(\tilde{a}/\tilde{a})\,\tilde{a} = \tilde{a}$, woraus die Behauptung folgt). Insbesondere folgt aus dem Gesagten die Gleichung $\tilde{0}/\tilde{a} = \tilde{0}$. In genau analoger Weise kann man $(\tilde{x}\,\tilde{a})/\tilde{a} = \tilde{x}$ zeigen. Die Abbildung $R_{\tilde{a}} = (\tilde{x} \to \tilde{x}\,\tilde{a})$ besitzt also eine Umkehrabbildung $R_{\tilde{a}}^{-1}$, d.h. $R_{\tilde{a}}^{-1} \circ R_{\tilde{a}} = R_{\tilde{a}} \circ R_{\tilde{a}}^{-1}$ ist die identische Abbildung.

(1.12) *Eine zusammenhängende, lokalzusammenhängende, lokal einfach zusammenhängende topologische Doppelloop K ist einfach zusammenhängend.*

BEWEIS. Die Bezeichnungen seien dieselben wie in (1.10) und (1.11). Für $\tilde{a} \notin \tilde{H}$ ist $\tilde{x} \to \tilde{x}\tilde{a}$ ein Homöomorphismus von $\tilde{K}$ auf sich. Aus $\tilde{H}\tilde{a} = \{0\}$ folgt dann aber $\tilde{H} = \{0\}$, w.z.b.w.

Nach einer Bemerkung von I, § 6 gilt auch der folgende Satz, in dem unter dem Begriff des einfachen Zusammenhangs der dort erwähnte Begriff zu verstehen ist:

Eine topologische kurvenzusammenhängende Doppelloop K ist einfach zusammenhängend (im Sinne von R. NOVOSAD).

Insbesondere ist jede zu R lokal homöomorphe Doppelloop zu R homöomorph. Es hätte ausgereicht, in (1.11) und (1.12) K als nullteilerfreie ringartige Struktur vorauszusetzen, d.h. als ringartige Struktur, in der aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt.

(1.13) *Sämtliche Sätze über Doppelloops, soweit sie bislang angegeben wurden, gelten für Strukturen $(K, +, .)$ folgender Art: K sei bezüglich $+$ eine Quasigruppe; in K existiere ein Element a derart, daß $(K\{a\}, .)$ eine Quasigruppe bildet und daß $ax = xa = a$ für alle $x \in K$ richtig ist.*

Der Beweis folgt aus einer Bemerkung von I, (1.3).

(1.12) liefert einen einfachen Beweis für einen Satz von SALZMANN [*4*, S. 455].

§ 2. Eindimensionale Doppelloops

In allen im folgenden betrachteten ringartigen Strukturen ist die additive Loop stets mindestens lokal monassoziativ, in der Regel sogar potenzassoziativ; ferner beschränken wir uns auf lokalkompakte Strukturen und solche, die wenigstens linksdistributiv sind. Die ringartigen Strukturen seien stets *nullteilerfrei*, d.h. aus $xy = 0$ folge stets $x = 0$ oder $y = 0$.

(2.1) Existiert in einer linksdistributiven Doppelloop K auch nur ein von 0 verschiedenes monassoziatives (bzw. potenzassoziatives) Element a, (wobei sich die Begriffe monassoziativ bzw. potenzassoziativ auf die Addition beziehen), so ist $(K, +)$ monassoziativ (bzw. potenzassoziativ).

BEWEIS. Da $\mathfrak{L}$ eine Automorphismengruppe bildet, liegen in Ka nur monassoziative (bzw. potenzassoziative) Elemente. Da K Doppelloop ist, gilt aber $Ka = K$.

Wenn wir also in Zukunft in linksdistributiven Doppelloops die Additionsloop monassoziativ (bzw. potenzassoziativ) voraussetzen, so hätte es auch ausgereicht, die Monassoziativität (bzw. Potenzassoziativität) eines einzigen von 0 verschiedenen Elementes zu fordern.

(2.2) *$(K, +, \circ)$ sei eine linksdistributive $+$ — monassoziative Doppelloop, die lokal einem reellen Intervall homöomorph sei* (die also in Wirklichkeit sogar zu R homöomorph ist). *Dann enthält $(K - \{0\}, \circ)$ einen Normalteiler K' vom Index 2* (d.h. einen Normalteiler dessen Restklassenstruktur aus zwei Elementen besteht), *der zur multiplikativen Gruppe der positiven reellen Zahlen isomorph ist, sowie eine Untergruppe A aus zwei Elementen, so daß $(K - \{0\}, \circ) = A \circ K'$.*

BEWEIS. $(K, +)$ enthält zwei verschiedene zu R_+ isomorphe Halbgruppen H_1 und H_2 mit dem Durchschnitt $\{0\}$ II, (6.4). Die Abbildungen $x \to a \circ x$ sind für $a \neq 0$ Automorphismen von $(K, +)$ und Isomorphismen von H_n auf H_m (wobei n und m unabhängig die Menge der Ziffern 1 und 2 durchlaufen). Das Element e sei in H_1 enthalten. f sei ein Isomorphismus von R_+ auf H_1 mit $f(1) = e$. Die sämtlichen Automorphismen von H_1 entsprechen eineindeutig sämtlichen Automorphismen von R_+, und diese sind gerade die Abbildungen $r \to sr$ $(s \in R_+, s \neq 0)$ von R_+ auf sich. Jeder Automorphismus von H_1 hat die Form $x \to f(sf^{-1}(x))$. Wir bezeichnen die Klasse aller Elemente $a \in K$, die durch $x \to a \circ x$ einen Automorphismus von H_1 definieren, mit K'. Zu jedem a aus K' gibt es genau ein reelles $s(a) \in R_+$, so daß $a \circ x = f(s(a) f^{-1}(x))$. Somit gilt, falls a und b beide in K' liegen, $b \circ (a \circ x) = b \circ (f(s(a) f^{-1}(x))) = f(s(b) f^{-1}(f(s(a) f^{-1}(x))))$ $= f(s(b)\, s(a)\, f^{-1}(x)) = a \circ (b \circ x)$. Setzt man $x = e$, so folgt zunächst $a \circ b = b \circ a$. Für ein Tripel a, b, c von Elementen aus K' gilt somit $a \circ (b \circ c) = a \circ (c \circ b) = c \circ (a \circ b) = (a \circ b) \circ c$; zu einem Element $a \in K'$ gibt es ein $a' \in K$ mit $a' \circ a = e$; dann ist aber die Abbildung $x \to a' \circ x$ ein Automorphismus von H_1 und a' liegt in K'. Die Menge K' bildet also eine Gruppe, die durch $x \to s(x)$ isomorph auf die multiplikative Gruppe von $R_+ - \{0\}$ abgebildet wird; zu jedem $s \neq 0$ aus R_+ gibt es ja ein $a \in K'$, so daß $s = s(a)$; man braucht dazu ja nur $a = f(s)$ zu setzen. K' ist also eine zusammenhängende Untergruppe von $(K - \{0\}, \circ)$, die zu $(R_+ - \{0\}, .)$ und damit auch zu $(R, +)$ isomorph ist. Die Zusammenhangskomponente von e in $(K - \{0\}, \circ)$ ist $H_1 - \{0\}$ und bildet eine zu R homöomorphe Unterloop, die K' enthält. K' ist in $H_1 - \{0\}$ ein offenes, e enthaltendes Intervall. $(H_1 - \{0\}, \circ)$ ist also lokal potenzassoziativ und ist nach II, (6.4) eine Einparametergruppe, die dann aber mit K' übereinstimmen muß. Nun sei g ein Isomorphismus der additiven Halbgruppe R_+ auf H_2. Die Abbildung $r \to p(r)$, die einen Element r aus $R_+ - \{0\}$ das eindeutig bestimmte Element $p(r) \in R_+ - \{0\}$ zu ordnet, für welches $g(r) \circ g(p(r)) = e$ gilt, ist ein Homöomorphismus von $R_+ - \{0\}$ auf sich, $g(R_+ - \{0\}) \backslash e$ ist nämlich in H_2 enthalten und stimmt sogar mit H_2 überein. Nach (1.5) strebt $p(r)$

gegen ∞, wenn r gegen 0 strebt. $r \to p(r)$ ist also monoton fallend und es gibt genau ein r_0 mit $r_0 = p(r_0)$. Das Element $\bar{e} = g(r_0)$ liegt in $H_2 - \{0\}$ und genügt der Gleichung $\bar{e} \circ \bar{e} = e$. Die Gruppe $\{e, \bar{e}\}$ sei mit A bezeichnet. Dann gilt in der Tat $(K - \{0\}, \circ) = A \circ K'$. Die Gruppe K' ist als Zusammenhangskomponente des neutralen Elements e von $(K - \{0\}, \circ)$ ein Normalteiler, der den Index 2 hat, weil $K - \{0\}$ aus genau zwei Zusammenhangskomponenten besteht. K' ist, um das nocheinmal zu wiederholen, isomorph zur additiven Gruppe der reellen Zahlen. Aus dem bisher Bewiesenen braucht nun noch nicht zu folgen, daß $(K - \{0\}, \circ)$ zur multiplikativen Gruppe der reellen Zahlen isomorph ist. Es sei z.B. $(R - \{0\}, .)$ die multiplikative Gruppe des Körpers der reellen Zahlen.

Die Verknüpfung $x \circ y = \begin{cases} xy, & \text{wenn } x \geqq 0, \quad \text{oder} \quad y \geqq 0 \\ 4xy, & \text{wenn } x < 0, \quad \text{und} \quad y < 0 \end{cases}$

hat mit $e = 1$ und $\bar{e} = -\frac{1}{2}$ alle oben abgeleiteten Eigenschaften ohne assoziativ zu sein. Zusammen mit der in II, (6.3) genannten Verknüpfung als Addition wird $(R, +, \circ)$ zu einer Doppelloop mit kommutativer monassoziativer Addition und kommutativer lokal assoziativer Multiplikation, die in beiden Verknüpfungen nicht assoziativ ist, die allerdings auch im Großen kein Distributivgesetz erfüllt. Die Loop $(R - \{0\}, \circ)$ ist bemerkenswert als Beispiel einer nichtassoziativen Loop, die eine abelsche Gruppe als Normalteiler vom Index 2 besitzt, deren Faktorgruppe nach diesem Normalteiler also eine abelsche Gruppe der Ordnung 2 bildet.

Die Gültigkeit des linksdistributiven Gesetzes erlaubt aber die Ableitung des schärferen Ergebnisses:

(2.3) *Unter den Voraussetzungen von* (2.2) *ist* $(K - \{0\}, \circ)$ *isomorph zur multiplikativen Gruppe des Körpers der reellen Zahlen.*

Beweis. Es sei h ein Automorphismus von $(K, +)$, der dann H_n auf H_m isomorph abbildet (wobei offen bleibe, wie die Abbildung $n \to m(n)$ der Menge (1, 2) auf sich beschaffen sei). Dann ist h durch die Angabe von $h(e)$ und $h(\bar{e})$ schon eindeutig bestimmt. Denn so hat z.B. jeder Isomorphismus von H_2 auf H_1 die Form $x \to f\left(sg^{-1}(x)\right)$ mit einem $s \in R_+ - \{0\}$; genau Entsprechendes gilt für alle anderen Fälle. Auf H_1 stimmt h also mit $x \to h(e) \circ x$ und auf H_2 mit $x \to h(\bar{e}) \circ (\bar{e} \circ x)$ überein. Unter $x \to \bar{x}$ sei die Abbildung $x \to \bar{e} \circ x$ verstanden; es gilt also $\bar{x} = \bar{e} \circ x$. Die Abbildung $x \to \bar{\bar{x}}$ ist ein Isomorphismus von H_n auf sich $(n = 1, 2)$ mit $\bar{\bar{e}} = e$ und $\overline{(\bar{e})} = \bar{e}$.

Die Abbildung $x \to \bar{\bar{x}}$ stimmt also mit dem identischen Automorphismus überein, d.h. $x \to \bar{x}$ ist ein involutorischer Automorphismus. Für einen beliebigen Automorphismus h von $(K, +)$ gilt also

$$h(x) = \begin{cases} h(e) \circ x, & \text{wenn} \quad x \in H_1 \\ h(\bar{e}) \circ \bar{x}, & \text{wenn} \quad x \in H_2. \end{cases}$$

Nun sei $x \in H_2$ fest gewählt, $x \neq 0$. Wir suchen ein Element $y \in H_1$ so, daß $x + y \in H_1$ gilt; diese Wahl ist möglich; denn wird K durch a kompakt abgeschlossen, so ist a Adhärenzpunkt von $x + H_1$, und $x + H_1$ enthält das

Element 0. Dann gilt aber $h(x+y)=h(x)+h(y)=h(\bar{e})\circ\bar{x}+h(e)\circ y$. Andrerseits gilt aber unter Benutzung des linksdistributiven Gesetzes $h(x+y)=h(e)\circ(x+y)=h(e)\circ x+h(e)\circ y$, woraus unmittelbar $h(\bar{e})\circ\bar{x}=h(e)\circ x$ folgt. Für jeden Automorphismus h von $(K,+)$ gilt also $h(x)=h(e)\circ x$ für alle $x\in K$.

Die Abbildung $x\to a\circ(b\circ x)$ ist für alle a und b aus $K-\{0\}$ ein Automorphismus von $(K,+)$ und hat die Form $x\to a\circ(b\circ x)=(a\circ b)\circ x$. Dies besagt aber gerade, daß $(K-\{0\},\circ)$ assoziativ ist. Unter diesen Umständen folgt aber in der Tat aus $K-\{0\}=A\circ K'$ die Isomorphie von $(K-\{0\},\circ)$ mit der multiplikativen Gruppe des Körpers der reellen Zahlen, denn $A\circ K'$ ist ein direktes Produkt abelscher Gruppen und ist daher selbst eine abelsche Gruppe. $x\to\bar{e}\circ x\circ\bar{e}$ ist nämlich ein Automorphismus von K', ist also von der Form $x\to s^{-1}(s(x)^{\alpha})$, $(x\to s(x)$ wie in (2.2), $\alpha\neq 0$ reell). Für $x\in K'$ gilt dann $\bar{x}\circ\bar{x}=\bar{e}\circ x\circ\bar{e}\circ x=s^{-1}(s(x)^{\alpha})\circ x$ oder $s(\bar{x}\circ\bar{x})=s(x)^{\alpha}s(x)$. Genau dann gilt $\bar{x}\circ\bar{x}=e$, wenn $1=s(x)^{\alpha}s(x)$, d.h. wenn $\alpha=-1$ oder $x=e$. Da $x\to\bar{x}\circ\bar{x}$ die Gruppe K' wegen $\lim\limits_{x\to 0}\bar{x}\circ\bar{x}=0$ nicht auf e abbildet scheidet $\alpha=-1$ aus. $A=(e,\bar{e})$ ist daher die einzige Untergruppe von $A\circ K'$ mit der Ordnung 2 und ist daher normal. Zur Konstruktion von $\bar{e}$ und um $\alpha=-1$ auszuscheiden, war kein Distributivgesetz erforderlich.

(2.4) *Ist $(K,+,\circ)$ sogar $+$ — potenzassoziativ, so ist K isomorph zum Körper der reellen Zahlen.*

BEWEIS. $(K,+)$ ist isomorph zur additiven Gruppe der reellen Zahlen [II, (6.4)]. Die multiplikative Struktur $(K-\{0\},\circ)$ ist isomorph zur multiplikativen Gruppe des Körpers der reellen Zahlen (2.3)]; und K ist infolge der Kommutativität der Multiplikation distributiv. f sei ein Isomorphismus von $(R,+)$ auf K mit $f(1)=e$. Dann gilt $f(a)\cdot f(b)=f\big(m(a,b)\big)$ mit $m(a,b)=m(b,a)$ und $f\big(m(a,b+c)\big)=f(a)\cdot f(b+c)=f(a)\ \big(f(b)+f(c)\big)=f(a)\cdot f(b)+f(a)\cdot f(c)=f\big(m(a,b)\big)+f\big(m(a,c)\big)=f\big(m(a,b)+m(a,c)\big)$; die Abbildung $(a,b)\to m(a,b)$ genügt also der Funktionalgleichung $m(a+b,c)=m(a,c)+m(b,c)$. Aus $m(a,b)=0$ folgt $a=0$ oder $b=0$ und umgekehrt. $r\to m(r,s)$ ist somit ein Isomorphismus von $(R,+)$ in sich und hat die Form $m(r,s)=p(s)\cdot r$. Ebenso schließt man $m(r,s)=q(r)\cdot s$, woraus dann $m(r,s)=c.\ rs$ folgt mit einer Konstanten c.

Wegen $f(1)f(1)=f(1)$ gilt $m(1,1)=c.\ 1.1=1$, also $c=1$. Wir haben damit die Gültigkeit der Funktionalgleichung $f(a)f(b)=f(ab)$ nachgewiesen und damit den Beweis vollendet.

(2.5) *Es gibt eine distributive in beiden Verknüpfungen kommutative Doppelloop, die zu R homöomorph ist, und deren multiplikative Loop der multiplikativen Gruppe des Körpers der reellen Zahlen isomorph ist.*

BEWEIS. Man nehme den Körper der reellen Zahlen und darin als Addition die in II, (6.3) benützte Verknüpfung

$$x\wedge y=\begin{cases} x+y\ , & \text{falls } xy\geqq 0,\\ \dfrac{x^3+y^3}{x^2+y^2}\ , & \text{falls } xy<0.\end{cases}$$

$(R,\wedge,.)$ ist distributiv.

Zusammenfassend formulieren wir folgenden SATZ:

(2.6) *Die Multiplikationsloop einer linksdistributiven, additiv monassoziativen, lokal zu einem reellen Intervall homöomorphen Doppelloop ist isomorph zur multiplikativen Gruppe der reellen Zahlen. Ihre Additionsloop braucht nicht assoziativ zu sein, sie ist dann assoziativ, wenn sie wenigstens potenzassoziativ vorausgesetzt wird.*

ANMERKUNGEN. Bei den Sätzen (2.2) und (2.3) ist bemerkenswert, daß abgesehen von der Koppelung der Addition und Multiplikation durch das Distributivgesetz über die Multiplikation nichts vorausgesetzt wurde, daß aber gerade über die Multiplikation voller Aufschluß erzielt wurde, während die Information über die Addition trotz der über sie gemachten Voraussetzungen unvollkommen bleiben mußte. Diese Erscheinung werden wir noch öfters antreffen. Diese Sätze bleiben auch richtig, wenn $(K, +, 0)$ nur als ringartige Struktur vorausgesetzt wird. (2.5) ist ein einfaches Beispiel eines kommutativen Neokörpers (s. z.B. [3]). Das Hauptergebnis dieses Paragraphen könnten wir auch in folgender Form angeben: Jede zu R lokal homöomorphe, linksdistributive ringartige topologische Struktur mit monassoziativer Addition ist ein Neokörper mit reeller Multiplikationsgruppe. SALZMANN beweist in [4], daß die multiplikative Gruppe eines zu R homöomorphen Neokörpers zur multiplikativen Gruppe von R isomorph ist, setzt dabei freilich die Assoziativität der multiplikativen Loop schon voraus.

§ 3. Die Charakteristik ringartiger Strukturen

(3.1) Wir sagen, eine nullteilerfreie ringartige Struktur $(K, +, .)$ habe die *Charakteristik* n, wenn sie $+$-potenzassoziativ und linksdistributiv ist, und wenn n die kleinste natürliche Zahl bezeichnet, so daß $n \cdot e = (e + \cdots + e) = 0$, falls eine solche existiert; andernfalls sei $n = 0$. Die von den Vielfachen von e gebildete Untermenge P ist ein Unterring von K, der zum Ring der ganzen Zahlen modulo n isomorph ist. In der Tat ist $(n \cdot e)(m \cdot e) = m \cdot (n \cdot e) = nm \cdot e$. In einer Doppelloop ist die Charakteristik n eine Primzahl p und es gilt $p \cdot a = 0$ für alle $a \in K$. Hier ist P isomorph dem Primkörper der Charakteristik p. Für alle $a \in P$ und alle $(y, z) \in K \times K$ gilt $y(za) = y(m \cdot z) = m \cdot (yz) = (yz) \cdot a$. Ist K sogar distributiv, so gilt auf Grund desselben Prinzips mit einer gewissen natürlichen Zahl m auch $(yz)a = y(za) = y(m \cdot z) = y(az) = (m \cdot y)z = (a \cdot y) \cdot z = m \cdot (yz) = a(yz)$, d.h. P liegt im Zentrum von $(K - \{0\}, .)$.

(3.2) *K sei eine linksdistributive Doppelloop endlicher Charakteristik. Dann ist K diskret oder $\mathfrak{U}(0)$ besitzt eine Basis aus Umgebungen, die Vereinigung von zyklischen $+$-Untergruppen sind.*

BEWEIS. Aus $ya = zb$ [wobei $(y, z) \in K \times K$, $(a, b) \in P \times P$, $a \neq 0$, $b \neq 0$] folgt nach dem eben Bewiesenen stets $y = zc$ mit $c = ba^{-1} \in P$. Es gibt also eine natürliche Zahl n $(0 \leqq n < p)$, so daß $y = n \cdot z$. Ist $n \neq 0$, so existiert ein m $(0 \leqq m < p)$, so daß $mn \equiv 1$ (p); d.h. es gilt $m \cdot y = z$. Ist nun $(y_i)_{i \in I}$ ein gegen 0 konvergierendes Netz mit $y_i \neq 0$, so gilt $\lim_{i \in I} z_i = 0$ für alle Netze $(z_i)_{i \in I}$ derart, daß $z_i \in y_i P$. Denn für jede Umgebung $U \in \mathfrak{U}(0)$ und für jedes n $(n = 0, \ldots p - 1)$ gibt es ein $i_n \in I$ derart, daß $n \cdot y_i U$ für $i > i_n$. Nun wähle man $i' = \max(i_0, i_1, \ldots i_{p-1})$. Dann liegen alle Elemente $m \cdot y_i$ $(m = 0, \ldots, p - 1, i > i')$ in U. Wegen $z_i = n_i \cdot y_i$ $(n_i = 0, \ldots, p - 1)$ ist dies die Behauptung. Ist U also eine fest vorgegebene Umgebung, so gibt es eine Umgebung $V \in \mathfrak{U}(0)$,

so daß für alle $W \subseteqq V$ stets $WP \subseteqq U$ gilt. Die Menge $\{WP;\ W \in \mathfrak{U}(0)\}$ bildet also eine Basis von $\mathfrak{U}(0)$.

(3.3) *$(K, +, .)$ sei eine nicht diskrete lokalkompakte linksdistributive nullteilerfreie ringartige Struktur. $(K, +)$ sei potenzassoziativ und eudoxisch* [II, 1.3)]. *Ist nun K $+$-alternativ lokal euklidisch oder aber eine Doppelloop, so hat K ein zusammenhängendes offenes Ideal H* (welches natürlich im zweiten Fall mit K übereinstimmt), *in welchem jeder Punkt auf einer $+$-Einparametergruppe isomorph zu R liegt.*

BEWEIS. K hat keine endliche von 0 verschiedene Charakteristik [(3.2)] und ist nicht totalunzusammenhängend [II, (1.4)]. Es sei U eine offene Umgebung von 0, die frei ist von nichttrivialen $+$-Untergruppen. Der Punkt x sei im Innern von U gelegen, und es sei $n \cdot x$ in U enthalten. In $\mathfrak{U}(e)$ gibt es eine Umgebung W, für die $n \cdot (xW) \subseteqq U$. Es sei $n \cdot x = n \cdot y$ mit $y \in xW$; dann gilt ja $n \cdot x = x(n \cdot e) = x(n \cdot w)$ mit einem $w \in W$ oder $0 = x \cdot (n \cdot w) + x\left((-n) \cdot e\right) = x \cdot (n \cdot w - n \cdot e) = 0$, woraus wegen der Nullteilerfreiheit $n \cdot (w - e) = 0$, oder wegen der nicht endlichen Charakteristik $w = e$ und $x = y$ folgt. Ist nun K lokal euklidisch und $+$-alternativ, so ist $(K, +)$ potenzoffen [II, (5.7)]. Dann liegt nach II, (5.6) jeder Punkt in U auf einer $+$-Einparametergruppe. Einfacher liegt der Fall, wenn K eine Doppelloop ist: Es existiert wenigstens eine $+$-Einparametergruppe in $(K, +)$ [II, (5.1)], zu ihr gehöre der stetige algebraische Isomorphismus f von R in K. Es liege etwa der Punkt a auf ihr. Dann liegt der beliebige Punkt b auf der $+$-Einparametergruppe, die durch den stetigen algebraischen Isomorphismus $r \to (b/a) f(r)$ von R in K definiert ist.

(3.4) *$(K, +, .)$ erfülle die Voraussetzungen von* (3.3) *und sei darüber hinaus distributiv und zusammenhängend. Bezeichnet man mit f den stetigen algebraischen Isomorphismus von R in K, der 1 auf e abbildet, so liegt $f(R)$ im Zentrum von $(K,.)$ und ist insbesondere isomorph zum Körper der reellen Zahlen.*

BEWEIS. Wir beweisen zunächst unter ausschließlicher Benützung der Linksdistributivität, daß $f(R)$ dem Körper der reellen Zahlen isomorph ist. Es seien $s = q^{-1}p_1$ und $t = q^{-1}p_2$ rationale Zahlen. Dann gilt $f(s)f(t) = \left(p_1 \cdot f(1/q)\right)\left(p_2 \cdot f(1/q)\right) = p_1 p_2 \cdot f(1/q) = f(q^{-1}p_1 p_2)$. f ist also ein Isomorphismus des Körpers der rationalen Zahlen in $f(R)$ und hat als stetige Fortsetzung einen Isomorphismus des Körpers R auf $f(R)$.

Ist nun K distributiv, so ist $f(r)a$ mit $a \neq 0$ eine $+$-Einparametergruppe. Die durch die Isomorphismen $s \to (ab)f(s)$, $s \to a\left(bf(s)\right)$, $s \to a\left(f(s)b\right)$, $s \to \left(af(s)\right)b$ $s \to \left(f(s)a\right)b$ und $s \to f(s)(ab)$ definierten $+$-Einparametergruppen laufen sämtlich durch ab und stimmen daher überein, wie man auf Grund der Nullteilerfreiheit leicht einsieht. Damit liegt aber $f(R)$ in der Tat im Zentrum von $(K, .)$. In Zukunft schreiben wir statt $xf(r)$ stets $r \cdot x$ und statt $r \cdot e$ nur r (sog. Ersetzungsverfahren).

(3.5) *$(K, +, .)$ sei eine lokalkompakte zusammenhängende, distributive nullteilerfreie ringartige Struktur; $(K, +)$ sei potenzassoziativ und eudoxisch. Ist*

K lokal euklidisch und $+$-alternativ oder aber eine Doppelloop, so bildet $(K, +)$ zusammen mit der Abbildung $(r, x) \to r \cdot x$ von $R \times K$ in K einen Fastvektorraum.

BEWEIS. Der Beweis ist auf Grund der Definition in II, (8.1) und der in der letzten Nummer bewiesenen Tatsachen trivial.

(3.6) SATZ: *$(K, +, .)$ sei eine lokalkompakte zusammenhängende, distributive nullteilerfreie ringartige Struktur. $(K, +)$ sei eine eudoxische Moufangloop. Ist K lokal euklidisch oder eine Doppelloop, dann ist K eine (möglicherweise nicht assoziative) Algebra endlichen Ranges über dem Körper der reellen Zahlen.* (Unter einer Algebra ist dabei eine Algebra im klassischen Sinne verstanden, ausgenommen, daß vielleicht $(K - \{0\}, .)$ nicht assoziativ ist).

BEWEIS. (3.5) und II, (8.17).

(3.7) SATZ: *$(K, +, .)$ sei eine lokalkompakte, distributive Doppelloop. $(K, +)$ sei eine eudoxische Moufangloop und $(K - \{0\}, .)$ sei eine I-Loop. Dann ist K isomorph entweder zum Körper der reellen Zahlen, zum Körper der komplexen Zahlen, zum Schiefkörper der Quaterionen über dem Körper der reellen Zahlen oder aber zur Cayley-Algebra über dem Körper der reellen Zahlen.*

BEWEIS. Aus dem vorangehenden Absatz und der zusätzlichen Voraussetzung der Kürzbarkeit der Multiplikation [d.h. der I-Loopeigenschaft von I, (1.4)] folgt, daß K ein Alternativkörper endlichen Ranges über dem Körper der reellen Zahlen ist. Daraus folgt die Behauptung (vgl. z. B. PICKERT [3], Kap. 6).

ANMERKUNGEN. Der Satz (3.7) ist eine Verallgemeinerung eines klassischen Satzes von Pontrjagin, der besagt, daß jeder lokalkompakte zusammenhängende Schiefkörper einem Unterkörper eines reellen Quaternionenschiefkörpers isomorph ist. Die additive Gruppe eines lokalkompakten zusammenhängenden Schiefkörpers ist eine zusammenhängende nicht kompakte abelsche Gruppe ohne kompakte Untergruppen und ist also ein n-dimensionaler Vektorraum und damit eudoxisch. Das Ergebnis von (3.6) für ringartige Strukturen benötigte die nicht ganz einfache Satzgruppe II, (5.6) und (5.7).

§ 4. Über die multiplikative Struktur ringartiger Strukturen und einige Kennzeichnungen des Körpers der komplexen Zahlen

(4.1) $(K, +, .)$ sei eine lokalkompakte zusammenhängende distributive nullteilerfreie ringartige Struktur. $(K, +)$ sei eine eudoxische potenzassoziative Loop; ferner sei K lokal euklidisch und $+$-alternativ oder aber eine Doppelloop. Bezeichnen wir wiederum mit f den Isomorphismus von R in K derart, daß $f(1) = e$ und nennen wir L die multiplikative Gruppe $f(R_+ - \{0\})$, so kann ein Restklassenraum $(K - \{0\})/L$ auf $K - \{0\}$ definiert werden. Auf $(K - \{0\})/L$ läßt sich eine Verknüpfung einführen, bezüglich der dieser Restklassenraum eine kompakte topologisch-algebraische Struktur bildet, die homomorphes Bild von $(K - \{0\}, .)$ ist. (Im Falle einer Doppelloop ist letzteres trivial.)

BEWEIS. Die Menge $M = \{xL;\ x \in K - \{0\}\}$ besteht aus Teilmengen xL von $K - \{0\}$; jeder Punkt x von $K - \{0\}$ liegt in wenigstens einer dieser Mengen nämlich in xL; andererseits haben zwei verschiedene Mengen xL und zL leeren Durchschnitt (andernfalls gäbe es ein $u \in K - \{0\}$ mit $u = r \cdot x = s \cdot z$,

woraus $x = r^{-1}s \cdot z$ und $xL = zL$ folgen würde). M definiert also eine Äquivalenzrelation auf $K - \{0\}$; den Restklassenraum in der Quotiententopologie bezeichnen wir mit $(K - \{0\})/L$. Auf diesem läßt sich die Verknüpfung $(xL, yL) \to xL \circ yL = xy \cdot L$ definieren. Wegen $(r \cdot x)(s \cdot y) = rs \cdot xy$ gilt nämlich $xL \circ yL = uL \circ vL$ für alle $u \in xL$ und $v \in yL$, und die Abbildung $x \to xL$ ist ein Homomorphismus von $(K - \{0\}, .)$ auf $(K - \{0\})/L$. Nun sei $W \in \mathfrak{U}(0)$ eine kompakte Umgebung von 0. Dann ist $W + W$ ebenfalls eine kompakte Umgebung von 0. Es kann nicht $W = W + W$ für alle kompakten $W \in \mathfrak{U}(0)$ gelten, denn $(K, +)$ ist lokal einfach. Es sei also $W + W \neq W$. Ist V das Innere von W, so ist $(W + W) - V$ ein kompakter Teilraum von $(K - \{0\})$. Zu jedem xL gibt es ein u, so daß $u \in V$, aber nicht $2 \cdot u \in V$ richtig ist (denn $r \to r \cdot x$ ist ein Isomorphismus von $(R_+, +)$ auf $xL \cup \{0\}$). Andererseits ist $2 \cdot u \in V + V \subseteq W + W$; d.h. $xL \cap (W + W) - V$ ist nicht leer. Da $x \to xL$ eine stetige Abbildung von $(W + W) - V$ auf $(K - \{0\})/L$ darstellt, ist $(K - \{0\})/L$ in der Tat kompakt.

(4.2) Ist $(K, +, .)$ eine Doppelloop und erfüllt die Voraussetzungen von (4.1) und ist $(K - \{0\}, .)$ ein multiplikativ geschriebener Fastvektorraum (d.h. eine eudoxische zusammenhängende, lokalalternative, kommutative Loop), so ist $(K - \{0\})/L$ isomorph einer Torusgruppe T^n.

BEWEIS. Der Satz II, (8.19) beweist, daß $(K - \{0\}, .)$ direktes Produkt eines zentralen kompakten Normalteilers isomorph einer Torusgruppe T^n und einem Fastvektorraum L' ist. Denn L ist ein (multiplikativ geschriebener) Untervektorraum von $(K - \{0\}, .)$; die Faktorloop $(K - \{0\})/L$ nach diesem ist kompakt; daraus folgt aber $L = L'$ und die Behauptung.

Wir haben darüber hinaus sogar bewiesen, daß die multiplikative Loop $(K - \{0\}, .)$ eine Gruppe ist. *K ist also ein Neokörper.*

(4.3) Kommt zu den Voraussetzungen von (4.2) noch hinzu, daß $(K, +)$ eine Moufangloop ist, so ist $(K, +, .)$ isomorph dem Körper der reellen Zahlen oder dem Körper der komplexen Zahlen. Der Satz bleibt richtig, wenn $(K, +)$ alternativ vorausgesetzt wird.

BEWEIS. Die Behauptung folgt aus dem Satz (3.7) und der Tatsache, daß $(K - \{0\}, .)$ eine abelsche Gruppe ist.

Wir geben für diesen Satz im folgenden einen unabhängigen Beweis, der die komplizierte Kennzeichnung der Alternativkörper nicht benötigt, und der außerdem nur die Alternativität der Addition benützt.

Nach (3.6) ist $(K, +)$ isomorph einem Vektorraum R^n. $(K - \{0\})/L$ ist nach BOURBAKI [1], Chap. VI, § 2 no. 3 homöomorph einer m-Sphäre und andererseits homöomorph einem n-dimensionalen Torus T^n. Dann ist aber notwendig $n = 1$ und $m = 2$. Nun sei $r \to \tilde{e}(r)$ der Isomorphismus der Gruppe der reellen Zahlen modulo 1 auf die Torusgruppe $(K - \{0\})/L$. $(K - \{0\}, .)$ ist das direkte Produkt eines kompakten Normalteilers C isomorph der Gruppe der reellen Zahlen modulo 1 und der Gruppe L isomorph zur multiplikativen Gruppe aller positiven reellen Zahlen. Bezeichnen wir mit $r \to e(r)$ den Isomorphismus der Gruppe der reellen Zahlen modulo 1 auf C, so gilt $\tilde{e}(r) = e(r)L$.

Es steht nun fest, daß $(K-\{0\},.)$ der multiplikativen Gruppe des Körpers der komplexen Zahlen isomorph ist, wobei wir stillschweigend vorausgesetzt haben, daß $(K-\{0\})/L$ aus mehr als einem Punkt besteht. (Andernfalls folgt sofort die Isomorphie von K zum Körper der reellen Zahlen.)

Nun sei K^* der Körper der komplexen Zahlen. Die Abbildung w, die einem Element $re(s)$ von K mit $r \neq 0$ die komplexe Zahl $re^{2\pi i s}$ und dem Element $0 \in K$ die Zahl 0 zuordnet ist ein Homöomorphismus von K auf K^*, der die Multiplikation isomorph überträgt. Wegen $e(\frac{1}{2})^2 = e$ und $(-e)^2 = e$ (also wegen $e(\frac{1}{2}) = -e$) gilt für alle reellen Zahlenpaare (a, b) und (a', b') die Gleichung $\left(a \cdot e + b \cdot e(\frac{1}{4})\right)\left(a' \cdot e + b' \cdot e(\frac{1}{4})\right) = aa' \cdot e + ab' \cdot e(\frac{1}{4}) + ba' \cdot e(\frac{1}{4}) + bb' \cdot e(\frac{1}{2}) = (aa' - bb') \cdot e + (ab' + ba') \cdot e(\frac{1}{4})$, denn infolge der Alternativität von $(K, +)$ erzeugen e und $e(\frac{1}{4})$ gemäß II, (8.3) einen Untervektorraum und außerdem waren beide Distributivgesetze vorausgesetzt. Die Abbildung $f = \left(a + bi \to a \cdot e + b \cdot e(\frac{1}{4})\right)$ ist also ein Homomorphismus und daher ein Isomorphismus von K^* in $(K, +, .)$. Die Abbildung $w^{-1} \circ f$ ist ein Isomorphismus der multiplikativen Struktur des Körpers der komplexen Zahlen in sich. Eine abelsche Gruppe, die zur multiplikativen Gruppe der komplexen Zahlen isomorph ist, besitzt außer ihren Automorphismen keine Isomorphismen in sich. Also ist $w^{-1} \circ f$ einer Abbildung von K^* auf sich, und f ist ein Isomorphismus von K^* auf K.

Diesen Beweisgang bauen wir aus zu folgendem Satz:

(4.4) *$(K, +, .)$ sei eine Doppelloop, die den Voraussetzungen von* (4.1) *genügt. Dann ist jeder eindimensionalen Torusgruppe von $(K-\{0\})/L$ als Urbild eine Untergruppe von $(K-\{0\},.)$ zugeordnet, die der multiplikativen Gruppe des Körpers der komplexen Zahlen isomorph ist.*

Beweis. $r \to \tilde{e}(r)$ sei ein Isomorphismus der Gruppe T der reellen Zahlen modulo 1 in $(K-\{0\})/L$. Das Urbild von $\tilde{e}(T)$ in $K-\{0\}$ bei dem Homomorphismus $x \to xL$ sei A. Nach II, (7.6) ist $A = C'L$ mit einer Einparametergruppe C'. Der Durchschnitt $C' \cap L$ ist eine diskrete zyklische Untergruppe von L, die etwa von r erzeugt sei. Ist $s \to f(s)$ ein Homomorphismus von R auf C' und ist $f(1) = r \cdot e$, so ist $s \to e(s) = e^{-s \cdot \ln r} \cdot f(s)$ ein Homomorphismus von R in A mit $e(1) = e$. Die Einparametergruppe $e(R) = C$ ist also ein isomorphes Bild von T und es gilt $A = CL$. Da L im Zentrum von A liegt und $C \cap L = \{e\}$ ist, ist A dem direkten Produkt von C und L isomorph.

Da die Addition nicht notwendig eine Gruppe bildet, ist der letzte, auf die Addition bezügliche Teil des Beweises (4.3) nicht anwendbar.

(4.5) *$(K, +, .)$ sei eine Doppelloop, die den Voraussetzungen von* (4.1) *genügt. Darüber hinaus sei $(K, +)$ alternativ. Dann ist jeder eindimensionalen Torusgruppe von $(K-\{0\})/L$ ein Unterkörper von K zugeordnet, der dem Körper der komplexen Zahlen isomorph ist.*

Beweis. $(K, +)$ ist ein kommutativer alternativer Fastvektorraum [II, (8.5)]. Jeder eindimensionalen Torusgruppe von $(K-\{0\})/L$ ist eine der multiplikativen Gruppe des Körpers der komplexen Zahlen isomorphe Gruppe in $(K^*-\{0\},.)$ zugeordnet. $re^{2\pi i \cdot s} \to r \cdot e(s)$ sei der zugehörige Isomorphismus

von $K^* - \{0\}$ in $K - \{0\}$. Da die Elemente e und $e(\frac{1}{4})$ in K nach II, (8.3) einen nach dem Beweis von (4.3) multiplikativ abgeschlossenen Untervektorraum erzeugen, gilt also dann auch der letzte, die Addition betreffende Teil des Beweises von (4.3), woraus die Behauptung folgt.

(4.6) *$(K, +, .)$ sei eine nicht diskrete lokalkompakte distributive Doppelloop; $(K, +)$ sei eine lokal einfache potenzassoziative Loop, $(K - \{0\}, .)$ sei ein lokaler Fastvektorraum (d.h. eine eudoxische zusammenhängende lokalalternative kommutative Loop). Dann ist $(K - \{0\})$ isomorph der multiplikativen Gruppe des Körpers der komplexen Zahlen. Ist $(K, +)$ sogar alternativ, so ist K isomorph zum Körper der komplexen Zahlen.*

BEWEIS. $(K - \{0\}, .)$ ist isomorph dem direkten Produkt einer n-dimensionalen Torusgruppe mit L. Wir müssen $n = 1$ beweisen. Jedes Element $x \in K$ $(x \neq 0)$ besitzt genau eine Darstellung der Form $r \cdot e_1(s_1) \dots e_n(s_n)$ mit n verschiedenen Isomorphismen der Gruppe der reellen Zahlen modulo 1 in $(K - \{0\}, .)$. Die Abbildung $g = (x \to (r, s_1, \dots, s_n))$ ist eine eineindeutige stetige und offene Abbildung von $K - \{0\}$ auf $(R_+ - \{0\}) \times T^n$. K ist lokal euklidisch $(n+1)$-dimensional, denn e besitzt eine zu einem Quader homöomorphe Umgebung $\{y;\ y = g(r, s_1, \dots, s_n),\ 0 < 1 - a < r < 1 + a,\ -\frac{1}{2}a < s_m < \frac{1}{2}a,\ m = 1, \dots, n\}$. Jeder Punkt x von K besitzt also eine Basis aus Umgebungen W derart, daß $W - \{x\}$ für $n > 1$ einfach kurvenzusammenhängend ist. Nun hat aber jede Umgebung W des Punktes 0 die Eigenschaft ,daß $W - \{0\}$ stets einen Teilraum der Form $B_a = \{g^{-1}(r, s_1, \dots, s_n);\ 0 < r < a,\ s_m \in T,\ m = 1, \dots, n\}$ enthält, denn zu jedem offenen $W \in \mathfrak{U}(0)$ existiert ein reelles r so, daß $r \cdot x \in W$ für alle $x \in g^{-1}(1, T^n)$, denn die Mengen $g^{-1}(]0, r], T^n) \cup \{0\}$ $(r \neq 0)$ bilden eine Umgebungsbasis für 0. Andernfalls gäbe es nämlich ein $W \in \mathfrak{U}(0)$,so daß zu jedem natürlichen l ein n-tupel $s^{(l)} = (s_1^{(l)}, \dots, s_n^{(l)})$ existieren würde, für welches $g^{-1}(a_l, s_1^{(l)}, \dots, s_n^{(l)}) \notin W$, wobei die Folge a_l gegen 0 konvergiert, wenn l gegen unendlich strebt. Ist $\bar{s} = (\overline{s_1}, \dots, \overline{s_n})$ der Limes einer Teilfolge $s^{(l_i)}$, so würde $0 = \lim_{l_i \to \infty} g^{-1}(a_{l_i}, s_1^{(l_i)}, \dots, s_n^{(l_i)})$ nicht im Innern von W liegen, was offenbar nicht möglich ist. Jede Umgebung von 0 der Form $g^{-1}(]0, r], T^n \cup \{0\}$ ist so beschaffen, daß für $n > 1$ der Raum $g^{-1}(]0, r], T^n)$ nicht einfach kurvenzusammenhängend ist. Andererseits müßte er für n größer als 1 einfach kurvenzusammenhängend sein oder wenigstens einen offenen einfach kurvenzusammenhängenden Teilraum der Form $W - \{0\}$ enthalten, wo W eine Umgebung von 0 wäre. Dieser Widerspruch beweist, daß $n = 1$ sein muß.

Besteht nun $(K - \{0\})/L$ nicht nur aus einem Punkt, was wir in der Formulierung des Satzes stillschweigend angenommen haben, so folgt daraus die Behauptung.

(4.7) *$(K, +, .)$ sei eine lokal euklidisch zweidimensionale distributive nullteilerfreie ringartige Struktur. $(K, +)$ sei potenzassoziativ und eudoxisch. $(K - \{0\})/L$ sei monassoziativ und die Rechtstranslationen in dieser Struktur seien eineindeutig; diese Voraussetzungen sind insbesondere erfüllt, wenn $(K - \{0\}, .)$ lokal monassoziativ ist und eineindeutige Rechtstranslationen besitzt. Entweder sei $(K, +)$ sogar alternativ oder K eine Doppelloop.*

Dann ist $(K-\{0\}, .)$ *isomorph der multiplikativen Gruppe des Körpers der komplexen Zahlen.*

BEWEIS. Nach den bisher bewiesenen Sätzen haben wir festzustellen, daß $(K-\{0\})/L$ einer eindimensionalen Torusgruppe isomorph ist. Wegen dem in II, (6.4) niedergelegten Ergebnis wird es unter den angegebenen Voraussetzungen genügen, nachzuweisen, daß der topologische Raum $(K-\{0\})/L$ eine Jordan-Kurve ist.

Es sei $K\cup\{a\}$ die Einpunktkompaktifizierung von K, dann ist dieser Raum wegen der in (1.5) bewiesenen Homogenitätseigenschaft eine zweidimensionale kompakte Mannigfaltigkeit. Diese hat die Eigenschaft nach der Entfernung eines Punktes noch einfach zusammenhängend zu sein. Sie ist dann notwendig homöomorph zu einer Kugeloberfläche, denn allen anderen zweidimensionalen kompakten Mannigfaltigkeiten kommt diese Eigenschaft nicht zu. Für alle x ist $xL\cup\{0\}\cup\{a\}$ ein Jordan-Bogen, der 0 mit a verbindet, denn $R_+ \cdot x = xL\cup\{0\}$ ist homöomorphes Bild von R_+ und es gilt ja $\lim_{r\to\infty} r\cdot x = a$. Sind nun xL und yL zwei verschiedene Punkte von $(K-\{0\})/L$, so ist $xL\cap yL=\emptyset$ und $xL\cup yL\cup\{0\}\cup\{a\}$ ist eine Jordan-Kurve auf $K\cup\{a\}$. Die Menge $(K-\{0\})\cap(xL\cup yL)^c$ besteht aus genau zwei Komponenten A_1 und A_2 mit der Eigenschaft, daß aus $z\in A_n$ auch $zL=A_n$ folgt; denn wäre z.B. $z\in A_1$ und $z'\in A_2$ mit $z=l\cdot z'$ $(l\in L)$, so enthielte zL einen zu $[0,1]$ homöomorphen Kurvenbogen mit den Endpunkten z und z'; dieser hätte jedoch mit $xL\cup yL\cup\{0\}\cup\{a\}$ wenigstens einen Punkt gemeinsam; denn eine Jordan-Kurve zerlegt die Kugel in genau zwei Gebiete, und z und z' liegen in verschiedenen Gebieten. Dieser gemeinsame Punkt ist andrerseits von $\{0\}$ und $\{a\}$ verschieden, denn weder 0 noch a ist ein innerer Punkt von zL. Dann wäre also z.B. $zL\cap xL\neq\emptyset$, woraus dann $zL=xL$ oder $z\in xL$ folgen würde im Widerspruch dazu, daß $z\in A_n$ und somit $z\notin xL\cup yL$ angenommen war.

Die Menge $(K-\{0\})/L-\{xL\}\cup\{yL\}$ hat also die zwei verschiedenen Komponenten, die bei der Abbildung $h=(x\to xL)$ aus A_1 und A_2 entstehen, denn aus $zL\in h(A_1)\cap h(A_2)$ würde die Existenz von zwei Elementen l_1 und l_2 in L folgen, für die $zl_1\in A_1$ und $zl_2\in A_2$ gelten würde, was aber unmöglich ist. Jedes Punktepaar in $(K-\{0\})/L$ trennt $(K-\{0\})/L$ in einen nicht zusammenhängenden Raum mit genau zwei Komponenten auf; daraus folgt aber, daß $(K-\{0\})/L$ einem eindimensionalen Torus homöomorph ist (Satz von R. L. MOORE, vgl. C. KURATOWSKI [2], Topologie II, S. 120).

Man kann das Ergebnis dieser Nummer in etwas speziellerer Form auch so formulieren:

SATZ: *Alle lokal euklidisch zweidimensionalen, distributiven nullteilerfreien ringartigen Strukturen mit potenzassoziativer eudoxischer Addition und Multiplikation sind Neokörper mit einer zur Gruppe der Multiplikation im Körper der komplexen Zahlen isomorphen Multiplikationsgruppe, wenn sie sogar alternative Addition haben oder Doppelloops sind. Im alternativen Fall ist K isomorph zum Körper der komplexen Zahlen (vgl.* (4.5)*).*

(4.8) Unter den Bedingungen von (4.7) gibt es einen Homöomorphismus von K auf den Körper der komplexen Zahlen, nämlich den Isomorphismus der multiplikativen Gruppe von K auf die multiplikative Gruppe von K^*, dem Körper der komplexen Zahlen, der durch die Festsetzung auf ganz K ausgedehnt wird, daß dem Punkt 0 in K der Punkt 0 in K^* zugeordnet wird. Dieser Homöomorphismus heiße w.

Nun definieren wir eine Verknüpfung in K durch die Definition $(x, y) \to x \circ y = w\big(w^{-1}(x) + w^{-1}(y)\big)$; $(K, \circ)$ ist dann isomorph zu $(K, +)$. Die Abbildung w kann man in der Form $w(x) = r(x)\, e^{2\pi i \cdot s(x)}$ angeben, wobei $r(x)$ und $s(x)$ durch $x = r(x) \cdot e\big(s(x)\big)$ definiert sind mit einem Isomorphismus $s \to e(s)$ der Gruppe der reellen Zahlen modulo eins in $(K - \{0\}, .)$. Gilt nun für zwei Elemente x und y aus K die Gleichung $p\,x = q\,y$ mit reellen Zahlen p und q, so ist $\operatorname{arc} x = \operatorname{arc} y$ und $w^{-1}(x) + w^{-1}(y) = |x| \cdot e(\operatorname{arc} x) + |y| \cdot e(\operatorname{arc} y) = (|x| + |y|) \cdot e(\operatorname{arc} x) = w^{-1}(x + y)$; unter diesen Bedingungen gilt also $x \circ y = x + y$. Außerdem folgt aus dem distributiven Gesetz wegen der Isomorphie von $(K, \circ, .)$ und $(K, +, .)$ die Identität $(x \circ y)\, z = xz \circ yz$. Setzt man nun allgemein

$$f(x, y) = \begin{cases} 1 & \text{wenn } x = -y, \\ \dfrac{x \circ y}{x + y}, & \text{wenn } x \neq -y, \end{cases}$$

so folgt

a) $f(x, y) = 1$, wenn $x = 0$ oder $y = 0$, oder wenn $x y^{-1}$ oder $y x^{-1}$ reell ist.

b) $(x \circ y)\, z = (x + y) f(x, y)\, z = (xz + yz) f(x, y) = (xz + yz) f(xz, yz)$ oder $f(xz, yz) = f(x, y)$; d.h. es gilt $f(x, y) = g(x y^{-1})$ (man braucht ja nur $z = y^{-1}$ zu setzen und bekommt dann $g(x y^{-1}) = f(x y^{-1}, 1)$). $z \to g(z)$ ist auf der vollen Zahlenkugel stetig außer vielleicht im Punkt $z = -1$, weil f auf ganz $K \times K - \{(x, -x);\ x \in K\}$ stetig ist. g ist auf dem vollen reellen Großkreis gleich eins. Da $x \circ y = u$ eindeutig nach x und nach y aufgelöst werden kann, muß dasselbe auch für die Gleichung $(x + y)\, g(x y^{-1}) = u$ gelten; d.h. die Abbildung $z \to (z + 1)\, g(z)$ muß eine eineindeutige Abbildung der Zahlenkugel auf sich darstellen.

Ist umgekehrt eine Funktion $z \to g(z)$ dieser Eigenschaft vorgegeben, so wird durch $x \circ y = (x + y)\, g(x y^{-1})$ eine Verknüpfung auf K definiert, so daß $(K, \circ, .)$ eine zweidimensionale Doppelloop darstellt, deren multiplikative Loop der multiplikativen Gruppe des Körpers der komplexen Zahlen isomorph ist, und deren „Addition" $\circ$ monassoziativ ist.

Es besteht also eine eineindeutige Zuordnung zwischen der Menge solcher Strukturen und der Menge aller Funktionen g mit den oben aufgezählten Eigenschaften.

Es ist klar, daß $(K, \circ, .)$ genau dann dem Körper der komplexen Zahlen isomorph ist, wenn $g(z)$ identisch gleich eins ist.

(4.9) *$(K, +, .)$ sei eine ringartige Struktur, die den Voraussetzungen von Satz* (4.7) *genügt. Der in* (4.8) *beschriebene Homöomorphismus w von K auf den Körper der komplexen Zahlen habe die zusätzliche Eigenschaft, daß $x \to x \circ 1$*

eine in einem reellen Punkt regulär analytische Abbildung ist. Dann ist K isomorph dem Körper der komplexen Zahlen.

BEWEIS. Die Abbildung $z \to z \circ 1 = (z+1)g(z)$ sei in dem reellen Punkt r regulär; sie stimmt dann auf einer sich gegen r häufende Punktmenge mit der regulären Funktion $z \to z+1$ überein und ist daher mit ihr identisch.

(4.10) *Es gibt einen lokal euklidisch zweidimensionalen Neokörper (also eine distributive Doppelloop mit assoziativer Multiplikation), dessen multiplikative Loop $(K - \{0\}, .)$ der multiplikativen Gruppe des Körpers der komplexen Zahlen isomorph ist, der aber nicht zum Körper der komplexen Zahlen isomorph ist.*

BEWEIS. Wir suchen eine geeignete Verknüpfung $x \circ y = (x+y)g(xy^{-1})$, so daß $(K, \circ, .)$ die angegebenen Eigenschaften besitzt. $(K, \circ)$ ist genau dann kommutativ, wenn $g(z) = g(z^{-1})$ gilt. Wir setzen nun $g(z) = 1 + \frac{|y|\,\varepsilon}{x^2+y^2+1}$ mit $z = x+iy$ und einem noch näher zu bestimmenden ε mit $\frac{1}{2} \geqq \varepsilon > 0$. Dann ist g auf der ganzen Kugel stetig und es gilt

$$g(z^{-1}) = 1 + \frac{|y| \cdot \varepsilon}{z\bar{z}} \cdot \frac{1}{\frac{1}{z\bar{z}} + 1} = g(z).$$

Ferner ist $1 \leqq g(z) < 1+\varepsilon$; und $g(z) = 1$ gilt genau dann, wenn z reell ist. Wir haben nun noch nachzuweisen, daß $z \to (z+1)g(z)$ eine eineindeutige Abbildung der Zahlenkugel auf sich darstellt. Es sei also w ein Element der Zahlenkugel. Gilt nun $w = \infty$ oder $w = 0$, so wird $w = (1+z)g(z)$ nur durch $z = \infty$ bzw. durch $z = -1$ befriedigt. Also sei im folgenden stets $w = u + iv \neq 0$. Dann muß die Existenz einer und nur einer reellen Zahl $r \neq 0$ nachgewiesen werden, für die $w = r^{-1}(1+z)$ und $r^{-1} = g(z)$ erfüllt ist. Diese zwei Identitäten sind mit $r^{-1} = g(rw-1)$ gleichwertig. Nun gilt $0 \leqq g(rw-1) - 1 < \varepsilon$. Die Kurven $s_1 = \frac{1}{r} - 1$ und $s_2 = g(rw-1) - 1$ schneiden sich sicher im Intervall $\frac{1}{\varepsilon+1} \leqq r \leqq 1$ und sicher nicht außerhalb dieses Intervalls. Es ist nachzuprüfen, daß sie sich in diesem Intervall auch nur höchstens einmal schneiden. Man berechnet $\frac{ds_1}{dr} = -\frac{1}{r^2}$ und $\frac{ds_2}{dr} = \frac{\varepsilon|y|\,(2 - |w|^2 r^2)}{(|w|^2 r^2 - 2rx + 2)^2}$ für $\frac{1}{\varepsilon+1} \leqq r \leqq 1$. Nun ist in diesem Intervall einerseits $\frac{ds_1}{dr} \leqq -1$ und andrerseits

$$\frac{ds_2}{dr} \geqq -\frac{\varepsilon|y|\,(\varepsilon+1)^4 |w|^2}{\left(\left(x - \frac{1}{r}\right)^2 + r^{-2}y^2 + r^{-2}\right)^2} \geqq -\frac{\varepsilon\left(\frac{3}{2}\right)^4 |y|\,|w|^2}{\left(\left(x - \frac{1}{r}\right)^2 + y^2 + 1\right)^2}$$

$$\geqq -\frac{|y|\,|w|^2}{(a(x)^2 + y^2 + 1)^2} \cdot \varepsilon \cdot \left(\frac{3}{2}\right)^4, \quad \text{wo} \quad a(x) = \begin{cases} (x-1) & \text{für } x \leqq 1 \\ 0 & \text{für } 1 \leqq x \leqq \frac{3}{2} \\ \left(x - \frac{3}{2}\right) & \text{für } \frac{3}{2} \leqq x. \end{cases}$$

Es gilt

$$\frac{|y|\,|w|^2}{(a(x)^2 + y^2 + 1)^2} = \frac{|y|\,|w|^2}{(|w|^2 + 1 + a(x)^2 - x^2)^2} = \frac{|y|}{|w|^2} \cdot \frac{1}{(1 + (1 + a(x)^2 - x^2)\,|w|^{-2})^2},$$

und für $|w| \to \infty$ strebt $(1+a(x)^2-x^2)|w|^{-2}$ gegen null. Es gibt also eine positive reelle Zahl A derart, daß dieser Bruch für alle komplexen w stets unterhalb A liegt. Wählt man nun ε so, daß $\varepsilon < \min\left(\frac{1}{2}, \left(\frac{2}{3}\right)^4 \cdot A^{-1}\right)$, so ist immer $\frac{ds_2}{dr} > -1$. Damit ist dann $\frac{d(s_2 - s_1)}{dr} > -1+1=0$, d.h. die Kurve $s = s_2 - s_1$ schneidet die r-Achse in höchstens einem Punkt in $\left[\frac{1}{\varepsilon+1}, 1\right]$.

Die Abbildung $z \to (z+1)g(z)$ ist somit eine eineindeutige Abbildung der Zahlenkugel auf sich. Es wäre wesentlich einfacher gewesen, ein Beispiel mit nichtkommutativer Addition anzugeben.

Das eben konstruierte Beispiel liefert auch eine lokal euklidische, zweidimensionale topologische Loop, die kommutativ, potenzassoziativ, eudoxisch und lokaltorsionsfrei ist, ohne assoziativ zu sein, nämlich die Loop $(K, \circ)$.

ANMERKUNGEN. Bei den verschiedenen Kennzeichnungen des Körpers der komplexen Zahlen treffen wir wieder auf die schon in § 2 aufgetretene Erscheinung, daß die vollständige Information zuerst über die multiplikative Loop geliefert wird. Ebenso wie damals das Beispiel (2.5) zeigt jetzt das Beispiel (4.10), daß dies eine notwendige Erscheinung ist. Als Ergänzung zu dem in II, § 9 konstruierten Beispiel ist die in (4.10) angegebene kommutative, potenzassoziative, eudoxische, lokal torsionsfreie, nichtassoziative zweidimensionale Loop bemerkenswert; ihre Translationen sind nicht überall differenzierbar, also erst recht nicht analytisch.

Literatur

[1] BOURBAKI, N.: Topologie générale, Eléments de Mathématique. Actual. sci. industr. **858** (1940); **1152** (1951). — [2] KURATOWSKI, C.: Topologie I und II. Monogr. Mat., Tom XX und XXI. — [3] PICKERT, G.: Projektive Ebenen. Berlin: Springer 1957. — [4] SALZMANN, H.: Topologische Ebenen. Math. Z. **67**, 436–466 (1957).

Tübingen, Mathematisches Institut der Universität

(Eingegangen am 27. März 1958)

FARAHAT, H. K., and L. MIRSKY
Math. Zeitschr. Bd. 70, S. 231—244 (1958)

Group Membership in Rings of Various Types

By

H. K. FARAHAT and L. MIRSKY

1. Introduction

Nearly fifty years ago, A. RANUM [2] used the theory of elementary divisors for determining the conditions that a given matrix should belong to some multiplicative group of (not necessarily non-singular) matrices and for investigating a number of related questions. In a subsequent paper [3] he reverted to the subject, but considered now the more general case of finite-dimensional algebras. Our aim in the present note is to discuss a series of problems which are closely related to those of RANUM, but with the important difference that whereas he considers *algebras*, we are largely concerned with *rings*. Thus there is very little overlap between his results and ours, while the methods we employ are also quite distinct from his. We propose to study multiplicative groups in rings, their relation to each other, criteria for group membership, and other problems which naturally suggest themselves in this context. In §§ 2—4 we shall develop the general theory, imposing progressively more restrictive conditions on the structure of the rings in question. In § 5 a few applications to the theory of numbers will be indicated; and finally, in § 6, we shall consider linear algebras and, more particularly, the algebra of matrices.

The main idea in our treatment is the use of direct sums and of "principal idempotent elements". The latter notion is, of course, familiar in matrix theory (see e.g. [4], pp. 28—30); and we shall show that it can be extended without difficulty to more general situations.

If R is a ring (or a multiplicative semigroup) and S is a subset of R, then S will be called a *group in* R if it is a group with respect to multiplication. If an element $a \in R$ belongs to at least one group in R, it will be called a *group member* (in R). Our object is to determine, for specified classes of rings, whether a given element is a group member or not; and also to characterize, as far as possible, all groups in a given ring.

An element a in a ring (or semigroup) R is said to be *idempotent* if $a^2 = a$. It is clear that every idempotent element is a group member, and also that every group in R contains exactly one idempotent.

If S is a subset of a ring R and $a \in R$, then aS will denote the set of all elements of the form ax, $x \in S$; and Sa is defined analogously. Similarly, $a + S$ will denote the set of all elements of the form $a + x$, $x \in S$.

If X is a finite set, we shall denote the number of its elements by $|X|$.

2. Semigroups and rings with unit element

2.1. We shall begin with two results on semigroups, i.e. systems closed with respect to an associative multiplication.

THEOREM 1. *Let R be a semigroup, and let a be a group member in R. Then there exists a group $\mathfrak{M}(a)$ in R such that every group in R containing a is a subgroup of $\mathfrak{M}(a)$. In particular, the unit element of any group containing a is the unit element of $\mathfrak{M}(a)$, and the inverse of a in any group to which it belongs is equal to its inverse in $\mathfrak{M}(a)$.*

Denote by $\{G_i\}_{i\in J}$, where J is an appropriate index set, the family of all groups in R which contain a. For every $i\in J$, denote by u_i the unit element of G_i and by a_i the inverse of a in G_i. We then have, for $i, j\in J$,

$$\begin{aligned} a_i &= a_i u_i = a_i a_i a = a_i a_i a u_j = a_i a_i a a a_j \\ &= a_i u_i a a_j = a_i a a_j = a_i a u_j a_j = a_i a a a_j a_j \\ &= u_i a a_j a_j = a a_j a_j = u_j a_j = a_j . \end{aligned}$$

Therefore $u_i = a a_i = a a_j = u_j$. Thus all groups G_i, $i\in J$, have a common unit element, say u; and a has the same inverse, say a^*, in every group G_i. Now denote by $\mathfrak{M}(a)$ the set of all elements $x\in R$ which can be represented in the form $x = x_1 x_2 \dots x_k$, where each x_j belongs to some G_i. It can be verified at once that $\mathfrak{M}(a)$ is a group (with $x_k^* \dots x_2^* x_1^*$ as the inverse of x); and clearly every G_i, $i\in J$, is a subgroup of $\mathfrak{M}(a)$[1]).

We shall call $\mathfrak{M}(a)$ the *maximal group of* a. Since it is now possible to speak of *the* inverse of a group member a, we shall denote this inverse by a^{-1}. From the preceding discussion we infer immediately the following result.

THEOREM 2. *If R is a semigroup and a, b are group members in R, then $\mathfrak{M}(a)$, $\mathfrak{M}(b)$ are either disjoint or identical*[2]).

It now follows at once that if a group $\mathfrak{M}$ in R is the maximal group of any one of its elements, then it is the maximal group of every one of its elements. A group in R with this property will be called *maximal*. We see, then, that the group members in a semigroup are distributed among disjoint maximal groups.

2.2. We shall now specialize R, and for the remainder of the present section shall assume that it is a ring with unit element 1. An element $x\in R$ will be said to be invertible if, for some $y\in R$, $xy = yx = 1$. (If such an element y exists, it is plainly unique, and will be denoted by x^{-1}.) We may note that the set of all invertible elements in R is a maximal group, namely $\mathfrak{M}(1)$.

THEOREM 3. *Let R be a ring with unit element 1. If a is a group member in R, e is the unit element of $\mathfrak{M}(a)$, and $\mathfrak{C}(e)$ is the set of all invertible elements*

[1]) We owe the proof given above to Professor R. RADO, who has also drawn our attention to the following more general result. Let R be a semigroup and let $\{G_i\}_{i\in J}$ be a family of pairwise intersecting groups in R; then there exists a group G in R such that every G_i is a subgroup of G.

[2]) RANUM ([3], p. 287) proved Theorem 2 for the special case when R is a finite-dimensional algebra. His proof is based on the additive structure of R.

in R which commute with e, then (i) $\mathfrak{M}(a) = e\,\mathfrak{C}(e)$; (ii) *the element* $1-e+a$ *is invertible, and* $a^{-1}=e(1-e+a)^{-1}$.

It is obvious that $e\,\mathfrak{C}(e)$ is a group. Since it contains e, we have

$$e\,\mathfrak{C}(e) \subseteqq \mathfrak{M}(e) = \mathfrak{M}(a). \tag{1}$$

Next, let $x \in \mathfrak{M}(a)$. Then

$$(1-e+x)(1-e+x^{-1}) = 1 = (1-e+x^{-1})(1-e+x), \tag{2}$$

so that $1-e+x$ is invertible. Moreover

$$x = e(1-e+x) = (1-e+x)e,$$

and so $x \in e\,\mathfrak{C}(e)$. Hence $\mathfrak{M}(a) \subseteqq e\mathfrak{C}(e)$; and (i) follows in view of (1). Furthermore, we note from (2) that $1-e+a$ is invertible. Since now $a^{-1}(1-e+a)=e$, the proof of (ii) is complete.

THEOREM 4. *If R is a ring with unit element* 1 *and e is an idempotent element in R, then*

$$\mathfrak{M}(e) \cong \mathfrak{C}(e)/\{e + \mathfrak{M}(1-e)\},$$

where $\mathfrak{C}(e)$ is defined as in Theorem 3.

It is obvious that $\mathfrak{C}(e)$ is a group. Since, by Theorem 3 (i), $\mathfrak{M}(e) = e\,\mathfrak{C}(e)$, it follows that the mapping $x \to ex$ effects a homomorphism of $\mathfrak{C}(e)$ onto $\mathfrak{M}(e)$, so that $\mathfrak{M}(e) \cong \mathfrak{C}(e)/N$, where N is the set of all $x \in \mathfrak{C}(e)$ such that $ex = e$. But it is clear by a straightforward argument that $N = e + \mathfrak{M}(1-e)$, and the proof is therefore complete.

COROLLARY. *If R is a commutative ring with unit element* 1, *and e is any idempotent element of R, then*

$$\mathfrak{M}(e) \cong \mathfrak{M}(1)/\{e + \mathfrak{M}(1-e)\}.$$

Thus every maximal group is a homomorphic image of $\mathfrak{M}(1)$.

3. Semi-divided rings

3.1. Let R be a ring. We shall denote its zero element by 0. An element $a \in R$ is said to be *nilpotent* if, for some positive integer k, $a^k = 0$. The smallest positive integer with this property will be called the *index* of a. (In particular we regard 0 as a nilpotent element of index 1.) It is clear that a non-zero nilpotent element cannot be a group member in R.

A ring R will be said to be the *direct sum* of the subrings $R_1, \ldots, R_r$ if every element $a \in R$ possesses a unique representation of the form

$$a = \sum_{k=1}^{r} a_k \qquad (a_k \in R_k;\ k = 1, \ldots, r),$$

and if, furthermore, $xy = 0$ whenever $x \in R_k$, $y \in R_j$, $k \neq j$. We express this relation between R and the R_k by writing

$$R = \sum_{k=1}^{r} R_k \qquad \text{(direct sum)}. \tag{3}$$

If (3) is given and x is any element of R, then we shall denote by x_k the "component" of x in R_k. Again, if S_k is a subset of R_k, then $\sum_{k=1}^{r} S_k$ will denote the set of all elements of R expressible in the form $y_1+\cdots+y_r$, where $y_k \in S_k$ $(k=1,\ldots,r)$.

A ring R is said to be *divided* if it possesses a unit element and if every element of R is either invertible or nilpotent. Further, we call R a *semi-divided ring* if it is the direct sum of a finite number of subrings, each of which is divided.

Throughout the present section R will denote a semi-divided ring, with unit element 1, which is the direct sum of the divided subrings $R_1,\ldots,R_r$. We shall denote the unit element of R_k by e_k, the set of elements invertible in R_k by I_k, and the set of nilpotent elements in R_k by N_k.

Again, let $a \in R$. We define $l(a_k)$ as 1 or as the index of a_k according as $a_k \in I_k$ or $a_k \in N_k$; and we put $l(a) = \max l(a_k)$, $1 \leqq k \leqq r$. The number $l(a)$ will be called the *index* of a. (It is clear that when a is nilpotent, this coincides with our previous definition.) We shall see from a subsequent theorem that $l(a)$ is, in fact, independent of the particular decomposition (3).

For any $a \in R$, we shall denote by $\Omega(a)$ the set of integers k in the range $1 \leqq k \leqq r$ such that $a_k \in I_k$. Further, we shall write

$$\mathrm{id}\, a = \sum_{k \in \Omega(a)} e_k,$$

and we shall call $\mathrm{id}\, a$ the *idempotent* of a. This, too, will be seen to be independent of (3).

3.2. It is easy to reduce the problem of group membership in R to that of group membership in the R_k.

THEOREM 5. *An element $a \in R$ is a group member in R if and only if, for every value of k, a_k is a group member in R_k.*

Suppose that a belongs to a group G in R. As x ranges over G, let x_k range over G_k. Then G_k is evidently a group in R_k, and $a_k \in G_k$ is a group member in R_k. On the other hand, suppose that, for every value of k, a_k belongs to some group G_k in R. Then $G = \sum_{k=1}^{r} G_k$ is a group in R, and a belongs to this group. We may also note that if ε_k denotes the unit element of G_k (so that ε_k is either 0 or e_k), then the unit element of G is $\sum_{k=1}^{r} \varepsilon_k$.

THEOREM 6. *If $a \in R$, then a^t is a group member in R if and only if*

$$t \geqq l(a). \tag{4}$$

If this condition is satisfied, then $\mathrm{id}\, a$ *is the unit element of* $\mathfrak{M}(a^t)$, *and*

$$\mathfrak{M}(a^t) = \sum_{k \in \Omega(a)} I_k. \tag{5}$$

In particular, therefore, if a is a group member in R, then

$$\mathfrak{M}(a) = \sum_{a_k \neq 0} I_k .$$

We have

$$a^t = \sum_{k=1}^{r} a_k^t .$$

By Theorem 5, a^t is a group member in R if and only if, for every value of k, a_k^t is a group member in R_k, i.e. $t \geqq l(a)$.

Next, let (4) be given; and write $b = a^t$. Then $b_k \in I_k$ or $b_k = 0$ according as $k \in \Omega(a)$ or $k \notin \Omega(a)$. Hence the unit element of any group in R_k containing b_k is e_k or 0 according as $k \in \Omega(a)$ or $k \notin \Omega(a)$. It follows, by the last remark in the proof of Theorem 5, that the unit element of $\mathfrak{M}(b)$ is id a. Again, it is clear that the right-hand side of (5) is a group which contains b; therefore

$$\sum_{k \in \Omega(a)} I_k \subseteqq \mathfrak{M}(b) .$$

Suppose, next, that $x \in \mathfrak{M}(b)$, and write $y = x^{-1}$. Then $xy = yx = \mathrm{id}\, a$ and so $x_k y_k = y_k x_k = (\mathrm{id}\, a)_k$ for every value of k. Hence, when $k \in \Omega(a)$, $x_k y_k = y_k x_k = e_k$, and so $x_k \in I_k$. Moreover, $x = x\, \mathrm{id}\, a$ and so $x_k = x_k (\mathrm{id}\, a)_k$. Hence, if $k \notin \Omega(a)$, then $x_k = 0$. We infer, then, that x is contained in the right-hand side of (5). Hence

$$\mathfrak{M}(b) \subseteqq \sum_{k \in \Omega(a)} I_k ,$$

and the proof is complete.

We note that, in view of Theorem 6, the index $l(a)$ is, in fact, independent of the particular decomposition (3). Equally, id a depends solely on R and a.

COROLLARY. *The element a is a group member in R if and only if*

$$a \cdot \mathrm{id}\, a = a . \tag{6}$$

If a is a group member, then, by Theorem 6, id a is the unit element of $\mathfrak{M}(a)$, and (6) follows. If, on the other hand, (6) is satisfied, then we infer that $a_k = 0$ when $k \notin \Omega(a)$. It follows, by Theorem 5, that a is a group member in R.

THEOREM 7. *The product of two group members in R is again a group member.*

Let a and b be two group members in R, and write $\Omega = \Omega(a) \cap \Omega(b)$. Then

$$ab = \sum_{k \in \Omega} a_k b_k .$$

But $a_k b_k \in I_k$ when $k \in \Omega$; hence the assertion follows by Theorem 5.

3.3. Theorem 6 shows, in particular, that all sufficiently high powers of any element are group members which belong to the same maximal group. Accordingly, we shall say that two elements $x, y \in R$ belong to the same *class* if, for some sufficiently large value of t, x^t and y^t belong to the same maximal group. The class containing x will be denoted by $\mathfrak{K}(x)$.

The following statements relating to classes are immediate.

(i) A divided ring contains just two classes, namely the set of invertible elements and the set of nilpotent elements.

(ii) In any semi-divided ring, the maximal group $\mathfrak{M}(1)$ is also a class.

(iii) The elements a, b of a semi-divided ring belong to the same class if and only if $\mathrm{id}\, a = \mathrm{id}\, b$.

(iv) Any class in a commutative semi-divided ring is a semigroup with respect to multiplication[3]).

3.4. We shall use the letter S to denote any one of the 2^r subsets (including the empty subset) of $\{1, 2, \ldots, r\}$. The complement of S will be denoted by S'.

THEOREM 8. *There are exactly 2^r idempotents in R, and these are given by*

$$e_S = \sum_{k \in S} e_k. \tag{7}$$

The maximal group and the class containing e_S are given by

$$\mathfrak{M}(e_S) = \sum_{k \in S} I_k, \tag{8}$$

$$\mathfrak{N}(e_S) = \sum_{k=1}^{r} X_k, \tag{9}$$

where $X_k = I_k$ or N_k according as $k \in S$ or $k \in S'$.

If $x \in R$ is an idempotent, then $x_k^2 = x_k$ $(k = 1, \ldots, r)$ and so $x_k = e_k$ or 0 according as $x_k \in I_k$ or $x_k \in N_k$. Thus x is of the form (7); and conversely any element of the form (7) is obviously an idempotent. Next, (8) follows by Theorem 6, and (9) is equally evident.

COROLLARY 1. *If R is finite, then*

$$|\mathfrak{M}(e_S)| = \prod_{k \in S} |I_k|,$$

$$|\mathfrak{N}(e_S)| = \prod_{k \in S} |I_k| \cdot \prod_{k \in S'} |N_k|.$$

COROLLARY 2. *If R is finite and commutative and $\mathfrak{N}$ is any class in R, then $|\mathfrak{M}(1)|$ is a multiple of $|\mathfrak{N}|$.*

Since $1 = e_1 + \cdots + e_r$, we have, by Corollary 1,

$$|\mathfrak{M}(1)| = \prod_{k=1}^{r} |I_k|.$$

Defining S by the equation $\mathfrak{N} = \mathfrak{N}(e_S)$, we therefore have

$$|\mathfrak{M}(1)|/|\mathfrak{N}| = \prod_{k \in S'} (|I_k|/|N_k|).$$

Now, since R_k is commutative, it follows that N_k is a subring of R_k. Thus N_k is a subgroup of the additive group R_k; and therefore $|R_k|$, and so $|I_k|$, is a multiple of $|N_k|$. This completes the proof.

3.5. The next theorem furnishes us with two further criteria for group membership of a given element.

[3]) Cf. RANUM [3], p. 293.

THEOREM 9. *Let $a \in R$. The following statements are then equivalent.* (i) *a is a group member in R;* (ii) $aR = a^2R$; (iii) $l(a) = 1$.

In the first place, let (i) be given; and suppose that a belongs to a group G in R. Denoting by u the unit element of G, we have $a = au = a(aa^{-1}) = a^2a^{-1}$, and so $aR \subseteqq a^2R$. Thus (i) implies (ii). Next, let (ii) be given. Since R possesses a unit element, we have $a = a^2b$ for some $b \in R$. Hence $a_k = a_k^2 b_k$ and therefore $a_k = a_k^s b_k^{s-1}$ $(k = 1, \ldots, r;\ s \geqq 2)$. It follows that $a_k = 0$ or $a_k \in I_k$ and therefore $l(a) = 1$. We have thus shown that (ii) implies (iii). Finally, if (iii) is given, then (i) follows immediately by Theorem 6. The proof is therefore complete.

We may note that, in deducing (ii) from (i), we only used the fact that R is closed with respect to multiplication. Thus, if a is a group member in any semigroup R, then $aR = a^2R$ [4]).

3.6. We conclude the present section with a result on rings which possess a semi-divided subring. This result will prove particularly useful in the discussion of algebras in § 6.

THEOREM 10. *Let R^* be a ring with a unit element, and let R be a semi-divided subring of R^*. If $a \in R$ is a group member in R^*, then it is a group member in R.*

Write R in the form (3). Suppose that a belongs to a group G^* in R^*, and denote by u^* the unit element of G^*. We have $a_k = ae_k = e_k a$ $(k = 1, \ldots, r)$. If a_k is nilpotent, say $a_k^n = 0$, then

$$a_k = (au^*)e_k = a(a^{-1}a)^n e_k = a(a^{-1})^n a^n e_k$$
$$= a(a^{-1})^n (ae_k)^n = a(a^{-1})^n a_k^n = 0.$$

It follows that the index of a in R is 1. Hence, by Theorem 9, a is a group member in R.

4. Residue class rings

4.1. In this section, R will denote a principal ideal domain, i.e. a commutative integral domain in which every ideal is principal. The unit element and the zero element of R will be denoted by 1 and 0 respectively. The highest common factor $(a_1, \ldots, a_s)$ of the elements $a_1, \ldots, a_s \in R$ is, of course, defined only to within an invertible multiplier, and equality between highest common factors must always be understood in this sense. If $\mathfrak{p}$, $a \in R$ and $\mathfrak{p}$ is irreducible, then the greatest integer k such that $\mathfrak{p}^k \mid a$ will be denoted by ord $(a; \mathfrak{p})$.

Throughout the present section, n will denote a fixed non-invertible element other than zero; and we shall write $R(n)$ for the residue class ring $R/(n)$. The elements of R will be denoted by small letters and those of $R(n)$ by capital letters. If $a \in R$, we shall denote by $C(a)$ the residue class (mod n) containing a. In particular, we shall write $I = C(1)$, $Z = C(0)$.

[4]) The implication (i) $\Rightarrow$ (ii) was proved by RANUM ([3], p. 287) for the case when R is a finite-dimensional algebra, and the implication (ii) $\Rightarrow$ (i) for the case when R is a finite-dimensional algebra with a right unit element ([3], p. 289).

If x, $x' \in R$, $x \equiv x' \pmod{n}$, and $d \mid n$, then $(d, x) = (d, x')$, so that (d, x) depends only on $C(x)$. We may therefore denote it unambiguously by (d, X) where $X = C(x)$.

As we know, n possesses an (essentially unique) representation

$$n = \eta \prod_{k=1}^{r} p_k^{a_k}, \tag{10}$$

where η is an invertible element, the p_k are irreducible elements (no two of which are associated), and the a_k are positive integers. Put

$$n_k = \prod_{j \neq k} p_j^{a_j} \qquad (k = 1, \ldots, r).$$

Then $(n_1, \ldots, n_r) = 1$; and there exist therefore elements $m_1, \ldots, m_r \in R$ such that

$$n_1 m_1 + \cdots + n_r m_r = 1. \tag{11}$$

Write $E_k = C(n_k m_k)$, $k = 1, \ldots, r$. It is now a matter of immediate verification that the E_k do not depend on the particular representation (10) nor on the particular choice of the m's. We shall call $E_1, \ldots, E_r$ the *principal idempotent elements* of $R(n)$.

Our subsequent discussion of the structure of $R(n)$ will depend, in essence, on the fact that $R(n)$ is isomorphic to the direct sum of the rings $R(p_k^{a_k})$, $k = 1, \ldots, r$. However, we find it convenient to use a slightly different language.

4.2. We begin with a number of easy preliminary results.

LEMMA 1. (i) $E_1 + \cdots + E_r = I$; (ii) $E_k E_j = Z$ $(k \neq j)$; (iii) $E_k^2 = E_k \neq Z$ $(k = 1, \ldots, r)$; (iv) *if* S, T *are subsets of* $\{1, \ldots, r\}$, *and*

$$\sum_{k \in S} E_k = \sum_{k \in T} E_k,$$

then $S = T$.

Lemma 1 (i) follows immediately from (11). The remaining assertions are then derived successively by obvious arguments.

LEMMA 2. (i) $R(n)\, E_k$ *is a ring with unit element* E_k. (ii) *Let* $X \in R(n)$. *Then* XE_k *is nilpotent or invertible in* $R(n)\, E_k$ *according as* $p_k \mid (n, X)$ *or* $p_k \nmid (n, X)$. *In particular, therefore,* $R(n)\, E_k$ *is a divided ring.* (iii) $R(n)$ *is the direct sum of its subrings* $R(n)\, E_k$ $(k = 1, \ldots, r)$, *and is therefore semi-divided.*

We obtain (i) by straightforward verification and the use of Lemma 1 (iii). To prove (ii), let $x \in R$ be such that $X = C(x)$. If $p_k \mid (n, X)$, then $p_k \mid x$ and it is easily seen that $(XE_k)^{a_k} = Z$, i.e. XE_k is nilpotent. On the other hand, if $p_k \nmid (n, X)$, then $p_k \nmid x$ and there exist elements $u, v \in R$ such that $1 = p_k^{a_k} u + xv$. Hence $x n_k m_k v \equiv n_k m_k \pmod{n}$; and so, writing $V = C(v)$, we have $XE_k V = E_k$. Thus $XE_k \cdot VE_k = E_k$, i.e. XE_k is invertible in $R(n)\, E_k$.

Finally, write $X_k = XE_k$ $(k = 1, \ldots, r)$. Then, in view of Lemma 1 (i), $X = X_1 + \cdots + X_r$, where $X_k \in R(n) E_k$ $(k = 1, \ldots, r)$. Again, by Lemma 1, (ii) and (iii), this representation is unique. Moreover, by Lemma 1 (ii), $AB = Z$

whenever $A \in R(n)\, E_k$, $B \in R(n)\, E_j$, $k \neq j$. Hence $R(n)$ is the direct sum of the $R(n)\, E_k$, and the proof is complete.

Since, then, $R(n)$ is a semi-divided ring, it follows that $\mathrm{id}\, X$ is defined for every element $X \in R(n)$. By Lemma 2, (i) and (ii), we immediately infer

LEMMA 3. *For any $X \in R(n)$, we have*

$$\mathrm{id}\, X = \sum_{p_k \nmid (n, X)} E_k .$$

Our next object is to determine the index of every element in $R(n)$. When ξ is a real number, we shall denote by $\{\xi\}$ the least integer k such that $k \geqq \xi$.

LEMMA 4. *Let X be any element of $R(n)$.* (i) *If XE_k is nilpotent, its index is equal to*

$$\left\{ \frac{\mathrm{ord}\,(n; p_k)}{\mathrm{ord}\,((n, X); p_k)} \right\}.$$

(ii) *If $p_k \nmid (n, X)$ for all k, then $l(X) = 1$; otherwise*

$$l(X) = \max_k \left\{ \frac{\mathrm{ord}\,(n; p_k)}{\mathrm{ord}\,((n, X); p_k)} \right\},$$

where the maximum is taken over integers k such that $1 \leqq k \leqq r$, $\mathrm{ord}\,((n, X); p_k) > 0$.

To prove (i), denote by x any element in R such that $X = C(x)$. Let m be the index of XE_k, i.e. the least positive integer such that $X^m E_k = Z$. This relation is equivalent to $n \mid (n, x)^m n_k m_k$, and this is satisfied if and only if

$$\mathrm{ord}\,(n; p_k) \leqq m \cdot \mathrm{ord}\,((n, X); p_k).$$

This proves (i); and (ii) follows at once by (i) and Lemma 2 (ii).

4.3. Since, by Lemma 2 (iii), $R(n)$ is a semi-divided ring, all conclusions of §§ 2, 3 now apply. For example, if $X \in R(n)$, then X^t is a group member if and only if $t \geqq l(X)$; if this condition is satisfied, then $\mathrm{id}\, X$ is the unit element of $\mathfrak{M}(X^t)$. Again, all idempotent elements in $R(n)$ can be written down in terms of the principal idempotent elements of $R(n)$. Further, all elements (all group members) in $R(n)$ are distributed among disjoint classes[5]) (maximal groups). Among the maximal groups we may, in particular, note the group $\Gamma(n)$ of all $X \in R(n)$ with $(n, X) = 1$; this is, in fact, the group $\mathfrak{M}(I)$ of all elements invertible in $R(n)$. Every maximal group in $R(n)$ is a homomorphic image of this group $\Gamma(n)$.

4.4. We conclude the present section with some results which do not follow solely from the fact that $R(n)$ is a semi-divided ring.

THEOREM 11. *The element $X \in R(n)$ is a group member if and only if*

$$\left(\frac{n}{(n, X)}, X \right) = 1 . \tag{12}$$

By Theorem 9 and Lemma 2 (iii), X is a group member if and only if $l(X) = 1$. In view of Lemma 4 (ii), this condition is satisfied if and only if

$$\mathrm{ord}\,(n; p_k) = \mathrm{ord}\,((n, X); p_k)$$

[5]) The term "class" should not, of course, be confused with "residue class".

whenever the right-hand side of this equation is positive; and this is clearly equivalent to (12).

THEOREM 12. *Let X, Y be group members in $R(n)$. Then $\mathfrak{M}(X)=\mathfrak{M}(Y)$ if and only if*

$$(n, X)=(n, Y). \tag{13}$$

We know that $\mathfrak{M}(X)=\mathfrak{M}(Y)$ if and only if $\mathrm{id}\, X=\mathrm{id}\, Y$. In view of Lemmas 3 and 1 (i), this condition is equivalent to

$$\sum_{p_k \mid (n, X)} E_k = \sum_{p_k \mid (n, Y)} E_k. \tag{14}$$

If (13) is satisfied, then so is obviously (14). On the other hand, if (14) is satisfied, then, by Lemma 1 (iv),

$$P_n(X)=P_n(Y), \tag{15}$$

where $P_n(X)$ denotes the set of those elements among $p_1, \ldots, p_r$ which divide (n, X). Also, since X, Y are group members, we have, by Theorem 11,

$$\left(\frac{n}{(n, X)}, X\right)=1=\left(\frac{n}{(n, Y)}, Y\right). \tag{16}$$

From (15) and (16) we at once infer (13), and the proof is therefore complete.

THEOREM 13. *Let X and Y be any elements in $R(n)$. Then $\mathfrak{N}(X)=\mathfrak{N}(Y)$ if and only if every irreducible element of R which divides (n, X) also divides (n, Y), and conversely.*

We know that $\mathfrak{N}(X)=\mathfrak{N}(Y)$ if and only if $\mathrm{id}\, X=\mathrm{id}\, Y$, i.e. if and only if (15) holds. The assertion therefore follows.

5. Applications to the theory of numbers

Let n be an integer greater than 1, and let its representation as a product of powers of primes be given by

$$n=p_1^{a_1}\ldots p_r^{a_r}.$$

In the present section we shall be concerned with surveying the groups and classes in the ring $R(n)$ of residue classes (mod n)[6]. It will be convenient, at times, to ignore the distinction between the integer a and the residue class (mod n) containing a.

As usual, $\varphi(n)$ will denote EULER's function. D_n is to denote the set of the 2^r divisors of n of the form $p_1^{b_1}\ldots p_r^{b_r}$, where, for each value of k, b_k is either a_k or 0. Further, S_n is to denote the set of square-free divisors of n. The letter p is reserved for primes.

A number of results relating to $R(n)$ follow immediately from the general theory of § 4. For example, a is a group member in $R(n)$ if and only if $(n, a)\in D_n$; this implies, in particular, that all elements in $R(n)$ are group members if and only if n is square-free. We may also note that every maximal group

[6]) A few special results concerning $R(n)$ were noted by RANUM. See [3], pp. 307—308.

in $R(n)$ is a homomorphic image of the group $\Gamma(n)$ of the $\varphi(n)$ residue classes (mod n) and prime to n.

We next deduce a few results which are not merely consequences of the general theory.

THEOREM 14. (i) *If a is a group member in $R(n)$, then*

$$|\mathfrak{M}(a)| = \varphi\left(\frac{n}{(n, a)}\right).$$

(ii) *The orders of the 2^r maximal groups in $R(n)$ are $\varphi(d)$, $d \in D_n$.*

(iii) *The number of group members in $R(n)$ is equal to*

$$n \prod_{k=1}^{r} (1 - p_k^{-1} + p_k^{-a_k}).$$

Let a be a group member in $R(n)$ and write $(n, a) = d$, so that $d \in D_n$. In view of Theorem 12, the order of $\mathfrak{M}(a)$ is equal to the number of integers k satisfying $0 < k \leqq n$, $(n, k) = d$, i.e. to $\varphi(n/d)$. This establishes (i). Next, if $d \in D_n$, then d is a group member and, by (i), $|\mathfrak{M}(d)| = \varphi(n/d)$. Moreover, if $d_1, d_2 \in D_n$, $d_1 \neq d_2$, then $(n, d_1) \neq (n, d_2)$ and so, by Theorem 12, $\mathfrak{M}(d_1) \neq \mathfrak{M}(d_2)$. The orders of the maximal groups are therefore the numbers $\varphi(n/d)$, $d \in D_n$; hence (ii) follows. This implies that the number of group members in $R(n)$ is equal to

$$\sum_{d \in D_n} \varphi(d),$$

and this leads at once to (iii).

THEOREM 15. (i) *If a is any integer, then*

$$|\mathfrak{R}(a)| = \varphi(n) \prod_{p|(n, a)} (p - 1)^{-1}.$$

(ii) *The orders of the classes*[7]) *in $R(n)$ are the numbers*

$$\varphi(n) \prod_{p|d} (p - 1)^{-1}, \qquad d \in S_n.$$

Denote by $\varrho_1, \ldots, \varrho_i$ those primes among $p_1, \ldots, p_r$ which divide a, and by $\sigma_1, \ldots, \sigma_j$ those which do not divide a. Then, by Theorem 13, $x \in \mathfrak{R}(a)$ if and only if x is divisible by every ϱ and by no σ. It follows that

$$\begin{aligned} |\mathfrak{R}(a)| &= n(\varrho_1 \ldots \varrho_i)^{-1}(1 - \sigma_1^{-1}) \ldots (1 - \sigma_j^{-1}) \\ &= n \prod_{p|(n, a)} p^{-1} \prod_{\substack{p|n \\ p \nmid a}} (1 - p^{-1}) = \varphi(n) \prod_{p|(n, a)} (p - 1)^{-1}, \end{aligned}$$

and (i) is proved. To establish (ii), let $d \in S_n$. Then, by (i),

$$|\mathfrak{R}(d)| = \varphi(n) \prod_{p|d} (p - 1)^{-1}.$$

Moreover, if $d_1, d_2 \in S_n$, $d_1 \neq d_2$, then, by Theorem 13, $\mathfrak{R}(d_1) \neq \mathfrak{R}(d_2)$. The assertion therefore follows.

[7]) The order of a class is the number of elements contained in it.

It may be of interest to observe that Theorems 14 and 15 can also be deduced without difficulty from Corollary 1 to Theorem 8. We may note further that, for any a, $|\Gamma(n)|$ is a multiple of $|\mathfrak{R}(a)|$, while, for any group member a, $|\mathfrak{R}(a)|$ is a multiple of $|\mathfrak{M}(a)|$. The reason for this is clear from the corollaries to Theorem 8.

6. Applications to the theory of algebras

6.1. Let F be a field, A a linear associative algebra over F, and $F[x]$ the ring of polynomials in x with coefficients in F. An element $a \in A$ will be said to be *algebraic* if it satisfies an equation of the form $\psi(x) = 0$, where $\psi(x)$ is a non-constant polynomial in $F[x]$. The monic polynomial of least degree with this property is called the *minimum polynomial* of a.

By considering the homomorphic mapping $f(x) \to f(a)$ of $F[x]$ into A, we establish at once the isomorphism of the rings $F[a]$ and $F[x]/(\psi(x))$, where $\psi(x)$ is the minimum polynomial of a. Hence, using Lemma 2 (iii) and Theorem 10, we obtain

THEOREM 16. *If a is an algebraic element of A, then $F[a]$ is a semi-divided subring of A. An element $b \in F[a]$ is a group member in A if and only if it is a group member in $F[a]$.*

In view of §§ 3 and 4, the theory of group membership of algebraic elements in A can now be regarded as complete. Thus, for example, we infer from Theorems 16 and 9 that an algebraic element $a \in A$ is a group member in A if and only if $aF[a] = a^2F[a]$. We devote the remainder of this section to the derivation of results which depend essentially on the present special situation.

Throughout, let a be an algebraic element of A; let $\psi(x)$ be its minimum polynomial; and let the polynomial $\vartheta(x)$ and the non-negative integer $\mu(a)$ be defined by the relations

$$\psi(x) = x^{\mu(a)}\vartheta(x), \qquad \vartheta(0) \neq 0. \tag{17}$$

If $\mu(a) = 0$, it is clear that $\mathrm{id}\, a = 1$. If, however, $\mu(a) > 0$, then there exist polynomials $g(x)$, $h(x) \in F[x]$ such that

$$x^{\mu(a)}g(x) + \vartheta(x)h(x) = 1,$$

and it is readily verified that $\mathrm{id}\, a = a^{\mu(a)}g(a)$. It is also evident that, for the purpose of this construction, any polynomial annihilating a can be taken in place of $\psi(x)$. For example, when A is the algebra of matrices, $\mathrm{id}\, a$ can be easily computed from the characteristic polynomial of a.

THEOREM 17. *If $f(x) \in F[x]$, then $f(a)$ is a group member in A if and only if*

$$\left(\frac{\psi}{(\psi, f)}, f\right) = 1.$$

In particular[8]*, a^t is a group member if and only if $t \geqq \mu(a)$.*

This follows at once from Theorems 16 and 11.

[8]) This last result was proved by RANUM ([3], p. 295) for the case when A is finite-dimensional.

THEOREM 18. *Let $\mu(a)=1$, so that a is a group member. If $\eta(x)$ denotes the polynomial $\{\vartheta(0)-\vartheta(x)\}/x\vartheta(0)$, then*

$$\mathrm{id}\, a = a\cdot\eta(a), \qquad a^{-1}=a\cdot\eta^2(a).$$

Writing $\vartheta(0)=c$, we have $x\eta(x)+c^{-1}\vartheta(x)=1$. Hence $\mathrm{id}\, a = a\cdot\eta(a)$, and therefore

$$a^{-1}=a^{-1}\,\mathrm{id}\, a = a^{-1}a\cdot\eta(a)=\mathrm{id}\, a\cdot\eta(a)=a\cdot\eta^2(a).$$

RANUM ([3], p. 295) gave an expression for $\mathrm{id}\, a$ equivalent to ours, and also indicated how a^{-1} could be calculated.

THEOREM 19. *If a, b are commuting algebraic elements which are group members in Λ, then ab is also a group member in Λ.*

The unit elements of the maximal groups containing a, b are $\mathrm{id}\, a$, $\mathrm{id}\, b$ respectively. Since $ab=ba$ and since $\mathrm{id}\, a$, $\mathrm{id}\, b$ are polynomials in a, b respectively, it follows that the four elements a, b, $\mathrm{id}\, a$, $\mathrm{id}\, b$ commute in pairs. Hence the set of all elements of Λ of the form $a^r b^s$ ($r, s=0, \pm1, \pm2, \ldots$), where $a^0=\mathrm{id}\, a$, $b^0=\mathrm{id}\, b$, is a group which contains ab. (It is, moreover, almost obvious that ab is algebraic, but we do not require this fact.)

The condition of commutativity in Theorem 19 cannot be dispensed with. For, if Λ is the algebra of 2×2 matrices and

$$a=\begin{pmatrix}1&0\\0&0\end{pmatrix}, \qquad b=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

then a, b are group members, but ab is not.

6.2. For the remainder of this section, we shall take Λ to be the algebra of $n\times n$ matrices over F, but shall continue to use the notation specified by (17). The rank of a matrix a will be denoted by $R(a)$.

It follows from Theorem 17 that a is a group member if and only if $\mu(a)\leqq1$. Now any matrix a is similar to the direct sum of a non-singular matrix a_1 and a nilpotent matrix a_2; and it is clear that $\mu(a)\leqq1$ if and only if $a_2=0$. Again, $R(a)=R(a^2)$ if and only if $a_2=0$, and this gives us another necessary and sufficient condition for group membership. Further, since $\mathrm{id}\, a=a^{\mu(a)}g(a)$ and $a_2^{\mu(a)}=0$, and since $g(a_1)$ is non-singular, it follows that $R(\mathrm{id}\, a)=R(a_1)$. Hence a is a group member if and only if $R(a)=R(\mathrm{id}\, a)$. Finally, a is a group member if and only if there exists a matrix u such that $u^2=u$, $au=ua=a$, $R(u)=R(a)$. The necessity of this condition is obvious; we establish the sufficiency by observing that u is similar to the direct sum of a unit matrix and a zero matrix, and hence deducing that $a_2=0$[9]).

6.3. We know that every group member a belongs to a unique maximal group $\mathfrak{M}(a)$. However, in general there exists no abelian group $\mathfrak{G}$ such that every abelian group containing a is a subgroup of $\mathfrak{G}$. (For example, take a to be the unit matrix and let b, c be non-commuting non-singular matrices. The cyclic groups generated by b and c are abelian and both contain a, but

[9]) Some further criteria for group membership are given by RANUM ([2], § 6).

they cannot be subgroups of the same abelian group.) Nevertheless, if a is non-derogatory (i.e. if its minimum polynomial and characteristic polynomial are equal), then a unique maximal abelian group containing a does, in fact, exist. To be more precise, we have the following result.

THEOREM 20. *If the non-derogatory matrix a is a group member, then every abelian group containing a is a subgroup of the abelian group* $(\mathrm{id}\, a)\, \mathfrak{P}(a)$, *where* $\mathfrak{P}(a)$ *denotes the set of all non-singular matrices in* $F[a]$.

Every abelian group containing a must be a subgroup of the normalizer $\mathfrak{N}(a)$ of a in $\mathfrak{M}(a)$. But, by Theorem 3 (i), $\mathfrak{N}(a)$ is the set of all matrices which commute with a and have the form $(\mathrm{id}\, a)\, y$, where y is a non-singular matrix commuting with $\mathrm{id}\, a$. Hence $\mathfrak{N}(a)$ is the set of all matrices of the form $(\mathrm{id}\, a)\, y$, where y is a non-singular matrix commuting with a. But, since a is non-derogatory, y must be a polynomial in a (see e.g. [1], pp. 69 and 107), and the assertion therefore follows. The trivial instance of the zero matrix shows, however, that there also exist derogatory matrices which are contained in a unique maximal abelian group.

In conclusion, we wish to thank Professor H. WIELANDT for a number of helpful comments.

Added in proof. Since submitting our paper, we have seen a short note by W. E. BARNES and H. SCHNEIDER [Arch. Math. **8**, 166–168 (1957)] in which some problems similar to those discussed by us are considered. In particular, BARNES and SCHNEIDER prove a result substantially equivalent to our Theorem 17. They also raise the following question: if S is a subring of a ring R and $a \in S$ is a group member in R, under what conditions is it a group member in S? Our Theorem 10 provides a partial answer to this question.

References

[1] JACOBSON, N.: Lectures in abstract algebra, vol. II. New York 1953. — [2] RANUM, A.: The group membership of singular matrices. Amer. J. Math. **31**, 18–41 (1909). — [3] RANUM, A.: The groups belonging to a linear associative algebra. Amer. J. Math. **49**, 285–308 (1927). — [4] WEDDERBURN, J. H. M.: Lectures on matrices. Amer. Math. Soc. Colloquium Publications, 1934.

Dept. of Mathematics, University of Sheffield (England)

(Eingegangen am 29. Mai 1958)

PERRON, O.
Math. Zeitschr. Bd. 70, S. 245—249 (1958)

Über zwei ausgeartete Heinesche Reihen und einen Kettenbruch von Ramanujan

Von
OSKAR PERRON

§ 1. Wir betrachten die beiden unendlichen Reihen

$$(1)\quad G(b,q;x)=1+\sum_{\lambda=1}^{\infty}\frac{q^{\lambda^2}}{(1-q)(1-q^2)\dots(1-q^\lambda)}\cdot\frac{b^\lambda x^\lambda}{(1+b)(1+bq)\dots(1+bq^{\lambda-1})},$$

$$(2)\quad H(b,q;x)=1+\sum_{\lambda=1}^{\infty}\frac{q^{\lambda}}{(1-q)(1-q^2)\dots(1-q^\lambda)}\cdot\frac{(-x)^\lambda}{(1+b)(1+bq)\dots(1+bq^{\lambda-1})},$$

die man, wenn man $b=-q^\nu$ setzt, leicht als Grenzfälle der bekannten HEINEschen Reihe erkennt. Dabei darf natürlich kein Nenner verschwinden, also insbesondere q keine Einheitswurzel sein. Auch wenn q zwar keine Einheitswurzel, aber doch $|q|=1$ ist, kann das Konvergenzverhalten sehr unterschiedlich sein, je nachdem, wie stark sich q durch Einheitswurzeln approximieren läßt. Wir sehen davon ab, setzen also $|q|\neq 1$ voraus.

Für $0<|q|<1$ ist $G(b,q;x)$ augenscheinlich eine *ganze* Funktion von x. Für $|q|>1$ ist die Reihe $G(b,q;x)$, falls $b=0$ ist, konstant gleich 1, und falls $b\neq 0$ ist, konvergiert sie nur im Kreis $|x|<1$; wir werden aber sehen, daß sie sich darüber hinaus als *meromorphe* Funktion von x fortsetzt, und werden sie auch als Quotienten von zwei ganzen Funktionen von x darstellen können [Formel (11)].

Für $|q|>1$ ist $H(b,q;x)$ eine *ganze* Funktion von x. Für $0<|q|<1$ konvergiert die Reihe $H(b,q;x)$ nur im Kreis $|x|<|q|^{-1}$; wir werden aber sehen, daß sie sich darüber hinaus als *meromorphe* Funktion von x fortsetzt, und werden sie auch als Quotienten von zwei ganzen Funktionen von x darstellen können [Formel (12)].

Zwischen den Funktionen G und H besteht, wie unmittelbar zu kontrollieren, der Zusammenhang

$$(3)\qquad G(b,q;x)=H(b^{-1},q^{-1};qx),$$

$$(4)\qquad H(b,q;x)=G(b^{-1},q^{-1};qx),$$

so daß es genügen würde, sich mit einer der beiden zu beschäftigen. Es ist aber doch nützlich, alle beide zu betrachten.

§ 2. Man verifiziert leicht die Identität

$$(5)\qquad G(b,q;x)-G(bq,q;x)=\frac{bqx}{(1+b)(1+bq)}G(bq^2,q;x),$$

und indem man b durch bq^ν ersetzt,

$$G(bq^\nu, q; x) - G(bq^{\nu+1}, q; x) = \frac{bq^{\nu+1}x}{(1+bq^\nu)(1+bq^{\nu+1})} G(bq^{\nu+2}, q; x).$$

Hieraus folgt, wenn zur Abkürzung

$$\frac{G(bq^\nu, q; x)}{G(bq^{\nu+1}; q; x)} = \mathfrak{P}_\nu(x)$$

gesetzt wird, sofort die Identität

$$\mathfrak{P}_\nu(x) = 1 + \frac{\dfrac{bq^{\nu+1}}{(1+bq^\nu)(1+bq^{\nu+1})}x}{\mathfrak{P}_{\nu+1}(x)},$$

und daraus nach Satz 3.5 S. 110 meines Buches[1]) die Korrespondenzformel

$$\mathfrak{P}_0(x) \sim 1 + \cfrac{\dfrac{bq}{(1+b)(1+bq)}x}{1} + \cfrac{\dfrac{bq^2}{(1+bq)(1+bq^2)}x}{1} + \cdots.$$

Dieser Kettenbruch stellt sowohl für $0<|q|<1$ als auch für $|q|>1$ nach Satz 3.28 S. 149 meines Buches eine meromorphe Funktion von x dar, die in der Umgebung des Nullpunktes gleich der korrespondierenden Reihe, also gleich $\mathfrak{P}_0(x) = \frac{G(b, q; x)}{G(bq, q; x)}$ ist. Daher kann man das Korrespondenzzeichen $\sim$ durch ein Gleichheitszeichen ersetzen; wenn man dann noch mit $1+b$ multipliziert und zur Vermeidung der Brüche in den Teilzählern zu einem äquivalenten Kettenbruch übergeht, erhält man die Formel

$$(6) \qquad (1+b)\frac{G(b, q; x)}{G(bq, q; x)} = 1 + b + \cfrac{bqx}{1+bq} + \cfrac{bq^2x}{1+bq^2} + \cfrac{bq^3x}{1+bq^3} + \cdots,$$

oder, indem man xb^{-1} an Stelle von x schreibt,

$$(7) \qquad 1 + b + \cfrac{xq}{1+bq} + \cfrac{xq^2}{1+bq^2} + \cfrac{xq^3}{1+bq^3} + \cdots = (1+b)\frac{G(b, q; xb^{-1})}{G(bq, q; xb^{-1})}.$$

Den Kettenbruch (7) hat RAMANUJAN in seinem berühmten Brief an HARDY erwähnt, ohne mehr von ihm zu verraten, als daß es über ihn ein „allgemeines Theorem" gebe, in dem gewisse sehr merkwürdige sich auf den Kettenbruch $1 + \cfrac{q}{1} + \cfrac{q^2}{1} + \cfrac{q^3}{1} + \cdots$ beziehende Formeln, die er ohne Beweis mitteilt, als Spezialfälle enthalten seien[2]). Die Formel (7) für den Spezialfall $b=0$, $|q|<1$ wurde von G. N. WATSON gefunden[3]) und sie diente ihm als Schlüssel, um bis zu den merkwürdigen Formeln von RAMANUJAN vorzudringen, wobei der ganze weitere Weg gar nichts mehr mit Kettenbrüchen zu tun hatte, sondern aus einem kunstvollen Operieren mit den Reihen bestand. Daher habe ich schon auf S. 127 meines Buches, woselbst

[1]) PERRON, O.: Die Lehre von den Kettenbrüchen, 3. Aufl., Bd. II. Stuttgart 1957

[2]) Siehe Collected Papers of Srinivasa Ramanujan, S. XXVIII. Cambridge 1927.

[3]) Man beachte, daß nach der Definitionsformel (1) die Reihe $G(b, q; xb^{-1})$ auch für $b=0$ sinnvoll bleibt und dann für $|q|<1$ konvergiert.

Literatur, die Vermutung geäußert, daß auch RAMANUJAN wohl im Besitz der Formel (7) mit $b=0$, $|q|<1$ war und einen ähnlichen Weg wie WATSON eingeschlagen hatte. Ich möchte nun nach diesen Zusammenhängen weiter vermuten, daß RAMANUJAN sogar im Besitz der allgemeinen Formel (7) war, obwohl ich allerdings keine Ahnung habe, welche weiteren merkwürdigen Formeln er daraus etwa noch gewonnen und mit dem „allgemeinen Theorem" gemeint haben mag.

§ 3. Man verifiziert auch leicht die Identität

$$H(b,q;x)-H(bq,q;x)=\frac{bqx}{(1+b)(1+bq)}H(bq^2,q;x). \tag{8}$$

Aus dieser ergibt sich, genau wie vorhin aus der Identität (5) die Formel (6) gewonnen wurde, die weitere Formel

$$(1+b)\frac{H(b,q;x)}{H(bq,q;x)}=1+b+\frac{bqx}{|1+bq}+\frac{bq^2x}{|1+bq^2}+\frac{bq^3x}{|1+bq^3}+\cdots. \tag{9}$$

Durch Vergleich mit (6) folgt dann

$$\frac{G(b,q;x)}{G(bq,q;x)}=\frac{H(b,q;x)}{H(bq,q;x)}$$

oder, etwas anders geschrieben:

$$\frac{H(b,q;x)}{G(b,q;x)}=\frac{H(bq,q;x)}{G(bq,q;x)}. \tag{10}$$

Das besagt, daß die linke Seite der Gl. (10) als Funktion von b sich nicht ändert, wenn man b durch bq ersetzt, und rückwärts gelesen, daß sie sich auch nicht ändert, wenn man b durch bq^{-1} ersetzt. Indem man beides wiederholt tut, ergibt sich allgemein:

$$\frac{H(b,q;x)}{G(b,q;x)}=\frac{H(bq^n,q;x)}{G(bq^n,q;x)} \qquad (n=\pm 1,\pm 2,\pm 3,\ldots).$$

Durch den Grenzübergang $n\to\pm\infty$ folgt hieraus, weil $|q|\neq 1$ ist,

$$\frac{H(b,q;x)}{G(b,q;x)}=\frac{H(0,q;x)}{G(0,q;x)}=\frac{H(\infty,q;x)}{G(\infty,q;x)}.$$

Da nun augenscheinlich $G(0,q;x)=1$ und $H(\infty,q;x)=1$ ist, ergibt sich:

$$G(b,q;x)=\frac{H(b,q;x)}{H(0,q;x)}=\frac{H(b,q;x)}{1+\sum_{\lambda=1}^{\infty}\frac{q^{\lambda}(-x)^{\lambda}}{(1-q)(1-q^2)\ldots(1-q^{\lambda})}}, \tag{11}$$

$$H(b,q;x)=\frac{G(b,q;x)}{G(\infty,q;x)}=\frac{G(b,q;x)}{1+\sum_{\lambda=1}^{\infty}\frac{q^{\frac{1}{2}\lambda(\lambda+1)}x^{\lambda}}{(1-q)(1-q^2)\ldots(1-q)^{\lambda}}}, \tag{12}$$

$$\left(1+\sum_{\lambda=1}^{\infty}\frac{q^{\frac{1}{2}\lambda(\lambda+1)}x^{\lambda}}{(1-q)(1-q^2)\ldots(1-q^{\lambda})}\right)\cdot\left(1+\sum_{\lambda=1}^{\infty}\frac{q^{\lambda}(-x)^{\lambda}}{(1-q)(1-q^2)\ldots(1-q^{\lambda})}\right)=1. \tag{13}$$

Die Formeln (11), (12), (13) gelten natürlich wie alle früheren sowohl für $0<|q|<1$ als auch für $|q|>1$ innerhalb ihres Konvergenzkreises in der x-Ebene. Speziell für $|q|>1$ ist die in diesem Fall nicht ganze Funktion $G(b, q; x)$ durch (11) als Quotient von zwei ganzen Funktionen dargestellt, wie in § 1 angekündigt. Und für $0<|q|<1$ ist die in diesem Fall nicht ganze Funktion $H(b, q; x)$ durch (12) als Quotient von zwei ganzen Funktionen dargestellt.

§ 4. Man verifiziert leicht durch einfaches Ausmultiplizieren die Identität

$$H(0, q; x) \cdot (1 + qx) = H(0, q; qx),$$

und indem man hier x durch $qx, q^2x, \ldots, q^n x$ ersetzt und dann multipliziert ergibt sich

$$H(0, q; x) \cdot (1 + qx)(1 + q^2x) \ldots (1 + q^n x) = H(0, q; q^n x).$$

Im Fall $|q|<1$ hat offenbar die rechte Seite für $n \to \infty$ den Limes 1, und man erhält, wenn man für $H(0, q; x)$ die Reihe einsetzt, die Formel

$$(14) \quad 1 + \sum_{\lambda=1}^{\infty} \frac{q^\lambda (-x)^\lambda}{(1-q)(1-q^2)\ldots(1-q^\lambda)} = \prod_{n=1}^{\infty} \frac{1}{1+q^n x} \quad \text{für } |q|<1,\ |x|<|q|^{-1}.$$

Aus (13) folgt dann weiter

$$(15) \quad 1 + \sum_{\lambda=1}^{\infty} \frac{q^{\frac{1}{2}\lambda(\lambda+1)} x^\lambda}{(1-q)(1-q^2)\ldots(1-q^\lambda)} = \prod_{n=1}^{\infty} (1+q^n x) \quad \text{für } |q|<1.$$

Diese beiden Formeln sind nicht neu. Sie stehen schon in EULERs Introductio in analysin infinitorum, tom. I, cap. XVI = Opera omnia, Ser. I, vol. VIII.

Indem man q durch q^{-1} ersetzt, gehen die Formeln (14), (15) über in

$$1 + \sum_{\lambda=1}^{\infty} \frac{q^{\frac{1}{2}\lambda(\lambda-1)} x^\lambda}{(1-q)(1-q^2)\ldots(1-q^\lambda)} = \prod_{n=1}^{\infty} \frac{1}{1+q^{-n}x} \quad \text{für } |q|>1,\ |x|<q,$$

$$1 + \sum_{\lambda=1}^{\infty} \frac{(-x)^\lambda}{(1-q)(1-q^2)\ldots(1-q^\lambda)} = \prod_{n=1}^{\infty} (1+q^{-n}x) \quad \text{für } |q|>1,$$

oder, wenn man x zwecks Angleichung an (15) und (14) durch qx ersetzt,

$$(16) \quad 1 + \sum_{\lambda=1}^{\infty} \frac{q^{\frac{1}{2}\lambda(\lambda+1)} x^\lambda}{(1-q)(1-q^2)\ldots(1-q^\lambda)} = \prod_{n=0}^{\infty} \frac{1}{1+q^{-n}x} \quad \text{für } |q|>1,\ |x|<1,$$

$$(17) \quad 1 + \sum_{\lambda=1}^{\infty} \frac{q^\lambda (-x)^\lambda}{(1-q)(1-q^2)\ldots(1-q^\lambda)} = \prod_{n=0}^{\infty} (1+q^{-n}x) \quad \text{für } |q|>1.$$

Aus (11) in Verbindung mit (17) erkennt man sofort die Pole der für $|q|>1$ meromorphen Funktion $G(b, q; x)$; es sind die Werte $x = -q^n$ ($n = 0$,

1, 2, ...). Ebenso erkennt man aus (12) in Verbindung mit (15) die Pole der für $0<|q|<1$ meromorphen Funktion $H(b, q; x)$; es sind die Werte $x=-q^{-n}$ $(n=1, 2, 3, \ldots)$.

§ 5. Bemerkt sei noch, daß in unseren Funktionen als Grenzfall auch die Exponentialfunktion steckt. Es ist nämlich, wie sofort zu sehen,

$$\lim_{q\to 1} G(b, q; (1-q)\,x) = 1 + \sum_{\lambda=1}^{\infty} \frac{b^\lambda x^\lambda}{\lambda!(1+b)^\lambda} = \exp\left(\frac{b\,x}{1+b}\right),$$

$$\lim_{q\to 1} H(b, q; (1-q)\,x) = 1 + \sum_{\lambda=1}^{\infty} \frac{(-x)^\lambda}{\lambda!(1+b)^\lambda} = \exp\left(\frac{-x}{1+b}\right).$$

Die Formeln (11, (12), (13) gehen bei diesem Grenzprozeß in simple Beziehungen über, die auf das Additionstheorem der Exponentialfunktion hinauslaufen, während die Kettenbruchformeln sogar nur in $1=1$ übergehen.

München 27, Friedrich-Herschel-Str. 11

(Eingegangen am 4. Juni 1958)

DEKKER, J. C. E.
Math. Zeitschr. Bd. 70, S. 250–262 (1958)

The Factorial Function for Isols*)

By

J.C.E. DEKKER

1. INTRODUCTION. The reader is assumed to be familiar with the first two sections of [*1*]. S. TENNENBAUM suggested to the author a definition of $X!$ in Λ which is an extension of the factorial function in ε[1]). In the present paper we shall establish a few properties of this factorial function in Λ, in particular:

$$(X+1)! = (X+1)\cdot X!, \tag{1.1}$$

$$Y \leqq X \Rightarrow Y! \,|\, X!. \tag{1.2}$$

As a side result we shall extend the function

$$C(x, y) = \frac{x!}{y!(x-y)!} \quad \text{for } y \leqq x,$$

from $\varepsilon \times \varepsilon$ to $\Lambda \times \Lambda$ and prove for this extension:

$$Y+1 \leqq X \Rightarrow C(X+1, Y+1) = C(X, Y) + C(X, Y+1).$$

We do not know whether the function $X!$ as defined below is the only extension of $x!$ from ε to Λ which satisfies (1.1) and (1.2).

2. THE DEFINITION. In the following the word *permutation* will only be used in the restricted sense of a permutation of ε which maps almost all elements of ε onto themselves. Under this agreement every permutation is a recursive function of one variable. It is readily verified that for every permutation p,

$$\{x \,|\, p(x) \neq x\} = \{p(x) \,|\, p(x) \neq x\}.$$

We define

$$\pi p = \{x \,|\, p(x) \neq x\}.$$

A permutation p is said to be *given* if the elements and the cardinality of the finite set πp are given and also the image under p of every element in πp. The proof of the following proposition is left to the reader.

---

*) Presented to the American Mathematical Society, October 26, 1957.

[1]) The author is indebted to Mr. S. TENNENBAUM for his permission to use this definition.

P1. *There exists a recursive function $p_n(x)$ of n and x such that:*

(a) for every n, $p_n(x)$ is a permutation,

(b) $p_0(x)$ is the identity, i.e., $\pi p_0 = o$,

(c) for any permutation $p(x)$ there is exactly one number i such that $p(x) = p_i(x)$, and given $p(x)$, i can be effectively found.

It is clear that there are denumerably many functions $p_n(x)$ with the properties listed in P1. From now on we assume, however, that one such function has been selected once and for all. We define:

$$\mathfrak{P}_\sigma = \{p_n | \pi p_n < \sigma\}$$
$$\sigma! = \{n | p_n \in \mathfrak{P}_\sigma\} = \{n | \pi p_n < \sigma\}.$$

Note that $o! = (0)$. The cardinality of any set σ will be denoted by $\mathrm{card}(\sigma)$, but this notation will only be used in case σ is finite. We shall write $fg(x)$ for $f(g(x))$.

A function $f(x)$ is called *special* if it has the following four properties: (1) δf is finite, (2) $\delta f = \varrho f$, (3) f is one-to-one, (4) $x \in \delta f$ implies $f(x) \neq x$. The special function $f(x)$ is said to be *given* if both the elements and the cardinality of δf are given and also the image under f of every element in δf.

P2. *There exists a partial recursive function $b_n(x)$ of n and x such that:*

(a) for every n, $b_n(x)$ is a special function,

(b) $b_0(x)$ is nowhere defined, i.e., $\delta b_0 = o$,

(c) for any special function $f(x)$ there is exactly one number i such that $f(x) = b_i(x)$, and given $f(x)$, i can be effectively found.

Proof. If for every n, $b_n(x)$ is the restriction of $p_n(x)$ to the domain πp_n, the function $b_n(x)$ of n and x satisfies the requirements.

From now on we assume that $b_n(x)$ denotes the function defined in terms of $p_n(x)$ as described in the proof of P2.

P3. $\sigma! = \{n | \delta b_n < \sigma\}$.

Proof. Left to the reader.

P4. $\sigma \simeq \tau \Rightarrow \sigma! \simeq \tau!$.

Proof. Assume $\sigma \simeq \tau$; let $q(x)$ be a partial recursive one-to-one function such that $\sigma < \delta q$ and $q(\sigma) = \tau$. Put $\eta = \{n | \delta b_n < \delta q\}$. For every $n \in \eta$ we associate with the function b_n a function $c_n = \Phi\langle b_n \rangle$ in the following manner:

$$\left.\begin{aligned} c_0(x) &= b_0(x), \\ \delta c_n &= q(\delta b_n) \\ c_n q(x) &= q b_n(x) \end{aligned}\right\} \quad \text{for } n \geqq 1.$$

It is readily seen that for every $n \in \eta$ the function c_n is special and that Φ is effective and one-to-one. There exists a partial recursive one-to-one function $r(n)$ such that $\delta r = \eta$ and $c_n = b_{r(n)}$. Hence

$$n \in \sigma! \Leftrightarrow \delta b_n < \sigma \Leftrightarrow \delta b_{r(n)} < \tau \Leftrightarrow r(n) \in \tau!$$

This implies $\sigma! \simeq \tau!$.

P5. *σ isolated $\Leftrightarrow \sigma!$ isolated.*

PROOF. We establish the contrapositives of the two conditionals. Assume $\sigma!$ not isolated; let δ be an infinite r.e. subset of $\sigma!$. Then the set $\gamma = \Sigma \pi p_n$ with n ranging over δ is an infinite r.e. subset of σ. Now assume σ is not isolated; let η be an infinite r.e. subset of σ and e_n a one-to-one recursive function ranging over η. There must now exist a one-to-one recursive function $t(n)$ such that:

$$p_{t(n)}(e_{2n}) = e_{2n+1}, \quad p_{t(n)}(e_{2n+1}) = e_{2n}$$
$$p_{t(n)}(x) = x \quad \text{for} \quad x \notin (e_{2n}, e_{2n+1}).$$

Then $\tau = \varrho t$ is an infinite r.e. subset of $\sigma!$.

P6. *Let σ be finite. Then $\sigma!$ is finite and*

$$card(\sigma!) = (card\, \sigma)!.$$

PROOF. Let σ be finite and have cardinality k. Then $\sigma! = \{n \mid \pi p_n < \sigma\}$ is clearly finite. Let $\mathfrak{F}$ be the family of all one-to-one mappings from σ onto itself. Let for every $f \in \mathfrak{F}$,

$$\Psi\langle f\rangle(x) = \begin{cases} f(x) & \text{for} \quad x \in \sigma, \\ x & \text{for} \quad x \notin \sigma, \end{cases}$$

then Ψ maps $\mathfrak{F}$ one-to-one into $\mathfrak{P}_\sigma$. For every $g \in \mathfrak{P}_\sigma$ there exists an $f \in \mathfrak{F}$ such that $\Psi\langle f\rangle = g$, namely, the restriction of g to the domain σ. $\mathfrak{P}_\sigma$ has therefore the same cardinality as $\mathfrak{F}$. Thus $\text{card}(\sigma!) = k! = (\text{card}\, \sigma)!$.

DEFINITION. $X! = \text{Req}\, \xi!$ for any $\xi \in X$.

This definition is independent of the choice of the set $\xi \in X$ by P4. The system A is closed under the factorial function by P5. The function $X!$ is an extension of the function $x!$ by P6. Note that $0! = 1$, since $o! = (0)$.

In addition to the properties of A listed in section 2 of [1] we shall use:

$$AC = BC \,\&\, C \neq 0 \Rightarrow A = B \tag{2.1}$$

which is proved in [2]. If $B \mid A$ and $B \neq 0$, the unique element X such that $BX = A$ is denoted by A/B. We clearly have:

$$B \neq 0 \,\&\, C \neq 0 \,\&\, B \mid A \Rightarrow BC \mid AC \,\&\, \frac{AC}{BC} = \frac{A}{B}, \tag{2.2}$$

$$C \neq 0 \,\&\, BC \mid AC \Rightarrow B \mid A, \tag{2.3}$$

$$C \neq 0 \,\&\, C \mid A \,\&\, C \mid B \Rightarrow C \mid A + B \,\&\, \frac{A+B}{C} = \frac{A}{C} + \frac{B}{C}. \tag{2.4}$$

3. THE PRINCIPAL THEOREMS.

THEOREM T1. $(A+1)! = (A+1) \cdot A!$.

PROOF. Let $\alpha \in A$, $t \notin \alpha$, $\beta = \alpha + (t)$, then $\alpha! \in A!$, $\beta \in A+1$ and $\beta! \in (A+1)!$. We wish to show that $j(\alpha! \times \beta) \simeq \beta!$. For any family $\mathfrak{P}$ of permutations and any set σ we denote the collection of all ordered pairs $\langle p, s\rangle$ with $p \in \mathfrak{P}$ and $s \in \sigma$ by $\mathfrak{P} \times \sigma$. Let $\mathfrak{P}_t$ denote the family of all permutations which leave t

fixed. We associate with every $\langle p, e\rangle \in \mathfrak{P}_t \times \varepsilon$ a function $q = \Phi\langle p, e\rangle$ defined by

$$\begin{cases} q(x) = p(x) & \text{for} \quad x \neq e \quad \text{and} \quad x \neq t, \\ q(e) = p(t) = t, \\ q(t) = p(e). \end{cases}$$

Note that $q = p$ in case $e = t$, whereas q is obtained from p by interchanging the images of e and t in case $e \neq t$. This shows that Φ maps $\mathfrak{P}_t \times \varepsilon$ into $\mathfrak{P}_\varepsilon$. We claim:

(I) Φ maps $\mathfrak{P}_\alpha \times \beta$ onto $\mathfrak{P}_\beta$,

(II) Φ is one-to-one.

Proof of (I). We first show:

(α) $\pi p < \pi q < \pi p + (e, t)$.

Let $x_0 \in \pi p$, i.e., $x_0 \neq p(x_0)$. If $x_0 \notin (e, t)$, $q(x_0) = p(x_0)$, hence $q(x_0) \neq x_0$ and $x_0 \in \pi q$. Now assume $x_0 \in (e, t)$. Observe that $x_0 \neq t$, because $p(x_0) \neq x_0$. Thus $x_0 = e$; this implies $e \neq t$, since $x_0 \neq t$. However, $q(e) = t$, hence $q(e) \neq e$ and $e \in \pi q$. We conclude that $x_0 \in \pi p$ implies $x_0 \in \pi q$, i.e., $\pi p < \pi q$. Since $q(x)$ is identical with $p(x)$ for $x \notin (e, t)$, the only numbers which might belong to $\pi q - \pi p$ are e and t. We have therefore verified (α). Let $q = \Phi\langle p, e\rangle$, where $p \in \mathfrak{P}_\alpha$, $e \in \beta$. Then $\pi p < \alpha < \beta$, $t \in \beta$ and $e \in \beta$. It follows by (α) that $\pi q < \beta$, i.e., $q \in \mathfrak{P}_\beta$. Thus Φ maps $\mathfrak{P}_\alpha \times \beta$ into $\mathfrak{P}_\beta$. Let $q \in \mathfrak{P}_\beta$. We distinguish two cases.

Case 1. $q(t) = t$. Then $q = \Phi\langle q, t\rangle$, where $\langle q, t\rangle \in \mathfrak{P}_\alpha \times \beta$.

Case 2. $q(t) \neq t$. Then there exist elements a_1 and a_2 in β such that $q(a_1) = t$ and $q(t) = a_2$. Let

$$r(x) = \begin{cases} q(x) & \text{for} \quad x \notin (a_1, t), \\ t & \text{for} \quad x = t, \\ a_2 & \text{for} \quad x = a_1. \end{cases}$$

From $\pi r < \beta = \alpha + (t)$ and $t \notin \pi r$ we infer that $\pi r < \alpha$. Hence $q = \Phi\langle r, a_1\rangle$ where $\langle r, a_1\rangle \in \mathfrak{P}_\alpha \times \beta$. Since every member of $\mathfrak{P}_\beta$ is the image under Φ of some member of $\mathfrak{P}_\alpha \times \beta$, it follows that Φ maps $\mathfrak{P}_\alpha \times \beta$ onto $\mathfrak{P}_\beta$.

Proof of (II). Let $q = \Phi\langle p, e\rangle$, $q' = \Phi\langle p', e'\rangle$, where $\langle p, e\rangle \neq \langle p', e'\rangle$. To establish $q \neq q'$ we distinguish two cases.

Case 1. $e \neq e'$. Then $p(e) \neq p(e')$, $q(t) = p(e)$ and $q'(t) = p(e')$. Hence $q(t) \neq q'(t)$ and $q \neq q'$.

Case 2. $e = e'$. Then $\langle p, e\rangle \neq \langle p', e'\rangle$ implies $p \neq p'$, say $p(x_1) \neq p'(x_1)$. Either $x_1 \neq e$ or $x_1 = e$. First consider the case $x_1 \neq e$. In view of $p(t) = t = p'(t)$, it is impossible that $x_1 = t$; hence $x_1 \notin (e, t)$. This implies $q(x_1) = p(x_1)$ and $q'(x_1) = p'(x_1)$; since $p(x_1) \neq p'(x_1)$, we now have $q(x_1) \neq q'(x_1)$, hence $q \neq q'$. Now consider the case $x_1 = e$. Then $p(e) \neq p'(e)$, $q(t) = p(e)$ and $q'(t) = p'(e)$. Hence $q(t) \neq q'(t)$ and $q \neq q'$. Thus Φ is one-to-one.

Let $\tau = \{n \mid p_n(t) = t\}$. The mapping Φ is clearly effective. In fact, there must exist a partial recursive function $f(m, y)$ with $\tau \times \varepsilon$ as domain such that

$$\langle n, y\rangle \in \tau \times \varepsilon \Rightarrow \Phi\langle p_n, y\rangle = p_{f(n,y)}.$$

Using the properties of Φ verified above we conclude that f maps $\tau \times \varepsilon$ one-to-one into ε, whereas f maps $\alpha! \times \beta$ onto $\beta!$. Let $k(z)$ and $l(z)$ be the primitive recursive functions such that $j(k(z), l(z)) = z$. Put $g(z) = f(k(z), l(z))$ and $\eta = j(\tau \times \varepsilon)$. Then

$$j(\alpha! \times \beta) \subset \eta = \delta g, \quad gj(\alpha! \times \beta) = \beta!,$$

where g is partial recursive and one-to-one. Hence $j(\alpha! \times \beta) \simeq \beta!$ and $(A+1) \cdot A! = (A+1)!$.

THEOREM T2. $A! \cdot B! \mid (A+B)!$.

PROOF. We first introduce some notations and terminology. For any two disjoint sets η and ϑ and any $p \in \mathfrak{P}_{\eta+\vartheta}$ we define:

$$\eta[p] = \{x \mid x \in \eta \,\&\, p(x) \in \vartheta\},$$
$$\vartheta[p] = \{x \mid x \in \vartheta \,\&\, p(x) \in \eta\},$$
$$\mathfrak{Q}_{\eta,\vartheta} = \{p \mid p \in \mathfrak{P}_{\eta+\vartheta} \,\&\, \eta[p] = \vartheta[p] = o\}.$$

The family $\mathfrak{Q}_{\eta,\vartheta}$ consists therefore of all members of $\mathfrak{P}_{\eta+\vartheta}$ which map η onto itself and ϑ onto itself. The permutation $p \in \mathfrak{P}_{\eta+\vartheta}$ is said to have the property $\Pi_{\eta,\vartheta}$ if

(1) $x, y \in \eta[p] \,\&\, x < y \Rightarrow p(x) < p(y)$,

(2) $x, y \in \vartheta[p] \,\&\, x < y \Rightarrow p(x) < p(y)$,

(3) $x \notin \eta[p] + \vartheta[p] \Rightarrow p(x) = x$.

Thus, a member of $\mathfrak{P}_{\eta+\vartheta}$ has $\Pi_{\eta,\vartheta}$ if it maps $\eta[p]$ and $\vartheta[p]$ on each other in the order-preserving manner, and acts otherwise as the identity; each such permutation p has the property that p^2 equals the identity.

LEMMA. *Let η and ϑ be disjoint, $\mathfrak{P} = \mathfrak{P}_{\eta+\vartheta}$, $\mathfrak{Q} = \mathfrak{Q}_{\eta,\vartheta}$ and $\mathfrak{T}$ = the family of all members of $\mathfrak{P}$ which have $\Pi_{\eta,\vartheta}$. Then*

(a) $\mathfrak{Q}$ is a subgroup of $\mathfrak{P}$,

(b) $u \in \mathfrak{P} \Rightarrow \eta[u] \sim \vartheta[u]$,

(c) the members $u, v \in \mathfrak{P}$ belong to the same right coset of $\mathfrak{Q}$ in $\mathfrak{P}$ if and only if $\eta[u] = \eta[v]$ and $\vartheta[u] = \vartheta[v]$,

(d) every right coset of $\mathfrak{Q}$ in $\mathfrak{P}$ contains exactly one member of $\mathfrak{T}$.

PROOF OF (a). Obvious.

PROOF OF (b). Let $x_0 \in \eta[u]$, then $x_0 \in \eta$ and $u(x_0) \in \vartheta$. Put $u^{n+1}(x_0) = uu^n(x_0)$ for $n \geqq 1$. If $u^n(x_0) \in \vartheta$ for every $n \geqq 1$, $u^n(x_0)$ would generate an infinite subset of πu, contradicting the fact that πu is finite. Hence

$$n_0 = (\mu z)\,[z \geqq 1 \,\&\, u^{z+1}(x_0) \notin \vartheta]$$

exists. Put

$$h(x_0) = u^{n_0}(x_0),$$

then $h(x_0) \in \vartheta[u]$. Thus $h(x)$ maps the finite set $\eta[u]$ into the finite set $\vartheta[u]$ and it is easily seen that h is one-to-one. Similarly one proves that $\vartheta[u]$ can be mapped one-to-one into $\eta[u]$. We conclude that $\eta[u] \sim \vartheta[u]$.

PROOF OF (c). Assume $\mathfrak{Q}u = \mathfrak{Q}v$, i.e., $uv^{-1} \in \mathfrak{Q}$ and $vu^{-1} \in \mathfrak{Q}$. We wish to prove $\vartheta[v] < \vartheta[u]$. Suppose $b \in \vartheta[v]$; put $a = v(b)$. Then $b \in \vartheta$, $a \in \eta$ and $b = v^{-1}(a)$. Hence

$$\left.\begin{array}{r} uv^{-1}(a) = u(b) \\ uv^{-1} \in \mathfrak{Q} \,\&\, a \in \eta \Rightarrow uv^{-1}(a) \in \eta \end{array}\right\} \Rightarrow u(b) \in \eta.$$

From $b \in \vartheta$ and $u(b) \in \eta$ we infer $b \in \vartheta[u]$. Thus $\vartheta[v] < \vartheta[u]$. Using $vu^{-1} \in \mathfrak{Q}$ we can similarly prove $\vartheta[u] < \vartheta[v]$. It follows that $\vartheta[u] = \vartheta[v]$. The relation $\eta[u] = \eta[v]$ can be established likewise. This concludes the proof of the conditional from the left to the right. We proceed to establish the conditional from the right to the left by proving its contrapositive. Suppose u and v do not belong to the same right coset of $\mathfrak{Q}$ in $\mathfrak{P}$, i.e., suppose $uv^{-1} \notin \mathfrak{Q}$. Then

$$(3.1) \qquad (\exists x)\left[(x \in \eta \,\&\, uv^{-1}(x) \in \vartheta) \;\boldsymbol{v}\; (x \in \vartheta \;\boldsymbol{v}\; uv^{-1}(x) \in \eta)\right].$$

Using the same reasoning as in the proof of (b) we see that if uv^{-1} maps an element of ϑ into η, it also maps an element of η into ϑ. Thus (3.1) implies that $uv^{-1}(x) \in \vartheta$ for some $x \in \eta$, say x_1; we now have $x_1 \in \eta$ and $uv^{-1}(x_1) \in \vartheta$. Putting $v^{-1}(x_1) = z$ we get

$$(3.2) \qquad v(z) \in \eta \,\&\, u(z) \in \vartheta.$$

Either $z \in \eta$ or $z \in \vartheta$; using (3.2) we see that in the former case $z \notin \eta[v]$ and $z \in \eta[u]$, whereas in the latter case $z \in \vartheta[v]$ and $z \notin \vartheta[u]$. Anyhow, either $\eta[u] \neq \eta[v]$ or $\vartheta[u] \neq \vartheta[v]$.

PROOF OF (d). Let $\mathfrak{Q}r$ be a right coset of $\mathfrak{Q}$ in $\mathfrak{P}$, then $\eta[r] \sim \vartheta[r]$ by (b). Let p be the permutation such that

(1) p maps $\eta[r]$ onto $\vartheta[r]$ and is strictly increasing on $\eta[r]$,
(2) p maps $\vartheta[r]$ onto $\eta[r]$ and is strictly increasing on $\vartheta[r]$,
(3) $p(x) = x$ for $x \notin \eta[r] + \vartheta[r]$.

Such a permutation p exists, because $\eta[r] \sim \vartheta[r]$; it belongs to $\mathfrak{Q}r$, since $\eta[p] = \eta[r]$ and $\vartheta[p] = \vartheta[r]$; finally, it has $\Pi_{\eta,\vartheta}$. There is clearly only one permutation satisfying the three conditions and every member of $\mathfrak{T}$ in $\mathfrak{Q}r$ must satisfy them. Thus $\mathfrak{Q}r$ contains exactly one member of $\mathfrak{T}$, namely p. This completes the proof of the lemma.

Let α and β be separable isolated sets, $\alpha \in A$, $\beta \in B$, $\alpha < \bar{\alpha}$, $\beta < \bar{\beta}$, where $\bar{\alpha}$ and $\bar{\beta}$ are r.e. and disjoint. Put $\gamma = \alpha + \beta$, $\bar{\gamma} = \bar{\alpha} + \bar{\beta}$,

$$\overline{\mathfrak{P}} = \mathfrak{P}_{\bar{\gamma}}, \quad \mathfrak{P} = \mathfrak{P}_{\gamma}, \quad \overline{\mathfrak{Q}} = \mathfrak{Q}_{\bar{\alpha},\bar{\beta}}, \quad \mathfrak{Q} = \mathfrak{Q}_{\alpha,\beta},$$
$$\overline{\mathfrak{T}} = \{p \mid p \in \overline{\mathfrak{P}} \,\&\, p \text{ has } \Pi_{\bar{\alpha},\bar{\beta}}\},$$
$$\mathfrak{T} = \{p \mid p \in \mathfrak{P} \,\&\, p \text{ has } \Pi_{\alpha,\beta}\},$$
$$\bar{\lambda} = \{n \mid p_n \in \overline{\mathfrak{Q}}\}, \quad \bar{\tau} = \{n \mid p_n \in \overline{\mathfrak{T}}\}.$$

Thus $\mathfrak{P}\subset\overline{\mathfrak{P}}$, $\mathfrak{Q}\subset\overline{\mathfrak{Q}}$, $\mathfrak{T}\subset\overline{\mathfrak{T}}$, $\overline{\mathfrak{P}}=\overline{\mathfrak{Q}}\,\overline{\mathfrak{T}}$, $\mathfrak{P}=\mathfrak{Q}\mathfrak{T}$. If we effectively generate the r.e. sets $\bar{\alpha}$ and $\bar{\beta}$ and simultaneously the sequence $p_0(x)$, $p_1(x)$, ... of all permutations, we can also effectively generate the sets $\bar{\lambda}$ and $\bar{\tau}$. We may assume without loss of generality that both $\bar{\alpha}$ and $\bar{\beta}$ are infinite (even if α or β is finite). Thus $\overline{\mathfrak{Q}}$ and $\overline{\mathfrak{T}}$ are infinite and there exist one-to-one recursive functions $\bar{q}(n)$ and $\bar{t}(n)$ such that $\bar{\lambda}=\varrho\bar{q}$, $\bar{q}(0)=0$, $\bar{\tau}=\varrho\bar{t}$, $\bar{t}(0)=0$. Put

$$u_i=p_{\bar{q}(i)},\qquad v_k=p_{\bar{t}(k)}.$$

The family $\overline{\mathfrak{P}}=\overline{\mathfrak{Q}}\,\overline{\mathfrak{T}}$ of permutations can now be tabulated as follows:

$\overline{\mathfrak{Q}}$	$\overline{\mathfrak{Q}}v_0$	$\overline{\mathfrak{Q}}v_1$	$\overline{\mathfrak{Q}}v_2$	...
u_0	u_0v_0	u_0v_1	u_0v_2	...
u_1	u_1v_0	u_1v_1	u_1v_2	...
u_2	u_2v_0	u_2v_1	u_2v_2	...
.	.	.	.	...
.	.	.	.	...

Since $\bar{q}(0)=\bar{t}(0)=0$ we have the identity permutation as the upper left hand entry in this table; $\overline{\mathfrak{Q}}$ itself is listed in the first column and $\overline{\mathfrak{T}}$ itself in the first row. The columns are the right cosets of $\overline{\mathfrak{Q}}$ in $\overline{\mathfrak{P}}$; each column contains exactly one element of $\overline{\mathfrak{T}}$ and that element occurs in the first row. We claim

$$u_iv_k\in\mathfrak{P}\Leftrightarrow u_i\in\mathfrak{Q}\ \&\ v_k\in\mathfrak{T}. \tag{3.3}$$

The conditional from the right to the left is obvious. Now assume $u_iv_k\in\mathfrak{P}$.

$$u_iv_k\in\overline{\mathfrak{Q}}v_k\Rightarrow\bar{\alpha}[u_iv_k]=\bar{\alpha}[v_k],$$
$$u_iv_k\in\mathfrak{P}\Rightarrow\bar{\alpha}[u_iv_k]<\alpha.$$

It follows that $\bar{\alpha}[v_k]<\alpha$; similarly one can prove $\bar{\beta}[v_k]<\beta$. Hence $v_k\in\mathfrak{P}$. Combining this with $u_iv_k\in\mathfrak{P}$ we obtain $u_i\in\mathfrak{P}$. We now see that $u_i\in\overline{\mathfrak{Q}}$ and $u_i\in\mathfrak{P}$ imply $u_i\in\mathfrak{Q}$, while $v_k\in\mathfrak{P}$ and $v_k\in\overline{\mathfrak{T}}$ imply $v_k\in\mathfrak{T}$. This completes the proof of (3.3). Putting

$$\lambda=\{n\,|\,p_n\in\mathfrak{Q}\},\qquad\tau=\{n\,|\,p_n\in\mathfrak{T}\},$$

we can rewrite (3.3) as follows:

$$\text{for } x\in\bar{\lambda},\ y\in\bar{\tau},\quad p_xp_y\in\mathfrak{P}\Leftrightarrow x\in\lambda\ \&\ y\in\tau. \tag{3.4}$$

There clearly exists a recursive function $f(n)$ such that $p_{f(n)}=p_{k(n)}p_{l(n)}$, where $k(n)$ and $l(n)$ are the functions such that $j(k(n),l(n))=n$. Let $g(n)$ be the restriction of $f(n)$ to the domain $j(\bar{\lambda}\times\bar{\tau})$. If n ranges over δg, the ordered pair $(k(n),l(n))$ ranges over $\bar{\lambda}\times\bar{\tau}$ and $p_{g(n)}$ over $\overline{\mathfrak{Q}}\,\overline{\mathfrak{T}}=\overline{\mathfrak{P}}$. The function $g(n)$ is partial recursive and one-to-one, since $\overline{\mathfrak{Q}}$ is a subgroup of $\overline{\mathfrak{P}}$ and $\overline{\mathfrak{Q}}\,\overline{\mathfrak{T}}=\overline{\mathfrak{P}}$. In view of (3.4) we have

$$g(n)\in\gamma!\Leftrightarrow k(n)\in\lambda\ \&\ l(n)\in\tau,$$
$$g(n)\in\gamma!\Leftrightarrow n\in j(\lambda\times\tau).$$

Thus $\gamma! \simeq j(\lambda \times \tau)$. Let $L = \text{Req}\,\lambda$ and $T = \text{Req}\,\tau$, then

$$(A+B)! = L \cdot T. \tag{3.5}$$

It follows from the definitions of $\overline{\mathfrak{Q}}$, $\mathfrak{Q}_{\bar{\alpha}}$ and $\mathfrak{Q}_{\bar{\beta}}$ that $\overline{\mathfrak{Q}} \cong \mathfrak{Q}_{\bar{\alpha}} \times \mathfrak{Q}_{\bar{\beta}}$. In fact, if p_x ranges over $\mathfrak{Q}_{\bar{\alpha}}$ and p_y ranges independently over $\mathfrak{Q}_{\bar{\beta}}$, then $p_x p_y$ ranges over $\overline{\mathfrak{Q}}$. Let $h(n)$ be the restriction of the function $f(n)$ to the domain $j(\bar{\alpha}! \times \bar{\beta}!)$. Then $h(n)$ is a partial recursive one-to-one function which maps $j(\bar{\alpha}! \times \bar{\beta}!)$ onto $\bar{\lambda}$ and $j(\alpha! \times \beta!)$ onto λ. Thus $\lambda \simeq j(\alpha! \times \beta!)$, i.e., $L = A!B!$. Combining this with (3.5) we get $A!B! \,|\, (A+B)!$.

REMARK. The isol T is uniquely determined by $(A+B)!$ and $A!B!$ in view of (2.1). The proof of T2 enables us to define a representative of T in terms of α and β. It is clear that the class Q of all finite sets can be effectively generated without repetitions in a sequence $\varrho_0, \varrho_1, \varrho_2, \ldots$ such that $\varrho_0 = o$, and given n both the elements and the cardinality of ϱ_n can be effectively found. In terms of a specific enumeration $\{\varrho_n\}$ of Q with these properties we define:

$$\overline{\Gamma} = \{(\varrho_x, \varrho_y) \,|\, \varrho_x \sim \varrho_y \,\&\, \varrho_x \subset \bar{\alpha} \,\&\, \varrho_y \subset \bar{\beta}\},$$
$$\Gamma = \{(\varrho_x, \varrho_y) \,|\, \varrho_x \sim \varrho_y \,\&\, \varrho_x \subset \alpha \,\&\, \varrho_y \subset \beta\}.$$

There clearly exists an effective one-to-one correspondence between $\overline{\Gamma}$ and $\overline{\mathfrak{T}}$ under which Γ corresponds to $\mathfrak{T}$. Put

$$\tau_{\alpha,\beta} = \{n \,|\, \varrho_{k(n)} \sim \varrho_{1(n)} \,\&\, \varrho_{k(n)} \subset \alpha \,\&\, \varrho_{1(n)} \subset \beta\}.$$

Then $\tau \simeq \tau_{\alpha,\beta}$, hence $\tau_{\alpha,\beta} \in T$.

4. COROLLARIES. In this section we shall discuss some properties of the factorial function in A which follow from its definition and the theorems T1 and T2. First of all we show that the proposition

$$1 \leqq k \leqq X \Rightarrow k! \,|\, X \cdot (X-1) \cdot \ldots \cdot (X-k+1)$$

mentioned in [*I*] [formula (2.15)] can now be proved in a few lines. Assume the hypothesis and put $A = X-k$, $B = k$. Then

$$(X-k)! \cdot k! \,|\, X!$$
$$X! = X \cdot (X-1) \cdot \ldots \cdot (X-k+1) \cdot (X-k)!$$

by T2 and T1 respectively. In view of (2.3) we conclude that $k!$ divides $X \cdot (X-1) \cdot \ldots \cdot (X-k+1)$.

P7. $X_1! \cdot \ldots \cdot X_n! \,|\, (X_1 + \cdots + X_n)!$.

PROOF. T2 and induction.

P8. $(X!)^m \,|\, (mX)!$.

PROOF. For $m = 0$ the relation reduces to 1 divides 1. For $m \geqq 1$ the relation follows from P7 by taking $n = m$, $X_1 = X_2 = \cdots = X_m = X$.

P9. $Y \leqq X \Rightarrow Y! \cdot (X-Y)! \,|\, X!$.

PROOF. Under the hypothesis we can express X as $Y+(X-Y)$

Note that P9 implies that $Y!\,|\,X!$ for $Y\leqq X$, i.e., (1.2).

DEFINITION. $C(X,Y)=\dfrac{X!}{Y!\,(X-Y)!}$ for $Y\leqq X$.

Since $Z!\geqq 1$ for all $Z\in A$ it follows from T2 and (2.1) that $C(X,Y)$ is uniquely determined for any two isols X and Y such that $Y\leqq X$. In case both X and Y are finite, $C(X,Y)$ is the ordinary binomial coefficient. The reader will easily verify

P10. $\begin{cases} C(X,0)=C(X,X)=1 \\ C(X,Y)=C(X,X-Y) \quad \text{for} \quad Y\leqq X. \end{cases}$

P11. $Y+1\leqq X\Rightarrow C(X+1,Y+1)=C(X,Y+1)+C(X,Y)$.

PROOF. Assume the hypothesis. Then all isols involved exist. The equality can now be proved as in the special case that X and Y are finite by using T1, (2.2) and (2.4) instead of the corresponding properties of ordinary numbers. Note that $Y<X$, hence $X-Y>0$. This permits us to multiply numerator and denominator of a fraction by $X-Y$. Since $(X+1)-(Y+1)=X-Y$ we have

$$C(X+1,Y+1)=\frac{(X+1)!}{(Y+1)!\,(X-Y)!}\,.$$

The desired equality now follows from

$$C(X,Y+1)+C(X,Y)=\frac{X!\,(X-Y)+X!\,(Y+1)}{(Y+1)!\,(X-Y)!}=\frac{(X+1)!}{(Y+1)!\,(X-Y)!}\,.$$

The next theorem involves 2^X and X^X. We shall therefore briefly discuss exponentiation in A. The function $f(x)$ from ε into ε is called *finite* if it is almost identical zero, i.e., if $\{x\,|\,f(x)\neq 0\}$ is finite. Thus every finite function is recursive. With every finite function $f(x)$ we associate the sets

$$\delta_e f=\{x\,|\,f(x)\neq 0\} \quad \text{and} \quad \varrho_e f=\{f(x)\,|\,f(x)\neq 0\}.$$

The finite function $f(x)$ is *given* if both the elements and the cardinality of $\delta_e f$ are given and also the image under f of each element in $\delta_e f$. The following proposition is proved in [2]. There exists a recursive function $r_n(x)$ of n and x such that

(a) for every n, $r_n(x)$ is a finite function,

(b) $r_0(x)=0$ for every x,

(c) for every finite function $f(x)$ there is exactly one number i such that $f(x)=r_i(x)$, and given $f(x)$, i can be effectively found.

From now on we assume that one such function $r_n(x)$ has been selected once and for all.

DEFINITIONS. $\alpha^\beta=\{n\,|\,\delta_e r_n\subset\beta \;\&\; \varrho_e r_n\subset\alpha\}$,

$$0^B=\begin{cases} 1 & \text{for} \quad B=0, \\ 0 & \text{for} \quad B\neq 0, \end{cases}$$

$$A^B=\operatorname{Req}\alpha^\beta, \quad \text{for} \quad A\neq 0, \quad 0\in\alpha\in A, \quad \beta\in B.$$

It can be shown that this definition of A^B is unique and that Λ is closed under this operation. The following properties of exponentiation are proved in [2]:

(4.1) $\quad A^B A^C = A^{B+C}; \quad (A^B)^C = A^{BC}; \quad (AB)^C = A^C B^C,$

(4.2) $\quad$ let $A, B, C \geqq 2$; $\quad$ then $\quad A < B \Rightarrow A^C < B^C \,\&\, C^A < C^B,$

(4.3) $\quad$ let $n \geqq 1$; $\quad$ then $X \in \Lambda - \varepsilon \Rightarrow X^n < 2^X.$

THEOREM T3. $X > 3 \Rightarrow 2^X < X! < X^X$.

PROOF. Since the assertion is obvious if X is finite, we restrict our attention to the case that X is infinite.

(1) For every number n one can effectively decide whether $\varrho r_n < (0, 1)$. Thus there exists a one-to-one recursive function $s(n)$ such that all finite functions which assume only values in (0, 1) are generated without repetitions in the sequence $r_{s(0)}(x), r_{s(1)}(x), \ldots$. We put $\varrho_n = \{x \mid r_{s(n)}(x) = 1\}$. The function $r_{s(n)}(x)$ is therefore the characteristic function of ϱ_n, and $\{\varrho_n\}$ is a sequence in which all finite sets are generated without repetitions such that given n both the elements and the cardinality of ϱ_n can be effectively found. We may assume without loss of generality that $s(0) = 0$; hence $\varrho_0 = o$. We define $2^\alpha = \{n \mid \varrho_n < \alpha\}$; thus $\alpha \in A$ implies $2^\alpha \in 2^A$. Let $\mathfrak{B}$ denote the family of all special functions (see Section 2) and $b_n(x)$ the partial recursive function mentioned in P2. We denote the class of all finite sets which are either empty or contain at least two elements by Q_1. We define a mapping Φ from Q_1 into $\mathfrak{B}$ as follows: $\Phi\langle o\rangle = b_0$; if $\alpha = (a_0, \ldots, a_n)$, where $a_0 < a_1 < \cdots < a_n$, $n \geqq 1$ then $\Phi\langle\alpha\rangle = f(x)$, where

$$\delta f = \alpha, \quad f(a_i) = a_{i+1} \quad \text{for} \quad 0 \leqq i \leqq n-1, \quad f(a_n) = a_0.$$

Let $d(x) = 2x$, $t(x) = 2x+1$, and $\tau = \varrho t$. Put

$$h(n) = \begin{cases} d(x) & \text{if} \quad \varrho_n \in Q_1 \quad \text{and} \quad \Phi\langle\varrho_n\rangle = b_x, \\ t(x) & \text{if} \quad \varrho_n = (x). \end{cases}$$

Let $\xi \in X$. We now claim:

(a) $h(n)$ is recursive and one-to-one,

(b) $h(2^\xi) < d(\xi!) + t(\xi)$,

(c) $h(2^\xi) \mid \big(d(\xi!) + t(\xi)\big) - h(2^\xi)$,

(d) $\big(d(\xi!) + t(\xi)\big) - h(2^\xi) \neq o$.

Re (a). Left to the reader.

Re (b). Put

$$\eta = \{x \mid (\exists n)\,[\varrho_n \in Q_1 \,\&\, b_x = \Phi\langle\varrho_n\rangle]\},$$

then η is a recursive set. Clearly,

$$\begin{aligned} x \in \xi &\Rightarrow (\exists n)\,[\varrho_n = (x) < \xi] \\ &\Rightarrow (\exists n)\,[n \in 2^\xi \,\&\, h(n) = t(x)] \\ &\Rightarrow t(x) \in h(2^\xi). \end{aligned}$$

Thus $t(\xi) < h(2^\xi)$ and by P3

$$h(2^\xi) = t(\xi) + \{d(x) \mid \delta b_x < \xi \,\&\, x \in \eta\} = t(\xi) + d(\xi! \cdot \eta)$$

which implies (b).

Re (c).

$$h(2^\xi) < \tau + d(\eta)$$
$$\big(d(\xi!) + t(\xi)\big) - h(2^\xi) < d(\xi!) - d(\xi! \cdot \eta) < d(\eta'),$$

where $\tau + d(\eta)$ and $d(\eta')$ are disjoint and recursive. This establishes (c).

Re (d). Let $a, b, c \in \xi$, $a < b < c$. There now exists a number x such that $b_x(c) = b$, $b_x(b) = a$, $b_x(a) = c$, hence

$$d(x) \in \big(d(\xi!) + t(\xi)\big) - h(2^\xi).$$

Combining (a), (b), (c), (d) with

$$2^\xi \in 2^X, \quad d(\xi!) \in X!, \quad d(\xi!) \mid t(\xi), \quad t(\xi) \in X$$

we conclude

(4.4) $$2^X < X! + X.$$

We now prove

(4.5) $$Y \in \Lambda - \varepsilon \Rightarrow 2^{Y+2} < (Y+2)!.$$

For under the hypothesis we have

$$2^{Y+2} = 4 \cdot 2^Y < 4(Y! + Y) \qquad \text{by (4.4)}$$
$$2^{Y+2} < (Y+2) \cdot Y! + (Y+2) \cdot Y! \cdot Y$$
$$2^{Y+2} < (Y+2) \cdot (Y+1) \cdot Y!$$
$$2^{Y+2} < (Y+2)!.$$

The desired result now follows from (4.5), since every $X \in \Lambda - \varepsilon$ can be written in the form $Y + 2$, where $Y \in \Lambda - \varepsilon$.

(2) Let again $\mathfrak{B}$ denote the family of all special functions. We write $\mathfrak{C}$ for the family of all finite functions. With every $f \in \mathfrak{B}$ we associate a function $g = \Psi\langle f \rangle$ as follows:

$$g(x) = \begin{cases} f(x) & \text{for} \quad x \in \delta f, \\ 0 & \text{for} \quad x \notin \delta f. \end{cases}$$

It is clear that Ψ maps $\mathfrak{B}$ into $\mathfrak{C}$. With every $g \in \mathfrak{C}$ we associate a set λg and a function $h = \Xi\langle g \rangle$ as follows:

$$\lambda g = \begin{cases} \varrho_e g & \text{if} \quad g(0) = 0, \\ \varrho_e g + (0) & \text{if} \quad g(0) \neq 0, \end{cases}$$

$$h(x) = \begin{cases} g(x) & \text{for} \quad x \in \lambda g, \\ \text{undefined for} & x \notin \lambda g. \end{cases}$$

We claim:

$$(4.6)\qquad \begin{cases} \text{If } g\in\mathfrak{C} \quad \text{and} \quad h=\Xi\langle g\rangle, \\ \quad g\in\Psi\langle\mathfrak{B}\rangle\Leftrightarrow g=\Psi\langle h\rangle \,\&\, h\in\mathfrak{B}. \end{cases}$$

For assume the hypothesis. The conditional from the right to the left is trivial. Now assume $g\in\Psi\langle\mathfrak{B}\rangle$, say $g=\Psi\langle f\rangle$, where $f\in\mathfrak{B}$. We wish to prove $f=h$. Since $f(x)=g(x)$ for $x\in\delta f$ and $f(x)$ is undefined for $x\notin\delta f$, it clearly suffices to prove $\delta f=\lambda g$. Using the fact that f is a special function we have

$$g(0)=0\Rightarrow 0\notin\delta f\Rightarrow 0\notin\varrho f\Rightarrow\varrho f=\varrho_e g$$
$$g(0)\neq 0\Rightarrow 0\in\delta f\Rightarrow 0\in\varrho f\Rightarrow\varrho f=\varrho_e g+(0).$$

This implies $\varrho f=\lambda g$, hence $\delta f=\lambda g$. This completes the proof of (4.6). Thus we see that (a) Ψ maps $\mathfrak{B}$ one-to-one into $\mathfrak{C}$, and (b) given g, we can effectively obtain $h=\Xi\langle g\rangle$ and check whether $g\in\Psi\langle\mathfrak{B}\rangle$ by testing whether h is a special function. Hence there is a one-to-one recursive function $d(n)$ with a recursive range such that $\Psi\langle b_n\rangle=r_{d(n)}$. Put $\delta=\varrho d_n$. Let $\xi\in X$; we may assume without loss of generality that $0\in\xi$. Denote the family of all special functions whose domain and range are included in ξ by $\mathfrak{B}_\xi$ and the family of all finite functions g such that $\delta_e g+\varrho_e g<\xi$ by $\mathfrak{C}_\xi$. Since

$$g=\Psi\langle f\rangle\Rightarrow\delta_e g<\delta f\,\&\,\varrho_e g<\varrho f,$$

we see that Ψ maps $\mathfrak{B}_\xi$ one-to-one into $\mathfrak{C}_\xi$. Let $\vartheta=d(\xi!)$, then $\vartheta\in X!$ by P3; moreover $\vartheta<\xi^\xi$. From

$$\vartheta<\delta,\qquad \xi^\xi-\vartheta<\delta',\qquad \delta \text{ recursive}$$

we conclude $\vartheta\,|\,\xi^\xi-\vartheta$. Put $Y=\mathrm{Req}(\xi^\xi-\vartheta)$, then $X!+Y=X^X$. It remains to be shown that $Y>0$. Let $\{t_n\}$ be an infinite sequence of distinct elements in $\xi-(0)$; let for $n\geqq 1$

$$\begin{cases} r_n^*(y_0)=r_n^*(y_n)=y_0, \\ r_n^*(x)=0 \quad \text{for} \quad x\notin(y_0,y_n). \end{cases}$$

Then $\{r_n^*\}$ is an infinite sequence of distinct functions in $\mathfrak{C}_\xi-\Psi\langle\mathfrak{B}_\xi\rangle$. Hence $\xi^\xi-\vartheta$ is an infinite set and the isol Y is not only greater than zero, but even infinite.

A r.e. set is called *simple* if its complement is immune. For the definition of a hypersimple set the reader is referred to [3, p. 497] or [4, p. 305]. Let S_0 denote the class of all hypersimple sets and S_1 the class of all simple sets. Post proved in [4] that S_0 is non-empty and properly included in S_1. Put

$$A_0=\{\mathrm{Req}\,\alpha\,|\,\alpha'\in S_0\vee\alpha\in Q\},$$
$$A_1=\{\mathrm{Req}\,\alpha\,|\,\alpha'\in S_1\vee\alpha\in Q\}.$$

It readily follows from the relations

$$(\alpha+\beta)'=\alpha'\cdot\beta'$$
$$(j(\alpha\times\beta))'=j(\varepsilon\times\beta')+j(\alpha'\times\varepsilon)$$
$$(\alpha^\beta)'=\{n\,|\,\delta_e r_n\cdot\beta'\neq o\vee\varrho_e r_n\cdot\alpha'\neq o\}$$

that Λ_1 is closed under addition, multiplication and exponentiation. It is shown in [2] that

(a) Λ_0 is closed under addition, multiplication and exponentiation,

(b) $B \leqq A \,\&\, A \in \Lambda_0 \Rightarrow B \in \Lambda_0$,

(c) $B \leqq A \,\&\, A \in \Lambda_1 \Rightarrow B \in \Lambda_1$.

Thus $[\Lambda_0, +, \cdot]$ is an extension of $[\varepsilon, +, \cdot]$ and $[\Lambda_1, +, \cdot]$ is an extension of $[\Lambda_0, +, \cdot]$. Both Λ_0 and Λ_1 are denumerable, because the classes S_0 and S_1 are denumerable.

Now suppose $X \in \Lambda_1$, then $X^X \in \Lambda_1$. Combining this with the fact that $X! < X^X$ for $X \in \Lambda_1 - \varepsilon$, it follows by (c) that $X! \in \Lambda_1$. Thus Λ_1 is closed under the factorial function. Similarly one can prove using (a), (b) and T3 that Λ_0 is closed under the factorial function.

P12. *There exists a collection of infinite isols in Λ_0 which when ordered by the $<$ relation has order type η*[2]).

PROOF. Let $Y = X!$, where $X \in \Lambda_0 - \varepsilon$. Then $q \mid Y$ for every positive number q and

$$\frac{pY}{q} < \frac{rY}{s} \Leftrightarrow \frac{p}{q} < \frac{r}{s}$$

for any four positive numbers p, q, r and s. Thus the collection

$$\Delta = \left\{ \frac{pY}{q} \;\middle|\; p \geqq 1 \,\&\, q \geqq 1 \right\}$$

satisfies the requirements.

References

[1] DEKKER, J. C. E.: Congruences in isols with a finite modulus. Math. Z. **70**, 113–124 (1958). — [2] DEKKER, J. C. E., and J. MYHILL: Recursive equivalence types, monograph, to be published in 1959 by the University of California Press. — [3] DEKKER, J. C. E.: Two notes on recursively enumerable sets. Proc. Amer. Math. Soc. **4**, 495–501 (1953). — [4] POST, E. L.: Recursively enumerable sets of positive integers and their decision problems. Bull. Amer. Math. Soc. **50**, 284–316 (1944).

Institute for Advanced Study Princeton, U.S.A.

(Eingegangen am 25. Januar 1958)

[2]) This proposition is due to J. MYHILL.

KASCH, F.
Math. Zeitschr. Bd. 70, S. 263–270 (1958)

Über eine metrische Eigenschaft der S-Zahlen

Von
FRIEDRICH KASCH

1. Fragestellung, Voraussetzungen

Eine Zahl ξ heißt bei der Mahlerschen Klasseneinteilung der transzendenten Zahlen[1]) eine S-Zahl, wenn es positive Zahlen $\varrho, c_1, c_2, c_3, \ldots$ so gibt, daß für jedes ganzzahlige Polynom $F(x) = \sum_i a_i x^i$ vom Grad $n \geqq 1$ und der Höhe $h = \max_i (|a_i|)$ die folgende Ungleichung gilt:

$$|F(\xi)| \geqq c_n h^{-\varrho n}. \tag{1}$$

Auf Grund des Schubfachschlusses ergibt sich bekanntlich, daß bei einer reellen bzw. komplexen S-Zahl ξ notwendig $\varrho \geqq 1$ bzw. $\varrho \geqq \frac{1}{2}$ sein muß.

In mehreren Arbeiten ist die Frage nach dem Maß der Menge der S-Zahlen in Abhängigkeit von ϱ untersucht worden. Hierzu besagt zunächst ein Ergebnis von A. J. CHINTSCHIN [*1*], daß das Maß der Menge der reellen S-Zahlen mit $\varrho = 1$ gleich Null ist. Andererseits zeigte K. MAHLER [*6*], daß fast alle reellen oder komplexen Zahlen S-Zahlen sind, und zwar bewies er dies für die reellen Zahlen mit $\varrho = 4$ und für die komplexen Zahlen mit $\varrho = \frac{7}{2}$. Richtungweisend für die weitere Entwicklung dieser Frage war die Vermutung von K. MAHLER [*6*], daß fast alle reellen Zahlen S-Zahlen mit $\varrho = 1 + \varepsilon$ und fast alle komplexen Zahlen S-Zahlen mit $\varrho = \frac{1}{2} + \varepsilon$ zu beliebig vorgegebenem $\varepsilon > 0$ seien.

Das Resultat von K. MAHLER wurde zunächst von J. F. KOKSMA [*3*] verbessert, der zeigte, daß man die Werte $\varrho = 4$ bzw. $\varrho = \frac{7}{2}$ durch 3 bzw. $\frac{5}{2}$ ersetzen kann. Schließlich konnte W. J. LEVEQUE [*5*] beweisen, daß es auch für die Werte 2 bzw. $\frac{3}{2}$ gültig ist[2]).

Wir bezeichnen mit $\mathfrak{M}_r(\varrho)$ die Menge der reellen S-Zahlen zu vorgegebenem ϱ in (1) und mit $\mathfrak{M}_k(\varrho)$ die entsprechende Menge der komplexen S-Zahlen. Sei ferner $\mathfrak{M}_r(\varrho, n)$ die Menge der reellen Zahlen ξ, die für feste Werte n und ϱ [und für geeignetes $c_n = c_n(\xi)$] der Ungleichung (1) genügen, und sei $\mathfrak{M}_k(\varrho, n)$ die entsprechende Menge komplexer Lösungen von (1). Dann gilt offenbar

$$\mathfrak{M}_r(\varrho) = \bigcap_{n=1}^{\infty} \mathfrak{M}_r(\varrho, n), \qquad \mathfrak{M}_k(\varrho) = \bigcap_{n=1}^{\infty} \mathfrak{M}_k(\varrho, n).$$

[1]) Siehe dazu z. B. [8], Kap. III.

[2]) Ein zweiter Beweis für dieses Resultat findet sich in [8], Kap. III.

Sei $\mu(\mathfrak{M})$ das Maß von $\mathfrak{M}$, dann ist aus maßtheoretischen Gründen $\mu(\mathfrak{M}_r(\varrho)) = 1$ äquivalent mit $\mu(\mathfrak{M}(\varrho_r, n)) = 1$ für $n = 1, 2, 3, \ldots$. Die Mahlersche Vermutung besagt dann

$$\mu(\mathfrak{M}_r(1+\varepsilon, n)) = 1 \tag{2}$$

bzw.

$$\mu(\mathfrak{M}_k(\tfrac{1}{2}+\varepsilon, n)) = 1 \tag{3}$$

für jedes $\varepsilon > 0$ und $n = 1, 2, 3, \ldots$.

Bei dieser Formulierung erhebt sich sofort die Frage, ob man (2) und (3) wenigstens für spezielle Werte von n beweisen könne. Für $n = 1$ ist die Gültigkeit von (2) wohlbekannt und für (3) läßt sie sich sofort verifizieren, sogar für den Wert 0 an Stelle $\frac{1}{2} + \varepsilon$. Von J. KUBILYUS [4] wurde (2) auch für $n = 2$ bewiesen. Er benutzte dabei wesentlich einen Hilfssatz von J. M. VINOGRADOV über trigonometrische Summen, also ein verhältnismäßig tiefliegendes Hilfsmittel. TH. SCHNEIDER schreibt in seinem Buch „Einführung in die transzendenten Zahlen"[3]) über das Resultat von J. KUBILYUS „Einen Anfang zum Beweis dieser (Mahlerschen) Vermutung hat vielleicht J. KUBILYUS gemacht ...".

Es dürfte daher von Interesse sein, für das Resultat von J. KUBILYUS einen ganz einfachen Beweis zu besitzen. Ein solcher Beweis wird im folgenden mitgeteilt. Wesentlich scheint mir dabei zu sein, daß sich dieser Beweis auch auf den komplexen Fall ausdehnen läßt*). Er liefert dort das Resultat: $\mu(\mathfrak{M}_k(\frac{1}{4}+\varepsilon, 2)) = 1$ für jedes $\varepsilon > 0$, also ein besseres Ergebnis, als es die Mahlersche Vermutung für beliebiges n besagt.

2. Hilfssätze

HILFSSATZ 1. *Sei $F(x) = a_0 + a_1 x + a_2 x^2$ ein Polynom mit ganzrationalen Koeffizienten und verschiedenen Nullstellen α_1, α_2. Mit $D = D(F)$ werde die Diskriminante von $F(x)$ bezeichnet. Dann gilt für jede komplexe Zahl ξ:*

$$\operatorname{Min}(|\xi - \alpha_1|, |\xi - \alpha_2|) \leq \frac{2}{\sqrt{|D(F)|}} |F(\xi)|.$$

BEWEIS. Sei etwa $\operatorname{Min}(|\xi - \alpha_1|, |\xi - \alpha_2|) = |\xi - \alpha_1|$, dann gilt

$$\sqrt{|D(F)|} = |a_2(\alpha_1 - \alpha_2)| \leq |a_2| (|\alpha_1 - \xi| + |\xi - \alpha_2|) \leq 2 |a_2(\xi - \alpha_2)|.$$

Daraus folgt

$$|\xi - \alpha_1| \leq \frac{2}{\sqrt{|D(F)|}} |a_2(\xi - \alpha_1)(\xi - \alpha_2)| = \frac{2}{\sqrt{|D(F)|}} |F(\xi)|.$$

HILFSSATZ 2. *Die folgende Summation erstrecke sich über alle Polynome $F(x)$ vom Grad 2, der festen Höhe h und mit verschiedenen Nullstellen. Dann gilt mit einer von h unabhängigen Konstanten γ_0:*

$$\sum \frac{1}{\sqrt{|D(F)|}} \leq \gamma_0 h. \tag{4}$$

[3]) [8], S. 83.

*) *Zusatz bei der Korr.:* Der Beweis läßt sich auch auf den p-adischen Fall übertragen und liefert auch dort das bestmögliche Resultat.

BEWEIS. Wegen $|D(F)| = |a_1^2 - 4a_0a_2|$ und da mindestens ein Koeffizient gleich $\pm h$ sein muß, gilt

$$(5) \qquad \sum \frac{1}{\sqrt{|D(F)|}} \leqq 2 \sum_{\substack{-h \leqq a_0 \leqq h \\ -h \leqq a_2 \leqq h}}{}' \frac{1}{|h^2 - 4a_0a_2|^{\frac{1}{2}}} + 4 \sum_{\substack{-h \leqq a_1 \leqq h \\ -h \leqq a \leqq h}}{}' \frac{1}{|a_1^2 - 4ha|^{\frac{1}{2}}};$$

die erste Summe besitzt den Faktor 2, da $a_1 = \pm h$ sein kann und die zweite den Faktor 4, da $a_0 = \pm h$ und $a_2 = \pm h$ sein können. Der Strich am Summenzeichen soll hier wie im folgenden $h^2 - 4a_0a_2 \neq 0$ bzw. $a_1^2 - 4ha \neq 0$ bedeuten. Betrachten wir jetzt die erste Summe auf der rechten Seite von (5) bei festem $a_0 \neq 0$. Der Ausdruck $|h^2 - 4a_0a_2|$ durchläuft für $-h \leqq a_2 \leqq h$ höchstens $2h+1$ von Null verschiedene Zahlen, von denen je zwei aufeinanderfolgende bis auf höchstens eine Ausnahme alle den Abstand $4|a_0|$ voneinander haben. Die eine Ausnahme kann auftreten, wenn der Ausdruck $h^2 - 4a_0a_2$ das Vorzeichen wechselt. Daher gilt

$$(6) \qquad \sum_{-h \leqq a_2 \leqq h}{}' \frac{1}{|h^2 - 4a_0a_2|^{\frac{1}{2}}} \leqq 2 \sum_{a=0}^{h} \frac{1}{(1 + 4|a_0||a)^{\frac{1}{2}}} \leqq 2 + \frac{1}{\sqrt{|a_0|}} \sum_{a=1}^{h} \frac{1}{\sqrt{a}} \leqq 4 \frac{\sqrt{h}}{\sqrt{|a_0|}}.$$

Damit folgt

$$(7) \qquad \sum_{\substack{-h \leqq a_2 \leqq h \\ -h \leqq a_0 \leqq h}}{}' \frac{1}{|h^2 - 4a_0a_2|^{\frac{1}{2}}} \leqq 4\sqrt{h} \sum_{\substack{-h \leqq a_0 \leqq h \\ a_0 \neq 0}} \frac{1}{\sqrt{|a_0|}} + \frac{2h+1}{h} \leqq 19h.$$

Aus (6) entnimmt man ferner für die zweite Summe in (5) bei festem a_1:

$$\sum_{-h \leqq a \leqq h}{}' \frac{1}{|a_1^2 - 4ha|^{\frac{1}{2}}} \leqq 4.$$

Daher erhält man

$$(8) \qquad \sum_{\substack{-h \leqq a \leqq h \\ -h \leqq a_1 \leqq h}}{}' \frac{1}{|a_1^2 - 4ha|^{\frac{1}{2}}} \leqq 4(2h+1) \leqq 12h.$$

Die Abschätzungen (5), (7) und (8) zusammen liefern die Behauptung (4).

Diese beiden Hilfssätze reichen aus, um das Resultat von J. KUBILYUS zu beweisen. Die nächsten Hilfssätze werden für den komplexen Fall gebraucht.

HILFSSATZ 3. *Sei $A(q, m)$ die Anzahl der mod q inkongruenten Lösungen von*

$$(9) \qquad x^2 \equiv m \pmod{q},$$

und sei r^2 der größte gemeinsame quadratische Teiler von q und m. Dann gilt mit einer von q und m unabhängigen Konstanten γ_2

$$A(q, m) \leqq \gamma_2 r q^{\frac{2}{\log \log q}}\ ^{4}).$$

---

4) Für $q = 1$ ist $q^{\frac{2}{\log \log q}}$ gleich 1 zu setzen; entsprechend im folgenden.

BEWEIS. Setzt man $m'=\frac{m}{r^2}$ und $q'=\frac{q}{r^2}$, dann erhält man aus jeder Lösung x von (9) eine Lösung $x'=\frac{x}{r}$ von

$$x'^2 \equiv m' \pmod{q'}. \tag{10}$$

Umgekehrt liefert jede Lösung x' von (10) eine Lösung $x=rx'$ von (9). Da aus $0\leqq x<q$ ferner $0\leqq x'<\frac{q}{r}=rq'$ folgt, hat man die Beziehung $A(q, m)=rA(q', m')$. Ist $q'=1$, also $q=r^2$, dann gilt $A(q, m)=r$ und die Behauptung ist erfüllt. Im folgenden kann daher $q'>1$ vorausgesetzt werden. Ist $q'=p_1^{e_1}\dots p_t^{e_t}$ die Primzahlpotenzzerlegung von q', dann gilt bekanntlich

$$A(q', m')=\prod_{i=1}^{t} A(p_i^{e_i}, m').$$

Ist $(p_i, m')=1$, dann hat man im Falle $p_i\neq 2$: $A(p_i^{e_i}, m')=2$ und im Falle $p_i=2$: $A(p_i^{e_i}, m')\leqq 4$. Sei nun $(p_i, m')\neq 1$, dann muß zunächst $(p_i^{e_i}, m')=p_i$ gelten, da kein quadratischer Faktor auftreten kann. Ist (10) überhaupt lösbar, dann folgt ferner $e_i=1$. Daraus ergibt sich aber $A(p_i^{e_i}, m')=A(p_i, m')=1$. Insgesamt folgt $A(q', m')\leqq 2^{t+1}$, wobei also t die Anzahl der verschiedenen Primteiler von q' ist. Sei $d(q')$ die Anzahl aller positiven Teiler von q', dann gilt $2^t\leqq d(q')$. Andererseits besteht die Abschätzung[5])

$$d(q')\leqq \gamma_1 q'^{\frac{2}{\log\log q'}},$$

mit einer von q' unabhängigen Konstanten γ_1. Daher erhält man schließlich

$$A(q, m)=rA(q', m')\leqq \gamma_1 r q'^{\frac{2}{\log\log q'}}\leqq \gamma_2 r q^{\frac{2}{\log\log q}},$$

wobei γ_2 von q und m unabhängig ist[6]).

HILFSSATZ 4[7]). *Voraussetzungen wie in Hilfssatz 2. Dann gilt mit von h unabhängigen Konstanten γ_3 und τ:*

$$\sum \frac{1}{|D(F)|}\leqq \gamma_3 h^{\frac{\tau}{\log\log h}}. \tag{11}$$

BEWEIS. Wir haben die Lösungszahl der diophantischen Gleichung

$$h^2-4a_0a_2=m$$

bzw.

$$\frac{h^2-m}{4}=a_0a_2$$

---

[5]) Siehe z.B. [7], S. 24, Satz 5.2.

[6]) Die Funktion $x^{\frac{2}{\log\log x}}$ ist für $x\geqq e^e$ monoton wachsend. Daher gilt die letzte Ungleichung für $q'\geqq e^e$. Für die endlich vielen Werte $1<q'<e^e$ kann die Ungleichung durch Vergrößerung der Konstanten erfüllt werden.

[7]) Auf dem hier eingeschlagenen Weg kann auch $\sum \frac{1}{\sqrt{|D(F)|}}\leqq \gamma h^{1+\frac{\tau}{\log\log h}}$ bewiesen werden, was an Stelle von Hilfssatz 2 ebenfalls zum Beweis der endgültigen Behauptung im reellen Fall ausreicht.

zu vorgegebenen ganzen Zahlen $h \geqq 1$ und m mit $-3h^2 \leqq m \leqq 5h^2$ in ganzen Zahlen a_0, a_2 zu betrachten. Sie ist nach unserer Bezeichnung gleich $4d\left(\frac{h^2-m}{4}\right)$, falls $\frac{h^2-m}{4}$ eine von 0 und ± 1 verschiedene ganze Zahl ist, d.h. falls $m \neq h^2$ bzw. $m \neq h^2 \pm 4$. Setzt man noch $\left|\frac{h^2-m}{4}\right| = M$, dann gilt zufolge der schon oben benutzten Abschätzung

$$d\left(\frac{h^2-m}{4}\right) = d(M) \leqq \gamma_1 M^{\frac{2}{\log\log M}} \leqq \gamma_2 h^{\frac{4}{\log\log h}}.$$

Daraus folgt

$$(12) \qquad \sum_{\substack{-h \leqq a_0 \leqq h \\ -h \leqq a_2 \leqq h}}{}' \frac{1}{|h^2 - 4a_0 a_2|} \leqq 8\gamma_2 h^{\frac{4}{\log\log h}} \sum_{\substack{m=1 \\ m \neq h^2, \\ m \neq h^2 \pm 4}}^{5h^2} \frac{1}{m} + \frac{6}{h} \leqq \gamma_4 h^{\frac{5}{\log\log h}},$$

wobei γ_4 wie auch die noch folgenden Konstanten $\gamma_5, \gamma_6, \ldots$ von h unabhängig sind.

Sodann haben wir die Lösungszahl der Gleichung

$$(13) \qquad a_1^2 - 4ha = m$$

unter entsprechenden Voraussetzungen wie oben zu bestimmen. Aus Hilfssatz 3 folgt: Die Anzahl der Lösungen von (13) mit $-h \leqq a_1 \leqq h$ ist kleiner oder gleich

$$A(4h, m) \leqq \gamma_5 r h^{\frac{2}{\log\log h}}.$$

Daraus folgt, wenn noch $r = r(m)$ gesetzt wird

$$(14) \qquad \sum_{\substack{-h \leqq a_1 \leqq h \\ -h \leqq a \leqq h}}{}' \frac{1}{|a_1^2 - 4ha|} \leqq 2\gamma_5 h^{\frac{2}{\log\log h}} \sum_{m=1}^{5h^2} \frac{r(m)}{m}.$$

Es bleibt noch die rechts stehende Summe abzuschätzen. Zu vorgegebenem $r(m) = k$ kommen darin höchstens die folgenden Glieder vor:

$$\sum_{i=1}^{5h^2} \frac{k}{ki} \leqq \gamma_6 \log(h+1).$$

Daraus folgt

$$\sum_{m=1}^{5h^2} \frac{r(m)}{m} \leqq d(4h)\,\gamma_6 \log(h+1) \leqq \gamma_7 h^{\frac{3}{\log\log h}}$$

und damit erhält man aus (14)

$$(15) \qquad \sum_{\substack{-h \leqq a_1 \leqq h \\ -h \leqq a \leqq h}}{}' \frac{1}{|a_1^2 - 4ha|} \leqq \gamma_8 h^{\frac{5}{\log\log h}}.$$

Die Abschätzungen (12) und (15) zusammen liefern die Behauptung (11).

3. Beweise

3.1. Wir behandeln zuerst den reellen Fall und zeigen:

Zu beliebig vorgegebenem $\varepsilon>0$ hat die Komplementärmenge von $\mathfrak{M}_r(1+\varepsilon, 2)$ das Maß Null.

Diese Komplementärmenge ist enthalten in der Menge $\mathfrak{N}$ der reellen Zahlen ξ, für die die Ungleichung

$$|F(\xi)| < h^{-2(1+\varepsilon)} \tag{16}$$

unendlich viele Lösungen in Polynomen $F(x)$ vom Grad 2 hat, und es genügt daher $\mu(\mathfrak{N})=0$ zu zeigen. Hat (16) unendlich viele Lösungen, so gibt es auch entweder unendlich viele Lösungen $F(x)$ mit verschiedenen Nullstellen oder unendlich viele Lösungen $F(x)$ mit gleichen Nullstellen. Die Menge der ξ, für die (16) unendlich viele Lösungen mit verschiedenen Nullstellen besitzt, nennen wir $\mathfrak{U}$, die Menge der ξ, für die (16) unendlich viele Lösungen mit gleichen Nullstellen besitzt, sei $\mathfrak{V}$. Dann gilt $\mathfrak{N}=\mathfrak{U}\cup\mathfrak{V}$.

BEHAUPTUNG. $\mu(\mathfrak{U})=0$.

Nach der Bezeichnung von Hilfssatz 1 sei $\operatorname{Min}(|\xi-\alpha_1|, |\xi-\alpha_2|)=|\xi-\alpha_1|$, dann folgt aus Hilfssatz 1 und (16):

$$|\xi-\alpha_1| < \frac{2}{\sqrt{|D|}} h^{-2(1+\varepsilon)}. \tag{17}$$

Bezeichnet man zu festem h mit $\mathfrak{U}_h$ die Menge der reellen Zahlen ξ, zu denen es ein $\alpha_1 \neq \alpha_2$ mit (17) gibt, so gilt wegen Hilfssatz 2

$$\mu(\mathfrak{U}_h) \leqq 8h^{-2(1+\varepsilon)} \sum \frac{1}{\sqrt{|D(F)|}} \leqq \gamma_9 h^{-(1+2\varepsilon)}. \tag{18}$$

Der Faktor 8 ergibt sich, weil jedes Polynom zwei Nullstellen hat und die Intervallänge aus (17) zweimal genommen werden muß. Für jedes natürliche r gilt offenbar

$$\mathfrak{U} \leqq \bigcup_{h=r}^{\infty} \mathfrak{U}_h.$$

Da die Reihe $\sum_{h=1}^{\infty} h^{-(1+2\varepsilon)}$ konvergiert, folgt $\mu(\mathfrak{U})=0$.

BEHAUPTUNG. $\mu(\mathfrak{V})=0$.

Es mögen jetzt unendlich viele Lösungen $F(x)$ von (16) mit $\alpha_1=\alpha_2$ existieren. Dann kann $F(x)$ in der Form $F(x)=a(bx-c)^2$ geschrieben werden und für die Höhen h von $F(x)$ und h_1 von $bx-c$ gilt $h \geqq h_1^2$. Daher folgt aus (16)

$$|b\xi - c| < h_1^{-2(1+\varepsilon)}. \tag{19}$$

Die Menge der reellen Zahlen ξ, die bei festem h_1 und (sonst) beliebigem b und c diese Gleichung lösen, sei $\mathfrak{V}_{h_1}$. Dann gilt offenbar

$$\mu(\mathfrak{V}_{h_1}) \leqq 4(2h_1+1)h_1^{-2(1+\varepsilon)} \leqq \gamma_{10} h_1^{-(1+2\varepsilon)}. \tag{20}$$

Besitzt (16) unendlich viele Lösungen $F(x)=a(bx-c)^2$, so besitzt auch (19) unendlich viele Lösungen $bx-c$. Wie im ersten Fall folgt jetzt $\mu(\mathfrak{V})=0$. Damit haben wir $\mu(\mathfrak{M}_r(1+\varepsilon, 2))=1$ für jedes $\varepsilon>0$ vollständig bewiesen.

3.2. Der Beweis für $\mu\left(\mathfrak{M}_k\left(\frac{1}{4}+\varepsilon, 2\right)\right)=1$ für jedes $\varepsilon>0$ wird analog geführt. $\mathfrak{U}$ und $\mathfrak{V}$ mögen die analoge Bedeutung wie im reellen Fall besitzen. An Stelle von (17) tritt jetzt

$$|\xi-\alpha_1|<\frac{2}{\sqrt{|D|}}h^{-2\left(\frac{1}{4}+\varepsilon\right)}.$$

Zufolge von Hilfssatz 4 erhält man daraus

$$\mu(\mathfrak{U}_h)\leqq 8\pi h^{-4\left(\frac{1}{4}+\varepsilon\right)}\sum\frac{1}{|D(F)|}\leqq\gamma_{11}h^{-(1+3\varepsilon)},$$

wobei jetzt an Stelle der Intervalle bei der Abschätzung von $\mu(\mathfrak{U}_h)$ in (18) Kreise mit dem Radius $\frac{2}{\sqrt{|D|}}h^{-2\left(\frac{1}{4}+\varepsilon\right)}$ getreten sind. Daraus folgt wieder $\mu(\mathfrak{U})=0$. Analog zu (19) gilt jetzt

$$|b\xi-c|<h_1^{-2\left(\frac{1}{4}+\varepsilon\right)}.$$

Diese Ungleichung hat aber bei nichtreellem $\xi=\xi_1+i\xi_2$ wegen $|b\xi-c|\geqq|b\xi_2|\geqq|\xi_2|$ nur endlich viele Lösungen in linearen Polynomen $bx-c$, woraus sofort $\mu(\mathfrak{V})=0$ folgt.

4. Schlußbemerkung

Es soll hier auf zwei Fragen aufmerksam gemacht werden, die sich im Anschluß an unsere Überlegungen stellen. Zunächst wird man fragen, ob sich die hier mitgeteilten Überlegungen auch auf den Fall $n>2$ ausdehnen lassen. Für Hilfssatz 1 ist das möglich, und man erhält das folgende Resultat, welches eine Verbesserung der entsprechenden Hilfssätze bei I. N. FELDMANN[8]) und TH. SCHNEIDER[9]) darstellt:

Sei $F(x)$ ein ganzzahliges Polynom von einem Grade $n\geqq 2$ ohne mehrfache Nullstellen $\alpha_1, \ldots, \alpha_n$. Dann gilt für jede Zahl ξ

$$\min_i\left(|\xi-\alpha_i|\right)\leqq\gamma\frac{h^{n-2}}{\sqrt{|D(F)|}}F|(\xi)|,$$

mit

$$\gamma=(n+1)^{n-2}2^{\frac{n(3n-5)}{2}}.$$

Die Möglichkeit, damit zu einer Verbesserung des im allgemeinen Falle bisher besten Resultates von W. J. LEVEQUE zu gelangen, hängt davon ab, die Summe $\sum\frac{1}{\sqrt{|D(F)|}}$ bzw. $\sum\frac{1}{|D(F)|}$ für festen Grad n und feste Höhe h nichttrivial abzuschätzen[10]).

Die zweite Frage, die sich hier erhebt, besteht darin, ob ein zu dem anfangs erwähnten Resultat von A. CHINTSCHIN [*1*] analoges Resultat auch im komplexen

[8]) [*2*], Lemma 5.

[9]) [*8*], S. 78, Hilfssatz 18.

[10]) *Zusatz bei der Korr.:* Siehe dazu die demnächst in den Math. Ann. erscheinende Arbeit von B. VOLKMANN und dem Verf.: Zur Mahlerschen Vermutung über S-Zahlen.

Falle gilt. In dieser Hinsicht ist

$$\mu\left(\mathfrak{M}_k\left(\frac{n-1}{2n}, n\right)\right) = 0, \qquad n = 2, 3, \ldots$$

zu vermuten.

Literatur

[1] CHINTSCHIN, A. J.: Zwei Bemerkungen zu einer Arbeit von Herrn PERRON. Math. Z. **22**, 274–284 (1925). — [2] FELDMANN, N. I.: Approximation einiger transzendenter Zahlen I (russ.). Izvestija Akad. Nauk SSSR., Ser. matm. **15**, 53–74 (1951). — [3] KOKSMA, J. F.: Über die Mahlersche Klasseneinteilung der transzendenten Zahlen und die Approximation komplexer Zahlen durch algebraische Zahlen. Monatshefte für Math. und Physik **48**, 176–189 (1939). — [4] KUBILYUS, J.: Über die Anwendung einer Vinogradowschen Methode auf die Lösung eines Problems aus der metrischen Zahlentheorie (russ.). Doklady Akad. Nauk SSSR. (N. S.) **67**, 783–786 (1949). — [5] LEVEQUE, W. J.: Note on S-Numbers. Proc. Amer. Math. Soc. **4**, 189–190 (1953). — [6] MAHLER, K.: Über das Maß der Menge aller S-Zahlen. Math. Ann. **106**, 131–139 (1932). — [7] PRACHAR, K.: Primzahlverteilung. Berlin: Springer 1957. — [8] SCHNEIDER, TH.: Einführung in die transzendenten Zahlen. Berlin: Springer 1957.

Heidelberg, Math. Institut der Universität

(Eingegangen am 13. Mai 1958)

FAN, K.
Math. Zeitschr. Bd. 70, S. 271–280 (1958)

On the Equilibrium Value of a System of Convex and Concave Functions

By
KY FAN

1. Let S denote the $(n-1)$-dimensional simplex formed by all those points $x=(x_1, x_2, \ldots, x_n)$ in the Euclidean n-space E^n whose coordinates satisfy $x_i \geqq 0$ $(1 \leqq i \leqq n)$ and $\sum_{i=1}^{n} x_i = 1$. For each index $i = 1, 2, \ldots, n$, let

$$S_i = \{(x_1, \ldots, x_n) \in S \mid x_i = 0\}.$$

We shall be concerned with a system $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ of $2n$ real-valued functions which are defined on S and satisfy the following conditions:

(a) *Each f_i is continuous and convex*[1]) *on S.*
(b) *Each g_i is continuous, concave and positive on S.*
(c) *$f_i(x) \leqq 0$ for $x \in S_i$.*
(d) *For each $x \in S$, there is an index i for which $f_i(x) > 0$.*

A real number λ will be called an *equilibrium value* of the system $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$, if there exists a point $x \in S$, called an *equilibrium point*, satisfying the n equations

$$g_i(x) = \lambda f_i(x) \qquad (1 \leqq i \leqq n). \tag{1}$$

The purpose of this note is to establish certain properties of the (necessarily unique) equilibrium value of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$. Our results may be regarded as a non-linear generalization of certain known theorems concerning the maximal eigenvalue of a matrix with positive elements.

2. Throughout this section, the system of functions $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ are assumed to satisfy the conditions (a), (b), (c), (d) previously stated. Besides the notation S, S_i $(1 \leqq i \leqq n)$ already explained, we shall also use the notation $\overset{\circ}{S} = \{(x_1, \ldots, x_n) \in S \mid x_i > 0 \text{ for } 1 \leqq i \leqq n\}$.

LEMMA 1. *For any two distinct points x, y of S given in this order, there is an index i for which either $\frac{f_i(x)}{g_i(x)} < \frac{f_i(y)}{g_i(y)}$, or both $f_i(x)$, $f_i(y)$ are $\leqq 0$.*

Proof. If $x \in S_i$ for some i, then $f_i(x) \leqq 0$ by (c). For this index i, either $\frac{f_i(x)}{g_i(x)} < \frac{f_i(y)}{g_i(y)}$, or both $f_i(x)$, $f_i(y)$ are $\leqq 0$, according to whether $f_i(y) > 0$ or $f_i(y) \leqq 0$.

[1]) As usual, a real-valued function f defined on S is said to be *convex*, if $f(\alpha x + \beta y) \leqq \alpha f(x) + \beta f(y)$ holds for any two points x, y of S and for any $\alpha \geqq 0$, $\beta \geqq 0$ with $\alpha + \beta = 1$. f is said to be *concave* if $-f$ is convex.

Next assume $x \in \overset{\circ}{S}$. We can find a point z such that $x = \alpha y + \beta z$ with $\alpha > 0$, $\beta > 0$, $\alpha + \beta = 1$ and $z \in S_i$ for some i. Consider now this index i. By (a), (c), we have $f_i(x) \leqq \alpha f_i(y) + \beta f_i(z) \leqq \alpha f_i(y)$. If $f_i(y) > 0$, then by (b), $\frac{f_i(x)}{g_i(x)} \leqq \frac{\alpha f_i(y)}{\alpha g_i(y) + \beta g_i(z)} < \frac{f_i(y)}{g_i(y)}$. If $f_i(y) \leqq 0$, then both $f_i(x)$, $f_i(y)$ are $\leqq 0$.

THEOREM 1. *The system* $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ *has a unique equilibrium value* λ *and a unique equilibrium point* $\hat{x}$. *We have*

$$\lambda > 0, \quad \hat{x} \in \overset{\circ}{S}, \tag{2}$$

and

$$\frac{1}{\lambda} = \operatorname*{Min}_{x \in S} \operatorname*{Max}_{1 \leqq i \leqq n} \frac{f_i(x)}{g_i(x)} = \operatorname*{Max}_{x \in S} \operatorname*{Min}_{1 \leqq i \leqq n} \frac{f_i(x)}{g_i(x)}. \tag{3}$$

Proof. Let

$$F_i = \left\{ x \in S \mid \frac{f_i(x)}{g_i(x)} = \operatorname*{Max}_{1 \leqq j \leqq n} \frac{f_j(x)}{g_j(x)} \right\}, \qquad (1 \leqq i \leqq n).$$

Then F_i are closed sets and $\bigcup_{i=1}^{n} F_i = S$. By (c), we have $\frac{f_i(x)}{g_i(x)} \leqq 0$ for $x \in S_i$. But by (d), $\operatorname*{Max}_{1 \leqq j \leqq n} \frac{f_j(x)}{g_j(x)} > 0$ for every $x \in S$. Hence $F_i \cap S_i = \emptyset$, where $\emptyset$ denotes the empty set. According to a classical result of SPERNER [*10*], the n closed sets F_i covering the $(n-1)$-dimensional simplex S and satisfying $F_i \cap S_i = \emptyset$ $(1 \leqq i \leqq n)$ must have a point in common. Let $\hat{x} \in \bigcap_{i=1}^{n} F_i$. Then

$$\frac{f_1(\hat{x})}{g_1(\hat{x})} = \frac{f_2(\hat{x})}{g_2(\hat{x})} = \cdots = \frac{f_n(\hat{x})}{g_n(\hat{x})}.$$

By (d), this common value is positive. If λ denotes the reciprocal of this common value, then $\hat{x}$ satisfies the n equations (1). Hence λ is an equilibrium value and $\hat{x}$ is an equilibrium point.

Since $\bigcap_{i=1}^{n} F_i$ is the set of all equilibrium points, and since $F_i \cap S_i = \emptyset$ $(1 \leqq i \leqq n)$, every equilibrium point is necessarily in $\overset{\circ}{S}$. Also by (d) and positiveness of g_i, every equilibrium value is necessarily positive.

Consider now an arbitrary equilibrium value λ and a corresponding equilibrium point $\hat{x}$. From Lemma 1 and $\frac{f_i(\hat{x})}{g_i(\hat{x})} = \frac{1}{\lambda} > 0$ $(1 \leqq i \leqq n)$, we infer that

$$\operatorname*{Min}_{1 \leqq i \leqq n} \frac{f_i(x)}{g_i(x)} < \frac{1}{\lambda} < \operatorname*{Max}_{1 \leqq i \leqq n} \frac{f_i(x)}{g_i(x)} \quad \text{for } x \in S,\ x \neq \hat{x}. \tag{4}$$

This implies (3) and therefore the uniqueness of the equilibrium value. At the same time, the uniqueness of the equilibrium value and (4) imply the uniqueness of the equilibrium point.

COROLLARY 1. *Let* λ *be the equilibrium value and* $\hat{x}$ *the equilibrium point of* $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$. *Then* $x = \hat{x}$ *is the only solution* $x \in S$ *of the system of inequalities*

$$g_i(x) \leqq \lambda f_i(x) \qquad (1 \leqq i \leqq n). \tag{5}$$

Also $x=\hat{x}$ is the only solution $x\in S$ of the system of inequalities

$$g_i(x)\geqq\lambda f_i(x) \qquad (1\leqq i\leqq n). \tag{6}$$

Proof. This follows from (4).

Besides the systems of inequalities (5), (6), we may consider the following systems of inequalities:

$$g_i(x)<\varrho f_i(x), \qquad (1\leqq i\leqq n); \tag{7}$$

$$g_i(x)\leqq\varrho f_i(x), \qquad (1\leqq i\leqq n); \tag{8}$$

$$g_i(x)>\varrho f_i(x), \qquad (1\leqq i\leqq n); \tag{9}$$

$$g_i(x)\geqq\varrho f_i(x), \qquad (1\leqq i\leqq n); \tag{10}$$

where ϱ is a real number[2]). By positiveness of g_i and conditions (c) and (d), it is clear that if system (7) [or (8)] has a solution $x\in S$, then ϱ is necessarily positive, and x is necessarily in $\overset{\circ}{S}$. Relation (3) of Theorem 1 can be restated in the following form.

COROLLARY 2. *Let λ be the equilibrium value of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$, and let ϱ be a real number. Then $\varrho>\lambda$ ($\varrho\geqq\lambda$, $\varrho<\lambda$, $\varrho\leqq\lambda$), if and only if there exists a point $x\in S$ satisfying* (7), [(8), (9), (10) *respectively*].

COROLLARY 3. *Let $v_1=(1, 0, \ldots, 0, 0)$, $v_2=(0, 1, \ldots, 0, 0)$, $\ldots$, $v_n=(0, 0, \ldots, 0, 1)$ be the vertices of the simplex S. Then the equilibrium value λ of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ satisfies the inequalities*

$$\frac{1}{\lambda}<\frac{f_i(v_i)}{g_i(v_i)} \qquad (1\leqq i\leqq n). \tag{11}$$

Proof. Let $(\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n)$ be the coordinates of the equilibrium point $\hat{x}$. As $\hat{x}\in\overset{\circ}{S}$, we have $\hat{x}_i>0$ $(1\leqq i\leqq n)$. By (c), (d), $f_i(v_i)\leqq 0$ for $i\neq j$; and $f_i(v_i)>0$. Therefore

$$f_i\left(\sum_{j=1}^{n}\hat{x}_j v_j\right)\leqq\sum_{j=1}^{n}\hat{x}_j f_i(v_j)\leqq\hat{x}_i f_i(v_i)$$

and

$$\frac{1}{\lambda}=\frac{f_i\left(\sum_{j=1}^{n}\hat{x}_j v_j\right)}{g_i\left(\sum_{j=1}^{n}\hat{x}_j v_j\right)}\leqq\frac{\hat{x}_i f_i(v_i)}{\sum_{j=1}^{n}\hat{x}_j g_i(v_j)}<\frac{f_i(v_i)}{g_i(v_i)}.$$

THEOREM 2. *If λ is the equilibrium value of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$, then*

$$\frac{1}{\lambda}=\operatorname*{Max}_{\alpha_i>0}\operatorname*{Min}_{x\in S}\frac{\sum_{i=1}^{n}\alpha_i f_i(x)}{\sum_{i=1}^{n}\alpha_i g_i(x)}. \tag{12}$$

[2]) For $\varrho>0$, the functions ϱf_i-g_i are convex. Hence, when $\varrho>0$, system (9) is of the type of inequalities discussed in [4], and (10) is of the type of inequalities studied in [2].

Proof. Let $\hat{x}$ be the equilibrium point of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$. For any n positive numbers α_i, we have

$$\operatorname*{Min}_{x\in S}\frac{\sum_{i=1}^{n}\alpha_i f_i(x)}{\sum_{i=1}^{n}\alpha_i g_i(x)} \leqq \frac{\sum_{i=1}^{n}\alpha_i f_i(\hat{x})}{\sum_{i=1}^{n}\alpha_i g_i(\hat{x})} = \frac{1}{\lambda}.$$

In order to prove (12), it suffices to find n positive numbers α_i for which

$$\operatorname*{Min}_{x\in S}\frac{\sum_{i=1}^{n}\alpha_i f_i(x)}{\sum_{i=1}^{n}\alpha_i g_i(x)} \geqq \frac{1}{\lambda}. \tag{13}$$

We use the same argument as in [4; p. 620]. For each $x\in S$, let $C(x) = \{u=(u_1, \ldots, u_n)\in E^n \mid u_i > \lambda f_i(x) - g_i(x) \text{ for } 1\leqq i\leqq n\}$. Let $C = \bigcup_{x\in S} C(x)$. Then C is open in E^n. If $x, y\in S$, $u\in C(x)$, $v\in C(y)$, and if $\alpha\geqq 0$, $\beta\geqq 0$, $\alpha+\beta=1$, then as the functions $\lambda f_i - g_i$ are convex, we have $\alpha u+\beta v\in C(\alpha x+\beta y)\subset C$. This shows that C is a convex set. By Corollary 2, no point $x\in S$ can satisfy all n inequalities $g_i(x)>\lambda f_i(x)$ $(1\leqq i\leqq n)$. So the origin $0=(0, 0, \ldots, 0, 0)$ is not contained in the open convex set C. Therefore there exists a hyperplane H in E^n passing through 0 such that C lies strictly on one side of H. In other words, there are n real numbers α_i such that $\sum_{i=1}^{n}\alpha_i u_i>0$ for all $(u_1, \ldots, u_n)\in C$. Then, for any $x\in S$ and for any arbitrary $\varepsilon_i>0$ $(1\leqq i\leqq n)$, we have

$$\sum_{i=1}^{n}\alpha_i[\lambda f_i(x) - g_i(x) + \varepsilon_i] > 0. \tag{14}$$

In particular, by taking $x=\hat{x}$, this implies that $\sum_{i=1}^{n}\alpha_i\varepsilon_i>0$ holds for arbitrary $\varepsilon_i>0$. Hence $\alpha_i\geqq 0$. If we take $x=v_n=(0, 0, \ldots, 0, 1)$ and $\varepsilon_i=g_i(v_n)$, then (14) becomes $\sum_{i=1}^{n}\alpha_i f_i(v_n)>0$. Since $\alpha_i f_i(v_n)\leqq 0$ for $1\leqq i\leqq n-1$, and $f_n(v_n)>0$, it follows that $\alpha_n>0$. Similarly one sees that each $\alpha_i>0$. From (14), it is clear that these positive numbers α_i have the desired property (13).

COROLLARY 4. *A positive number ϱ is greater than the equilibrium value λ of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$, if and only if there exist n positive numbers α_i such that*

$$\sum_{i=1}^{n}\alpha_i[\varrho f_i(x) - g_i(x)] > 0 \qquad \textit{for all } x\in S. \tag{15}$$

THEOREM 3. *Let $\gamma_i\geqq 0$ $(1\leqq i\leqq n)$, $\sum_{i=1}^{n}\gamma_i=1$. Let λ be the equilibrium value of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$. Then a real number ϱ is greater than λ, if and only if there exist a point x* (necessarily in $\mathring{S}$) *and $\beta>0$ such that*

$$\varrho f_i(x) - g_i(x) = \beta\gamma_i \qquad (1\leqq i\leqq n). \tag{16}$$

Proof. Assume $\varrho > \lambda$. By Corollary 4, there exist $\alpha_i > 0$ $(1 \leqq i \leqq n)$ satisfying (15). We may require $\sum_{i=1}^{n} \alpha_i \gamma_i = 1$. Define n functions h_i on S by

$$h_i(x) = \frac{\alpha_i [\varrho f_i(x) - g_i(x)]}{\sum_{j=1}^{n} \alpha_j [\varrho f_j(x) - g_j(x)]}, \qquad (x \in S,\ 1 \leqq i \leqq n).$$

Then h_i are continuous on S and $\sum_{i=1}^{n} h_i(x) = 1$ for all $x \in S$. Let

$$F_i = \{x \in S \mid h_i(x) \geqq \alpha_i \gamma_i\} \qquad (1 \leqq i \leqq n).$$

As $\sum_{i=1}^{n} h_i(x) = \sum_{i=1}^{n} \alpha_i \gamma_i$ for all $x \in S$, we have $\bigcup_{i=1}^{n} F_i = S$. If $x \in S_i$, then $f_i(x) \leqq 0$ and $h_i(x) < 0 \leqq \alpha_i \gamma_i$. Hence $F_i \cap S_i = \emptyset$ $(1 \leqq i \leqq n)$. Then by SPERNER's covering theorem (already used in the proof of Theorem 1), the n closed sets F_i must have a point in common. For any $x \in \bigcap_{i=1}^{n} F_i$, we have $h_i(x) = \alpha_i \gamma_i$, or

$$\varrho f_i(x) - g_i(x) = \beta \gamma_i \quad \text{with} \quad \beta = \sum_{j=1}^{n} \alpha_j [\varrho f_j(x) - g_j(x)] > 0.$$

Conversely, if, for some real ϱ, there exist $x \in S$ and $\beta > 0$ satisfying (16), then since (16) implies $\varrho f_i(x) \geqq g_i(x)$ $(1 \leqq i \leqq n)$, we have necessarily $\varrho \geqq \lambda$ (Corollary 2) and $x \in \overset{\circ}{S}$ [by condition (c)]. Suppose $\varrho = \lambda$. Then by Corollary 1, x would coincide with the equilibrium point $\hat{x}$ of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$, and (16) would become $\lambda f_i(\hat{x}) - g_i(\hat{x}) = \beta \gamma_i$ $(1 \leqq i \leqq n)$. But this is absurd, since $\beta \gamma_i > 0$ for at least one i. Hence $\varrho > \lambda$.

In Theorem 3, when one of the γ_i's is 1 and all the others are 0, then for any given $\varrho > \lambda$, x and β are uniquely determined by (16). This can be easily seen by using Lemma 1.

3. Let $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ be a system of $2n$ functions defined on the $(n-1)$-dimensional simplex S and satisfying the conditions (a), (b), (c), (d). For any fixed index k between 1 and n, we shall consider the system $\{f_1^{(k)}, \ldots, f_{k-1}^{(k)}, f_{k+1}^{(k)}, \ldots, f_n^{(k)}; g_1^{(k)}, \ldots, g_{k-1}^{(k)}, g_{k+1}^{(k)}, \ldots, g_n^{(k)}\}$ of $2(n-1)$ functions defined on $S_k = \{(x_1, \ldots, x_n) \in S \mid x_k = 0\}$ by

$$f_i^{(k)}(x) = f_i(x) \qquad \text{for } x \in S_k \text{ and } i \neq k,$$

$$g_i^{(k)}(x) = g_i(x) \qquad \text{for } x \in S_k \text{ and } i \neq k.$$

It is clear that this system $\{f_1^{(k)}, \ldots, f_{k-1}^{(k)}, f_{k+1}^{(k)}, \ldots, f_n^{(k)}; g_1^{(k)}, \ldots, g_{k-1}^{(k)}, g_{k+1}^{(k)}, \ldots, g_n^{(k)}\}$ of $2(n-1)$ functions on S_k satisfies the conditions (a), (b), (c), (d). In the following theorem, the role played by the index n can, of course, be played by any index k between 1 and n.

THEOREM 4. *Let λ be the equilibrium value of the system $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ on S, and let λ_n be the equilibrium value of the system $\{f_1^{(n)}, f_2^{(n)}, \ldots, f_{n-1}^{(n)}; g_1^{(n)}, g_2^{(n)}, \ldots, g_{n-1}^{(n)}\}$ on S_n. Then*

(i) $\lambda > \lambda_n$.

(ii) *A positive number ϱ is greater than λ_n, if and only if there exists a point $x \in \overset{\circ}{S}$ satisfying the $n-1$ equations*

$$\varrho f_i(x) - g_i(x) = 0 \qquad (1 \leqq i \leqq n-1). \tag{17}$$

(iii) *A positive number ϱ satisfies the inequalities $\lambda > \varrho > \lambda_n$, if and only if there exists a point $x \in \overset{\circ}{S}$ satisfying (17) and*

$$\varrho f_n(x) - g_n(x) < 0. \tag{18}$$

Proof. (i) Let $\hat{y} \in S_n$ be the equilibrium point of $\{f_1^{(n)}, f_2^{(n)}, \ldots, f_{n-1}^{(n)}; g_1^{(n)}, g_2^{(n)}, \ldots, g_{n-1}^{(n)}\}$, i.e.

$$g_i(\hat{y}) = \lambda_n f_i(\hat{y}) \qquad (1 \leqq i \leqq n-1). \tag{19}$$

Since $f_n(\hat{y}) \leqq 0$ and $\lambda_n > 0$, we have

$$g_n(\hat{y}) > \lambda_n f_n(\hat{y}). \tag{20}$$

Then by Corollary 2, $\lambda_n \leqq \lambda$. As $\hat{y} \notin \overset{\circ}{S}$, $\hat{y}$ is distinct from the equilibrium point $\hat{x}$ of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$. Therefore, by Corollary 1, (19), (20) imply that $\lambda_n \neq \lambda$. Hence $\lambda > \lambda_n$.

(ii) Assume $\varrho > \lambda_n$. Let

$$F_i = \{x \in S \mid \varrho f_i(x) - g_i(x) \geqq 0\} \qquad (1 \leqq i \leqq n-1),$$
$$F_n = \{x \in S \mid \varrho f_i(x) - g_i(x) \leqq 0 \quad \text{for } 1 \leqq i \leqq n-1\}.$$

For $i = 1, 2, \ldots, n-1$, it is clear that $F_i \cap S_i = \emptyset$. As $\varrho > \lambda_n$, we have also $F_n \cap S_n = \emptyset$ (see Corollary 2). Since each F_i is closed and $\bigcup_{i=1}^{n} F_i = S$, SPERNER's covering theorem yields $\bigcap_{i=1}^{n} F_i \neq \emptyset$. Any point $x \in \bigcap_{i=1}^{n} F_i$ is in $\overset{\circ}{S}$ and satisfies (17).

To prove the converse, assume that (17) is satisfied by some $\varrho > 0$ and some $x \in \overset{\circ}{S}$. Let $x = (x_1, x_2, \ldots, x_n)$, $y = \left(\frac{x_1}{1-x_n}, \ldots, \frac{x_{n-1}}{1-x_n}, 0\right)$ and $z = (0, 0, \ldots, 0, 1)$. Then $x = (1-x_n)y + x_n z$. From (17), we have $\varrho f_i(x) = g_i(x) > 0$ $(1 \leqq i \leqq n-1)$. As $\varrho > 0$, it follows that $f_i(x) > 0$ $(1 \leqq i \leqq n-1)$. Since $f_i(z) \leqq 0$ $(1 \leqq i \leqq n-1)$ and $0 < x_n < 1$, we have for $i = 1, 2, \ldots, n-1$:

$$\frac{1}{\varrho} = \frac{f_i(x)}{g_i(x)} \leqq \frac{(1-x_n) f_i(y) + x_n f_i(z)}{(1-x_n) g_i(y) + x_n g_i(z)} < \frac{f_i(y)}{g_i(y)},$$

or

$$\varrho f_i(y) > g_i(y) \qquad (1 \leq i \leq n-1).$$

Since $y \in S_n$, this implies $\varrho > \lambda_n$ by Corollary 2.

(iii) Let $\lambda > \varrho > \lambda_n$. By (ii), there is a point $x \in \overset{\circ}{S}$ satisfying (17). By Corollary 2, (17) together with $\varrho < \lambda$ imply (18).

Conversely, if there exists a point $x \in \mathring{S}$ satisfying (17) and (18), then by (ii), $\varrho > \lambda_n$. According to Corollary 2, we have $\varrho \leqq \lambda$. Suppose $\varrho = \lambda$. Then by Corollary 1, x would be the equilibrium point of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$, against (18). Hence $\varrho < \lambda$.

COROLLARY 5. *Let λ_n be the equilibrium value of $\{f_1^{(n)}, f_2^{(n)}, \ldots, f_{n-1}^{(n)}; g_1^{(n)}, g_2^{(n)}, \ldots, g_{n-1}^{(n)}\}$. Then a positive number ϱ is $> \lambda_n$, if and only if there is a point $x \in \mathring{S}$ satisfying*

$$\varrho f_i(x) - g_i(x) \geqq 0 \qquad (1 \leqq i \leqq n-1). \tag{21}$$

Proof. In the proof of part (ii) of Theorem 4, (17) can be replaced by (21).

COROLLARY 6. *Let λ, λ_n be the equilibrium values of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ and $\{f_1^{(n)}, f_2^{(n)}, \ldots, f_{n-1}^{(n)}; g_1^{(n)}, g_2^{(n)}, \ldots, g_{n-1}^{(n)}\}$ respectively. If $\varrho > \lambda_n$ and $\varrho \neq \lambda$, then for any n real numbers γ_i, not all zero, there is a point $x \in S$ such that*

$$\sum_{i=1}^{n} \gamma_i [\varrho f_i(x) - g_i(x)] \neq 0. \tag{22}$$

Proof. If $\gamma_n \neq 0$, the point $x \in \mathring{S}$ satisfying (17) [see part (ii) of Theorem 4] will satisfy (22). If $\gamma_n = 0$, then there is an index k between 1 and $n-1$ such that $\gamma_k \neq 0$. Since $\varrho > \lambda_n$, by applying Theorem 3 to the system $\{f_1^{(n)}, f_2^{(n)}, \ldots, f_{n-1}^{(n)}; g_1^{(n)}, g_2^{(n)}, \ldots, g_{n-1}^{(n)}\}$ on S_n, there exists a point $x \in S_n$ such that

$$\varrho f_i(x) - g_i(x) \begin{cases} = 0 & \text{for } 1 \leqq i \leqq n-1 \text{ and } i \neq k \\ > 0 & \text{for } i = k. \end{cases}$$

Then this point x will satisfy (22).

We add two remarks in connection with Theorem 4. If f_n is positive throughout $\mathring{S}$, then for any $\varrho > \lambda_n$, the point $x \in \mathring{S}$ satisfying (17) is unique. This can be easily seen by using Lemma 1.

If each f_i remains non-negative on S, then in parts (ii), (iii) of Theorem 4, the words "a positive number ϱ" can be replaced by "a real number ϱ". Indeed, as f_i are non-negative on S, (17) can be satisfied by some x only when $\varrho > 0$.

4. In this section, we shall apply the above results to matrices with positive elements. Let $A = (a_{ij})$ be a square matrix of order n with positive elements. Define f_i, g_i $(1 \leqq i \leqq n)$ on S by

$$f_i(x) = x_i, \qquad g_i(x) = \sum_{j=1}^{n} a_{ij} x_j \tag{23}$$

for $x = (x_1, \ldots, x_n) \in S$. Then clearly conditions (a), (b), (c), (d) are satisfied.

In this case, the first part of Theorem 1 becomes a classical theorem of PERRON, namely: A has a positive eigenvalue λ and a corresponding eigenvector $\hat{x}$ with positive components; λ is the only eigenvalue of A for which there corresponds an eigenvector with non-negative components. It is well known that λ is not less than the absolute value of any other eigenvalue of A, so we shall call λ the *maximal eigenvalue* of A. Relation (3) in Theorem 1

becomes WIELANDT'S extremal characterization of the maximal eigenvalue [11]. Theorem 2 reduces to one of the two extremal properties, recently given by BIRKHOFF and VARGA [1; p. 28], of the maximal eigenvalue of A. Theorem 3* includes the following classical result of FROBENIUS [5]: ϱ is greater than the maximal eigenvalue λ of A, if and only if the inverse matrix $(\varrho I - A)^{-1}$ exists and has all its elements positive, where I denotes the identity matrix of order n.

In this special case (23), the equilibrium value λ_k of the system

$$\{f_1^{(k)}, \ldots, f_{k-1}^{(k)}, f_{k+1}^{(k)}, \ldots, f_n^{(k)};\ g_1^{(k)}, \ldots, g_{k-1}^{(k)}, g_{k+1}^{(k)}, \ldots, g_n^{(k)}\}$$

on S_k is clearly the maximal eigenvalue of the principal submatrix A_k obtained from A by deleting its k-th row and k-th column. From Corollary 6 and part (iii) of Theorem 4, we derive the following statement: If λ and λ_n are the maximal eigenvalue of A and A_n respectively, and if $\lambda > \varrho > \lambda_n$, then $\varrho I - A$ is non-singular, and all elements on the n-th column of $(\varrho I - A)^{-1}$ are negative. [By considering the transposed matrix, we see that all elements on the n-th row of $(\varrho I - A)^{-1}$ are also negative.] This result has been recently obtained by HOUSEHOLDER [7] and includes the following proposition of the author [3; Theorem 7]: If $\lambda > \varrho > \operatorname{Max}_{1 \leqq k \leqq n} \lambda_k$, then $\varrho I - A$ is non-singular, and all elements of $(\varrho I - A)^{-1}$ are negative. The converse of this last proposition (or the converse of HOUSEHOLDER'S result) is also true, according to part (iii) of Theorem 4 (see also the remark at the end of § 3).

5. Let $A = (a_{ij})$, $B = (b_{ij})$ be two square real matrices of order n. Let the functions f_i, g_i $(1 \leqq i \leqq n)$ on S be defined by

$$f_i(x) = \sum_{j=1}^{n} b_{ij} x_j, \qquad g_i(x) = \sum_{j=1}^{n} a_{ij} x_j \tag{24}$$

for $x = (x_1, x_2, \ldots, x_n) \in S$. Then clearly the system $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ will satisfy our conditions (a), (b), (c), (d), if and only if the matrices A, B possess the following three properties:

(α) $a_{ij} > 0$ $\quad (1 \leqq i \leqq n,\ 1 \leqq j \leqq n)$.

(β) $b_{ij} \leqq 0$ $\quad (1 \leqq i \leqq n,\ 1 \leqq j \leqq n,\ i \neq j)$.

(γ) *For any* $x = (x_1, x_2, \ldots, x_n) \in S$, *there is an index* i *for which* $\sum_{j=1}^{n} b_{ij} x_j > 0$.

The following lemma gives two other forms of condition (γ). For several other equivalent conditions, see [8], [6; p. 338–340], [9], [3; Theorem 5'].

LEMMA 2. *For a square real matrix* $B = (b_{ij})$ *of order* n *with* $b_{ij} \leqq 0$ $(i \neq j)$, *condition* (γ) *is equivalent to each of the following two conditions:*

(γ') B *is non-singular and all elements of the inverse matrix* B^{-1} *are non-negative.*

(γ'') *There exist* n *positive numbers* $\alpha_i > 0$ *such that* $\sum_{i=1}^{n} \alpha_i b_{ij} > 0$ *for* $1 \leqq j \leqq n$.

Proof. We first choose a $\varrho \geqq \operatorname{Max}_{1 \leqq i \leqq n} b_{ii}$. Let $C = \varrho I - B = (c_{ij})$. Then C is a matrix with non-negative elements.

$(\gamma)\to(\gamma')$: According to (γ), for any $x=(x_1, x_2, \ldots, x_n)\in S$, there is an index i for which $\varrho x_i > \sum_{j=1}^{n} c_{ij}x_j$. By taking as x an eigenvector of C corresponding to its maximal eigenvalue, we infer that ϱ must be greater than the maximal eigenvalue of C. Then by a result of FROBENIUS, $\varrho I - C = B$ is non-singular, and all elements of B^{-1} are non-negative.

$(\gamma')\to(\gamma'')$: By (γ'), $\varrho I - C$ is non-singular, and all elements of $(\varrho I - C)^{-1}$ are non-negative. If C^* denotes the transpose of C, then all elements of $(\varrho I - C^*)^{-1}$ are non-negative. Take any vector $\beta=(\beta_1, \beta_2, \ldots, \beta_n)$ with all $\beta_i>0$, and let $\alpha=(\alpha_1, \alpha_2, \ldots, \alpha_n)=(\varrho I - C^*)^{-1}\beta$. Then we have $\alpha_i>0$ and $\sum_{i=1}^{n}\alpha_i b_{ij}=\beta_i>0$.

$(\gamma'')\to(\gamma)$: This follows immediately from

$$\sum_{i=1}^{n}\alpha_i\left(\sum_{j=1}^{n}b_{ij}x_j\right)=\sum_{j=1}^{n}x_j\left(\sum_{i=1}^{n}\alpha_i b_{ij}\right)>0,$$

which holds for any $x=(x_1, x_2, \ldots, x_n)\in S$.

According to this lemma, the real matrices $B=(b_{ij})$ satisfying conditions (β), (γ) are precisely the "M-matrices" introduced and studied by OSTROWSKI [8], [9], also discussed by KOTELYANSKIĬ (see [6; p. 338]).

For f_i, g_i given by (24), the system of equations (1) may be written $Ax=\lambda Bx$ or $B^{-1}Ax=\lambda x$. From (α) and (γ'), all elements of the product matrix $B^{-1}A$ are positive. Hence, in the linear case (24), with A, B satisfying conditions (α), (β), (γ), the equilibrium value of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ is equal to the maximal eigenvalue of the positive matrix $B^{-1}A$, and the equilibrium point is an eigenvector of $B^{-1}A$ corresponding to its maximal eigenvalue. Let A_k, B_k denote the matrices of order $n-1$ obtained from A, B respectively by deleting the k-th row and k-th column. Let λ, λ_k denote the maximal eigenvalues of $B^{-1}A$ and $B_k^{-1}A_k$ respectively. Then, according to Corollary 6 and Theorem 4: A positive number ϱ satisfies the inequalities $\lambda>\varrho>\lambda_k$, if and only if $\varrho B - A$ is non-singular and all elements on the k-th column (also on the k-th row) of $(\varrho B - A)^{-1}$ are negative.

6. For the general case, the problem of determining the equilibrium value and equilibrium point is, of course, much more difficult than the linear case (24). For this task, the remarks given in this section may be useful.

Let $f_1, f_2, \ldots, f_n$ be n functions defined on S and satisfying conditions (a), (c), (d). Let g_{ij} $(1\leqq i\leqq n,\ 1\leqq j\leqq m)$ be mn continuous, concave, positive functions on S. Let

$$g_i(x)=\operatorname*{Min}_{1\leqq j\leqq m} g_{ij}(x) \qquad (x\in S,\ 1\leqq i\leqq n). \tag{25}$$

For any choice of $(j_1, j_2, \ldots, j_n)$ with $1\leqq j_i\leqq m$, let $\lambda(j_1, j_2, \ldots, j_n)$ denote the equilibrium value of the system $\{f_1, f_2, \ldots, f_n; g_{1j_1}, g_{2j_2}, \ldots, g_{nj_n}\}$. Let λ denote the equilibrium value of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$.

Since $g_i \leqq g_{ij}$, one sees easily from (3) that $\lambda \leqq \lambda(j_1, j_2, \ldots, j_n)$ holds for any choice of $(j_1, j_2, \ldots, j_n)$. If $\hat{x}$ is the equilibrium point of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$, then in view of (25), there is at least one n-tuple $(j_1, j_2, \ldots, j_n)$ such that $g_{ij_i}(\hat{x}) = \lambda f_i(\hat{x})$ for $1 \leqq i \leqq n$. Hence

$$\lambda = \operatorname*{Min}_{j_1, j_2, \ldots, j_n} \lambda(j_1, j_2, \ldots, j_n), \tag{26}$$

where the minimum is taken over all m^n n-tuples $(j_1, j_2, \ldots, j_n)$ with $1 \leqq j_i \leqq m$.

Furthermore, if the minimum is attained for $j_1 = k_1$, $j_2 = k_2, \ldots, j_n = k_n$, i.e. if $\lambda = \lambda(k_1, k_2, \ldots, k_n)$, then the equilibrium point of $\{f_1, f_2, \ldots, f_n; g_{1k_1}, g_{2k_2}, \ldots, g_{nk_n}\}$ is the equilibrium point of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$. In fact, let $\hat{y}$ be the equilibrium point of $\{f_1, f_2, \ldots, f_n; g_{1k_1}, g_{2k_2}, \ldots, g_{nk_n}\}$, i.e. $g_{ik_i}(\hat{y}) = \lambda f_i(\hat{y})$ for $1 \leqq i \leqq n$. As $g_i \leqq g_{ik_i}$, we have $g_i(\hat{y}) \leqq \lambda f_i(\hat{y})$ for $1 \leqq i \leqq n$. Then by Corollary 1, $\hat{y}$ must be the equilibrium point of $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$.

Consider now another situation. Let each of the systems $\{f_1, f_2, \ldots, f_n; g_1, g_2, \ldots, g_n\}$ and $\{f_{1j}, f_{2j}, \ldots, f_{nj}; g_{1j}, g_{2j}, \ldots, g_{nj}\}$ $(j = 1, 2, 3, \ldots)$ satisfy conditions (a), (b), (c), (d). Let their equilibrium values and equilibrium points be designated by λ, $\lambda(j)$ and $\hat{x}$, $\hat{x}(j)$ respectively. If

$$f_{ij}(x) \leqq f_{i,j+1}(x), \qquad g_{ij}(x) \geqq g_{i,j+1}(x), \tag{27}$$

$$f_i(x) = \lim_{j \to \infty} f_{ij}(x), \qquad g_i(x) = \lim_{j \to \infty} g_{ij}(x) \tag{28}$$

hold for all $x \in S$, then it is easily seen that

$$\lambda = \lim_{j \to \infty} \lambda(j), \qquad \lambda(j) \geqq \lambda(j+1), \tag{29}$$

$$\hat{x} = \lim_{j \to \infty} \hat{x}(j). \tag{30}$$

Bibliography

[1] BIRKHOFF, G., and R. S. VARGA: Reactor criticality and non-negative matrices. U. S. Atomic Energy Commission Research and Development Report, WAPD 166 (1957). — [2] FAN, K.: Existence theorems and extreme solutions for inequalities concerning convex functions or linear transformations. Math. Z. **68**, 205—216 (1957). — [3] FAN, K.: Topological proofs for certain theorems on matrices with non-negative elements. Monatshefte für Math. **62**, 219—237 (1958). — [4] FAN, K., I. GLICKSBERG and A. J. HOFFMAN: Systems of inequalities involving convex functions. Proc. Amer. Math. Soc. **8**, 617—622 (1957). — [5] FROBENIUS, G.: Über Matrizen aus positiven Elementen. Sitzungsber. Preuß. Akad. Wiss. Berlin **1908**, 471—476. — [6] GANTMAHER, F. R.: Theory of matrices (Russian). Moscow 1954. — [7] HOUSEHOLDER, A. S.: On matrices with non-negative elements. Monatshefte für Math. **62**, 238—242 (1958). — [8] OSTROWSKI, A.: Über die Determinanten mit überwiegender Hauptdiagonale. Commentarii Math. Helvetici. **10**, 69—96 (1937). — [9] OSTROWSKI, A.: Determinanten mit überwiegender Hauptdiagonale und die absolute Konvergenz von linearen Iterationsprozessen. Commentarii Math. Helvetici. **30**, 175—210 (1956). — [10] SPERNER, E.: Neuer Beweis für die Invarianz der Dimensionszahl und des Gebietes. Abhandl. Math. Sem. Hamburg. Univ. **6**, 265—272 (1928). — [11] WIELANDT, H.: Unzerlegbare, nicht negative Matrizen. Math. Z. **52**, 642—648 (1950).

Oak Ridge National Laboratory, Oak Ridge, Tenn. (U.S.A.)

(Eingegangen am 2. Juni 1958)

ZAREMBA, S. K.
Math. Zeitschr. Bd. 70, S. 281–282 (1958)

On Necessary Conditions for the Central Limit Theorem

By
S. K. ZAREMBA

A short proof of the most general form of the Central Limit Theorem for independent random variables being now available [3], it may be worth showing how a direct and completely elementary argument leads to the converse proposition, which FELLER [1] had established by means of sophisticated and not quite simple methods. The relevant proposition can be stated as follows:

THEOREM. Let $\{x_k\}$ be a sequence of independent random variables, and $\{a_n\}$ and $\{B_n\}$ numerical sequences with $a_n>0$ $(n=1, 2, \ldots)$; if the distribution of $X_n=a_n^{-1}(x_1+\cdots+x_n)-B_n$ tends to a normal distribution with a zero mean and a unit variance, and if $\{a_n^{-1}x_k\}$ are infinitesimal, i.e. if

$$(1)\qquad \begin{cases} \max\{P[a_n^{-1}|x_1|>\varepsilon], \ldots, P[a_n^{-1}|x_n|>\varepsilon]\}\to 0 \\ \text{for every positive } \varepsilon \text{ when } n\to\infty, \end{cases}$$

then, for every positive number η,

$$(2)\qquad P[|x_1|>\eta a_n]+\cdots+P[|x_n|>\eta a_n]\to 0 \quad \text{when } n\to\infty.$$

PROOF. Assume that the conditions of the theorem are satisfied, while, for a given positive η, (2) does not hold. Without loss of generality, we can assume that the sequence $\{P[x_1>\eta a_n]+\cdots+P[x_n>\eta a_n]\}$ has a positive upper limit Λ, finite or infinite. Let λ be any positive constant smaller than Λ. Clearly, there exists a sub-sequence $\{n(i)\}$ of the sequence $1, 2, \ldots$ for which $P[x_1>\eta a_{n(i)}]+\cdots+P[x_{n(i)}>\eta a_{n(i)}]$ is never smaller than λ. Given this sub-sequence, we form, in any of the various possible ways, a family $\{e_{n,k}\}$ $(n=1, 2, \ldots;$ $k=1, \ldots, n)$ of events having the following three properties: (i) For every n, $\{e_{n,1}, \ldots, e_{n,n}\}$ form a set of independent events; (ii) for every n and k, $e_{n,k}$ entails $x_k>\eta a_n$ with certainty; (iii) $P[e_{n(i),1}]+\cdots+P[e_{n(i),n(i)}]=\lambda$ for every i.

Owing to (1), $\max\{P[e_{n(i),1}], \ldots, P[e_{n(i),n(i)}]\}\to 0$ when $i\to\infty$. Hence, in view of (iii), if ν_n is the number of events $e_{n,1}, \ldots, e_{n,n}$ occurring for a given n, the distribution of $\nu_{n(i)}$ is Poissonian in the limit (cf. e.g. [2], p. 234), with

$$(3)\qquad P[\nu_{n(i)}=q]\to \exp(-\lambda)\cdot\lambda^q/q! \qquad \text{when } i\to\infty.$$

Clearly, we can choose an integer r, henceforth regarded as constant, satisfying

$$(4)\qquad \begin{cases} \frac{1}{2}\exp(-\lambda)\cdot\min\{1, \lambda^r/r!\}>4(r-1)^{-1}\eta^{-1}(2\pi)^{-\frac{1}{2}}\exp[-(r-1)^2\eta^2/8]> \\ >\dfrac{1}{\sqrt{2\pi}}\displaystyle\int_{(r-1)\eta/2}^{+\infty}\exp(-x^2/2)\,dx. \end{cases}$$

Let $j(1), \ldots, j(n)$ be any permutation of the numbers $1, \ldots, n$. Since (1) applies a fortiori to the conditional distributions arising out of the relevant

events $\bar{e}_{n,k}$, complementary to the respective $e_{n,k}$, the maximum, over the various permutations $j(1), \ldots, j(n)$, of $P[a_n^{-1}(x_{j(n-r+1)} + \cdots + x_{j(n)}) > \eta | \bar{e}_{n,j(n-r+1)} \cdots \bar{e}_{n,j(n)}]$ tends to 0 when $n \to \infty$. Thus, if m_n is the median of the conditional distribution of X_n given that $\nu_n = 0$,

$$\liminf_{n\to\infty} \min P\left[a_n^{-1}\sum_{t=1}^{n-r} x_{j(t)} - B_n > m_n - \eta \,|\, \bar{e}_{n,j(1)} \cdots \bar{e}_{n,j(n-r)}\right] \geqq \tfrac{1}{2},$$

the minimum referring to all the possible permutations $j(1), \ldots, j(n)$. Consequently,

$$\liminf_{n\to\infty} P[X_n > m_n + (r-1)\eta \,|\, \nu_n = r] \geqq \tfrac{1}{2},$$

and further, in view of (3),

$$\liminf_{i\to\infty} P[X_{n(i)} > m_{n(i)} + (r-1)\eta] \geqq \tfrac{1}{2}\exp(-\lambda)\cdot\lambda^r/r! \tag{5}$$

On the other hand, clearly,

$$\liminf_{i\to\infty} P[X_{n(i)} < m_{n(i)}] \geqq \tfrac{1}{2}\exp(-\lambda). \tag{6}$$

However, for every i at least one of the inequalities $m_{n(i)} + (r-1)\eta \geqq \frac{1}{2}(r-1)\eta$ and $m_{n(i)} \leqq -\frac{1}{2}(r-1)\eta$ must hold, and $\{n(i)\}$ can be replaced, if necessary, by a sub-sequence for which the same inequality is satisfied throughout. But then, if the distribution of $X_{n(i)}$ tends to the assumed limit, the left-hand side of either (5) or (6) cannot exceed the right-hand side of (4), which is thus contradicted. Hence the proof is complete.

The proposition no longer holds if, instead of being independent, $\{x_k\}$ are m-dependent. Indeed, let $\{u_i\}$ be independent and normally distributed with zero means and unit variances, and let

$$P[v_k = (2k)^{\frac{1}{2}}] = (2k)^{-1} \quad \text{and} \quad P[v_k = 0] = 1 - (2k)^{-1};$$

finally, make

$$x_{2j-1} = u_{2j-1} + v_j; \quad x_{2j} = u_{2j} - v_j \qquad (j = 1, 2, \ldots);$$

and

$$a_n = \sqrt{n}; \; B_n = 0 \qquad (n = 1, 2, \ldots).$$

Then $\{x_n\}$ are 1-dependent, $\{a_n^{-1}x_k\}$ are infinitesimal, and X_n is asymptotically normal with unit variance and mean 0, although (2) is not true when $\eta < 1$; it might be added that Condition (iii) of Theorem 2 in [3] is still satisfied.

The author wishes to thank Mr. J. D. NORTH, Chairman and Managing Director of Boulton Paul Aircraft, Ltd., for his encouragement and his permission to publish the present note.

References

[1] FELLER, W.: Über den zentralen Grenzwertsatz der Wahrscheinlichkeitsrechnung. Math. Z. **40**, 521–559 (1935) and 301–312 (1937). — [2] FELLER, W.: An Introduction to Probability Theory and its Applications. New York: Wiley & Sons 1950. — [3] ZAREMBA, S. K.: Note on the Central Limit Theorem. Math. Z. **69**, 295–298 (1958).

Boulton Paul Aircraft, Ltd., Wolverhampton, England

(Now: University College of Swansea, Wales)

(Eingegangen am 14. Mai 1958)

BENZ, W.
Math. Zeitschr. Bd. 70, S. 283–296 (1958)

$(8_3, 6_4)$-Konfigurationen in Laguerre-, Möbius- und weiteren Geometrien

Von

WALTER BENZ

In [3] hat L. PECZAR einen Beweis des Miquelschen Satzes (formuliert in Abschnitt 4 der vorliegenden Note) gemeinsam für Laguerre-, Möbius- und weitere Geometrien gegeben. Er stützt sich dabei auf einen kommutativen Ring $\mathfrak{R}$, der einen Körper $\mathfrak{K}$ enthält und in dem die Gleichung $qz = p$, wenn q und p Elemente von $\mathfrak{R}$ sind und q kein Nullteiler ist, stets eine Lösung z hat[1]). Nach von Staudtschem Vorbild führt PECZAR mit Hilfe von Doppelverhältnissen Ketten (wir sagen Kreise) ein: Sind w_1, w_2, w_3 verschiedene Elemente aus $\mathfrak{R}$ dergestalt, daß $w_2 - w_3$ nicht Nullteiler ist, so wird unter der Kette $(w_1 w_2 w_3)$ neben dem Element w_1 die Menge aller z verstanden, für die $w_1 - z$ nicht Nullteiler und für die das Doppelverhältnis

$$\begin{bmatrix} w_1 & w_2 \\ z & w_3 \end{bmatrix} = \frac{w_1 - w_3}{w_2 - w_3} \cdot \frac{w_2 - z}{w_1 - z} \equiv a$$

Element von $\mathfrak{K}$ ist[2]). Auf Grund von Hilfsbetrachtungen über lineare Substitutionen folgt, daß das Doppelverhältnis von vier verschiedenen Elementen der Kette $(w_1 w_2 w_3)$ in $\mathfrak{K}$ liegt, wenn von vornherein vorausgesetzt wird, daß

---

[1]) Um das auf S. 213 in [3] benutzte Beweisglied, daß jedes von Null verschiedene Element von $\mathfrak{K}$ nicht Nullteiler in $\mathfrak{R}$ ist [vgl. Fußnote [2])], aufrechtzuerhalten, ist (im Sinne von notwendig und hinreichend) noch zu fordern, daß $\mathfrak{R}$ ein Einselement besitzt und daß weiterhin dieses Einselement mit dem Einselement von $\mathfrak{K}$ übereinstimmt. Äquivalent hiermit ist die Forderung, daß mindestens ein von 0 verschiedenes Element von $\mathfrak{K}$ nicht Nullteiler in $\mathfrak{R}$ ist. — Es gibt Ringe mit den im Haupttext genannten Eigenschaften, die kein Einselement besitzen[1a]) und es gibt Ringe mit den im Haupttext genannten Eigenschaften, die ein Einselement besitzen, das jedoch verschieden ist von dem Einselement von $\mathfrak{K}$[1b]).

[1a]) $\mathfrak{R}$ sei der Ring aller geordneten Paare (x, ξ), wo x eine reelle Zahl und $\xi \in \{0, I\}$ ist, mit den Kompositionsvorschriften $(a, \alpha) + (b, \beta) = (a + b, \alpha + \beta)$, $(a, \alpha)(b, \beta) = (ab, \alpha\beta)$, wobei sein soll: $0 + 0 = I + I = 0$, $0 + I = I + 0 = I$ und $\alpha\beta = 0$ für alle $\alpha, \beta \in \{0, I\}$. Es sei $\mathfrak{K}$ der (zum Körper der reellen Zahlen isomorphe) Körper aller Paare $(x, 0)$.

[1b]) $\mathfrak{R}$ sei der Ring aller geordneten Paare (x, y) reeller Zahlen x, y mit komponentenweiser Addition und Multiplikation. $\mathfrak{K}$ sei der Körper aller Paare $(x, 0)$. Es ist $(1, 1)$ Einselement von $\mathfrak{R}$, das verschieden ist vom Einselement $(1, 0)$ von $\mathfrak{K}$. In diesem Beispiel ist offenbar jedes von Null verschiedene Element von $\mathfrak{K}$ Nullteiler.

[2]) Für den Fall $a \neq 0$ ergibt sich hieraus, daß $w_1 - w_3$ und $w_2 - z$ nicht Nullteiler in $\mathfrak{R}$ sind, wenn man noch voraussetzt, daß jedes Element $\neq 0$ von $\mathfrak{K}$ nicht Nullteiler in $\mathfrak{R}$ ist [vgl. hierzu die in Fußnote [1]) gemachte Bemerkung].

$w_1 - w_2$ und $w_1 - w_3$ nicht Nullteiler sind. Den Satz von MIQUEL entnimmt PECZAR nun der folgenden Doppelverhältnisidentität

$$\begin{bmatrix} z_1 & z_2 \\ z_4 & z_3 \end{bmatrix} \begin{bmatrix} z_5 & z_6 \\ z_8 & z_7 \end{bmatrix} \equiv \begin{bmatrix} z_1 & z_5 \\ z_4 & z_8 \end{bmatrix} \begin{bmatrix} z_6 & z_2 \\ z_7 & z_3 \end{bmatrix} \begin{bmatrix} z_1 & z_6 \\ z_8 & z_3 \end{bmatrix} \begin{bmatrix} z_5 & z_2 \\ z_4 & z_7 \end{bmatrix},$$

in der die z_i noch gewissen Bedingungen genügen müssen, um das Auftreten von Nullteilern im Nenner zu vermeiden. Läßt man $\mathfrak{K}$ den Körper der reellen Zahlen sein und $\mathfrak{R}$ resp. den Ring der dualen Zahlen, den Körper der komplexen Zahlen, so hat man den Satz von MIQUEL resp. in der Laguerre-, in der Möbius-Geometrie.

Das Ergebnis von PECZAR kann schon gewonnen werden (vgl. unsere Nr. 4), wenn man für $\mathfrak{R}$ — wie wir das im Vorliegenden stets tun wollen — allgemeiner einen kommutativen Ring zuläßt, der einen Körper $\mathfrak{K}$ so enthält, daß das Einselement von $\mathfrak{K}$ auch Einselement von $\mathfrak{R}$ ist: Die regulären Elemente von $\mathfrak{R}$ (d.h. die Elemente von $\mathfrak{R}$, die ein Inverses in $\mathfrak{R}$ besitzen) übernehmen dann diejenige Rolle, die bisher die Nichtnullteiler innehatten.

In der vorliegenden Note wird vornehmlich eine andere — in Laguerre-, Möbius- und weiteren Geometrien geltende — $(8_3, 6_4)$-Konfiguration, der sog. Büschelsatz (formuliert in 5), behandelt. Bemerkenswert ist hier die Feststellung, daß es — in zu präzisierendem Sinne — keine zur Doppelverhältnisidentität von PECZAR analoge Identität gibt, die den Büschelsatz beweist (Satz 2). Eine weitere — hiermit zusammenhängende — Besonderheit ist die: Der Satz von MIQUEL gilt in allen Geometrien $(\mathfrak{K}, \mathfrak{R})$, der Büschelsatz nicht. Wohl gilt der Büschelsatz in allen Geometrien $(\mathfrak{K}, \mathfrak{R})$, für die $(\mathfrak{R}:\mathfrak{K}) = 2$ erfüllt ist (Satz 3). Damit ist ein gemeinsamer Beweis des Büschelsatzes in Laguerre-, Möbius- und natürlich unendlich vielen weiteren, paarweise nichtisomorphen, Geometrien erbracht.

Mit dem in 8 eingeführten Begriff des L-Ringes in bezug auf einen Körper gelingt es schließlich, die Geometrien $(\mathfrak{K}, \mathfrak{R})$ zu kennzeichnen, die dem Büschelsatz genügen (Satz 4). Diese Kennzeichnung wurde für den Fall, daß $\mathfrak{R}$ kommutativer Körper ist, bereits in [1] geleistet.

1. Im folgenden seien stets (wenn nichts anderes gesagt ist) $\mathfrak{R}$ ein kommutativer Ring mit Einselement und $\mathfrak{K}$ ein in $\mathfrak{R}$ enthaltener Körper; wir verlangen, daß das Einselement von $\mathfrak{K}$ auch Einselement von $\mathfrak{R}$ ist. Die Menge der regulären Elemente von $\mathfrak{R}$ (also der Elemente, die ein Inverses in $\mathfrak{R}$ besitzen), wird mit $\mathfrak{r}$ bezeichnet. $\mathfrak{r}$ bildet gegenüber der Multiplikation eine Gruppe, die die multiplikative Gruppe $\mathfrak{K}^*$ von $\mathfrak{K}$ umfaßt. Die Elemente von $\mathfrak{R}$ heißen im folgenden Punkte. Eine Punktmenge $\mathfrak{m}$, $|\mathfrak{m}| \geqq 2$[3]), heiße *eigentlich*, wenn zu je zwei verschiedenen ihrer Elemente die Differenz regulär ist. Enthält die eigentliche Punktmenge $\{A_1, A_2, A_3, \ldots, A_n\}$ genau n verschiedene Punkte, n endlich, so heiße $A_1, A_2, A_3, \ldots, A_n$ ein *eigentliches Punkte-n-tupel*. Jedem geordneten eigentlichen Punktequadrupel A, B, C, D

[3]) Ist $\mathfrak{M}$ eine Menge, so wird mit $|\mathfrak{M}|$ ihre Mächtigkeit bezeichnet.

wird ein *Doppelverhältnis* $\begin{bmatrix} A & B \\ D & C \end{bmatrix}$ zugeordnet: dies sei das Element

$$\begin{bmatrix} A & B \\ D & C \end{bmatrix} = \frac{A-C}{B-C}\,\frac{B-D}{A-D},$$

das offensichtlich regulär ist.

Zu jedem eigentlichen Punktetripel A, B, C wird eine Punktmenge (ABC) definiert. (ABC) enthalte die Punkte A, B, C und weiterhin genau die Punkte X, für die A, B, C, X ein eigentliches Punktequadrupel und für die $\begin{bmatrix} A & B \\ X & C \end{bmatrix} \in \mathfrak{K}$ ist[4,5]). Die Mengen (ABC) heißen *Kreise*. Die Punktmenge $\{P, Q, \ldots\}$ heißt *konzyklisch*, wenn sie insgesamt einem Kreise angehört. Ist P ein Punkt und ist k ein Kreis mit $P \in k$, so werden die üblichen Redewendungen benutzt: *Der Punkt P liegt auf dem Kreis k, der Kreis k geht durch den Punkt P*, usf.

2. Ist $\mathfrak{K}$ der reelle Zahlkörper, $\mathfrak{R}$ der komplexe, so liegt die gewöhnliche Kreisgeometrie vor.

Ist $\mathfrak{K}$ der reelle Zahlkörper, $\mathfrak{R}$ der Ring der dualen Zahlen, so liegt die Laguerre-Geometrie vor. Dabei sind (vgl. [*3*]) die Punkte mit den Speeren — bis auf eine Klasse gleichsinnig paralleler — zu identifizieren und die Kreise mit den Zykeln. Die gleiche Algebra $\mathfrak{R}:\mathfrak{K}$ beschreibt auch eine Parabelgeometrie (vgl. PECZAR, a.a.O.).

Bildet man den Ring $x + y\eta$ über den reellen Zahlen x, y mit $\eta^2 = +1$, so kommt man zu einer Hyperbelgeometrie.

Der Bereich der definierten Geometrien umfaßt weitere anschauliche Geometrien.

3. Über Kreise, eigentliche Punktmengen und Doppelverhältnisse gelten die folgenden Eigenschaften:

(1) *Die verschiedenen Punkte eines Kreises bilden insgesamt eine eigentliche Punktmenge.*

Beweis. Es sei $k = (ABC)$ ein Kreis. Besteht der Kreis k nur aus drei oder nur aus vier verschiedenen Punkten, so ist nichts zu beweisen. Seien also X, Y untereinander und von A, B, C verschiedene Punkte auf k. Zu zeigen ist $X - Y \in \mathfrak{r}$. Es gilt

$$x \equiv (A-C)(B-C)^{-1}(B-X)(A-X)^{-1} \in \mathfrak{K}$$

und auch

$$y \equiv (A-C)(B-C)^{-1}(B-Y)(A-Y)^{-1} \in \mathfrak{K}.$$

---

[4]) Es könnte offenbar auch $\begin{bmatrix} A & B \\ X & C \end{bmatrix} \in \mathfrak{K}^*$ geschrieben werden.

[5]) Schwächer kann man (ABC) auch so definieren: (ABC) enthalte neben den Punkten A, B, C genau die Punkte X, für die $A - X$ regulär und für die $\frac{A-C}{B-C}\,\frac{B-X}{A-X} \in \mathfrak{K}$ ist. ($B - X$, $C - X \in \mathfrak{r}$ kann dann gefolgert werden.)

Da alle benutzten Differenzen in $\mathfrak{r}$ liegen, ist $x, y \in \mathfrak{r}$, d.h. $y \neq 0$ und somit

$$\mathfrak{R} \ni y^{-1}x = (A - Y)(B - Y)^{-1}(B - X)(A - X)^{-1}.$$

Weiter ist wegen $B - Y$, $A - X \in \mathfrak{r}$:

$$z = (A - B)(Y - B)^{-1}(Y - X)(A - X)^{-1}$$

bildbar; man hat

$$\begin{aligned} z &= [(A - Y) + (Y - B)](Y - B)^{-1}[(B - X) + (Y - B)](A - X)^{-1} \\ &= -y^{-1}x + (A - Y)(A - X)^{-1} + (B - X)(A - X)^{-1} + (Y - B)(A - X)^{-1} \\ &= -y^{-1}x + 1 \in \mathfrak{R}. \end{aligned}$$

Es ist sogar $z \neq 0$, d.h. $z \in \mathfrak{R}^*$: Sonst wäre

$$Y - X = (Y - B)(A - B)^{-1} \cdot (A - B)(Y - B)^{-1}(Y - X)(A - X)^{-1} \cdot (A - X) = 0,$$

d.h. $Y = X$, was nicht sein sollte. —

Nun gilt wegen $\mathfrak{R}^* \subseteq \mathfrak{r}$, d.h. wegen $z \in \mathfrak{r}$,

$$Y - X = (Y - B)(A - B)^{-1} z (A - X) \in \mathfrak{r}, \quad \text{q. e. d.}$$

Der folgende Satz veranschaulicht den Begriff der eigentlichen Punktmenge. Man denke dabei an die bereits in der Laguerre-Geometrie vorkommende Tatsache, *daß durch zwei verschiedene Punkte nicht notwendig ein Kreis geht.* (Zwei verschiedene, gleichsinnig parallele Speere können durch keinen Zykel verbunden werden.)

(2) *Dann und nur dann ist die Punktmenge* $\mathfrak{m}$, $|\mathfrak{m}| \geqq 3$, *eigentlich, wenn je zwei verschiedene ihrer Punkte konzyklisch sind.*

Beweis. Sind je zwei verschiedene Punkte X, Y der Menge $\mathfrak{m}$, $|\mathfrak{m}| \geqq 3$, konzyklisch, so folgt aus (1) $Y - X \in \mathfrak{r}$. Damit ist $\mathfrak{m}$ eigentlich. — Ist umgekehrt die Punktmenge $\mathfrak{m}$, $|\mathfrak{m}| \geqq 3$, eigentlich und sind X, Y, Z beliebige verschiedene Punkte aus $\mathfrak{m}$, so ist $X, Y \in (XYZ)$.

(3) a) *Ist* A, B, C, D *ein eigentliches Punktequadrupel, so gilt*

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} A & B \\ D & C \end{bmatrix}^{-1}; \quad \begin{bmatrix} B & A \\ D & C \end{bmatrix} = \begin{bmatrix} A & B \\ D & C \end{bmatrix}^{-1}; \quad \begin{bmatrix} A & C \\ D & B \end{bmatrix} = 1 - \begin{bmatrix} A & B \\ D & C \end{bmatrix}$$

und ferner

$$\begin{bmatrix} A & B \\ D & C \end{bmatrix} = \begin{bmatrix} B & A \\ C & D \end{bmatrix} = \begin{bmatrix} C & D \\ B & A \end{bmatrix} = \begin{bmatrix} D & C \\ A & B \end{bmatrix}.$$

b) *Ist* A, B, C, D, E *ein eigentliches Punktequintupel, so gilt*

$$\begin{bmatrix} A & B \\ E & C \end{bmatrix} = \begin{bmatrix} A & B \\ D & C \end{bmatrix} \begin{bmatrix} A & B \\ E & D \end{bmatrix}.$$

Gelegentlich benötigen wir das folgende Korrolar zu (3):

(4) a) *Ist A, B, C, D ein eigentliches Punktequadrupel und ist* $\begin{bmatrix} A & B \\ D & C \end{bmatrix} \in \mathfrak{K}$, *so gilt*

$$\begin{bmatrix} B & A \\ D & C \end{bmatrix}, \begin{bmatrix} A & C \\ D & B \end{bmatrix}, \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathfrak{K}.$$

b) *Ist A, B, C, D, E ein eigentliches Punktequintupel und ist*

$$\begin{bmatrix} A & B \\ D & C \end{bmatrix}, \begin{bmatrix} A & B \\ E & D \end{bmatrix} \in \mathfrak{K}, \qquad \text{so gilt auch} \qquad \begin{bmatrix} A & B \\ E & C \end{bmatrix} \in \mathfrak{K}.$$

Wie bereits angemerkt, gilt in der Laguerre-Geometrie nicht, daß durch drei verschiedene Speere stets genau ein Zykel geht. Allgemein hat man

Satz 1. *Durch drei verschiedene Punkte geht höchstens ein Kreis. Ferner: Durch drei verschiedene Punkte geht stets dann und nur dann genau ein Kreis, wenn $\mathfrak{R}$ Körper ist.*

Beweis. Der erste Teil des Satzes wird auf Grund von (4) wie Satz 1_2 in [1] bewiesen. Zum zweiten Teil: Ist $\mathfrak{R}$ Körper und sind A, B, C verschiedene Punkte, so geht — da $\{A, B, C\}$ gewiß eigentlich ist — (ABC) durch A, B, C. — Geht umgekehrt durch drei verschiedene Punkte stets genau ein Kreis, so muß $\mathfrak{R} = \mathfrak{r} \cup \{0\}$, d.h. es muß $\mathfrak{R}$ Körper sein: Wäre nämlich n ein von 0 verschiedenes Element aus $\mathfrak{R} - \mathfrak{r}$, so müßte durch die drei verschiedenen Punkte $0, 1, n$ ein Kreis gehen. Damit wäre nach (1) die Menge $\{0, 1, n\}$ eigentlich, was $n = n - 0 \in \mathfrak{r}$ ergäbe.

(5) *Sind A, B, C, D vier verschiedene Punkte eines Kreises k, so ist* $\begin{bmatrix} A & B \\ D & C \end{bmatrix} \in \mathfrak{K}$.

Beweis. Da durch drei verschiedene Punkte höchstens ein Kreis geht, ist $(ABC) = k$. Wegen $D \in k = (ABC)$ ist damit $\begin{bmatrix} A & B \\ D & C \end{bmatrix} \in \mathfrak{K}$.

4. Wir wenden uns hier dem Satz von MIQUEL zu auf der in der Einleitung angekündigten allgemeinen Grundlage. Der Beweis des Miquelschen Satzes von PECZAR kann unverändert übernommen werden.

Satz von Miquel[6]. *Lassen sich acht verschiedene Punkte, von denen je zwei gemeinsam auf mindestens einem Kreise liegen*[7], *so den Eckpunkten eines Würfels zuordnen, daß es fünfmal vorkommt, daß den Eckpunkten einer Seitenebene des Würfels vier konzyklische Punkte entsprechen, so ist dies auch bei den Eckpunkten der sechsten Seitenebene der Fall* (Fig. 1).

Beweis. Der Satz folgt unmittelbar aus der folgenden Identität

$$\textbf{(M)} \quad \begin{bmatrix} A & B \\ D & C \end{bmatrix} \begin{bmatrix} E & F \\ H & G \end{bmatrix} = \begin{bmatrix} A & E \\ D & H \end{bmatrix} \begin{bmatrix} F & B \\ G & C \end{bmatrix} \begin{bmatrix} A & F \\ H & C \end{bmatrix} \begin{bmatrix} E & B \\ D & G \end{bmatrix}.$$

[6]) Formuliert nach VAN DER WAERDEN, SMID [4].

[7]) Eine solche Voraussetzung kann nicht entbehrt werden, wie bereits der Fall der Laguerre-Geometrie lehrt: Sei $A = -\frac{5}{7} + \frac{24}{49}\varepsilon$, $B = 5 - \varepsilon$, $C = 4 + \varepsilon$, $D = -1$, $E = 1 + \varepsilon$, $F = 1 - \varepsilon$, $G = 2 + \varepsilon$, $H = 2 - \varepsilon$. Hier sind zwar die Quadrupel $ABCD$, $AEHD$, $FBCG$, $AFCH$, $EBGD$ konzyklisch, hingegen nicht $EFGH$, da E, F gleichsinnig parallele Speere sind wegen $E - F = 2\varepsilon$.

In der Tat: Liegen fünf der angeschriebenen Doppelverhältnisse in $\mathfrak{R}^*$, so auch gewiß das sechste, da $\mathfrak{R}^*$ Gruppe ist.

5. Eine weitere $(8_3, 6_4)$-Konfiguration ist der **Büschelsatz.** Er lautet[8]: *Gegeben seien vier Paare von insgesamt acht verschiedenen, paarweise konzyklischen, Punkten. Aus den vier Punktepaaren kann man durch Zusammenstellung je zweier verschiedener Paare sechs Punktequadrupel herstellen. Kommt es dann vor, daß fünf dieser Punktequadrupel konzyklisch sind auf insgesamt mindestens vier verschiedenen Kreisen, so ist auch das letzte Punktequadrupel konzyklisch* (Fig. 2).

Bei geeigneter Bezeichnung der Punkte kann der Büschelsatz äquivalent auch so formuliert werden: *Es seien* $A, B, C_1, C_2, A', B', C_1', C_2'$ *acht ver-*

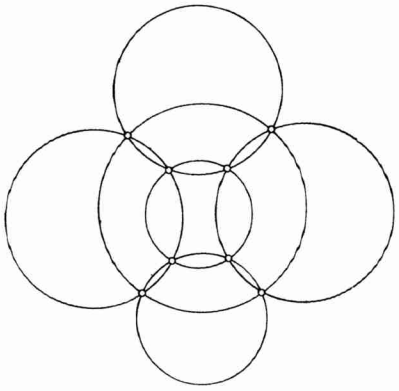

Fig. 1

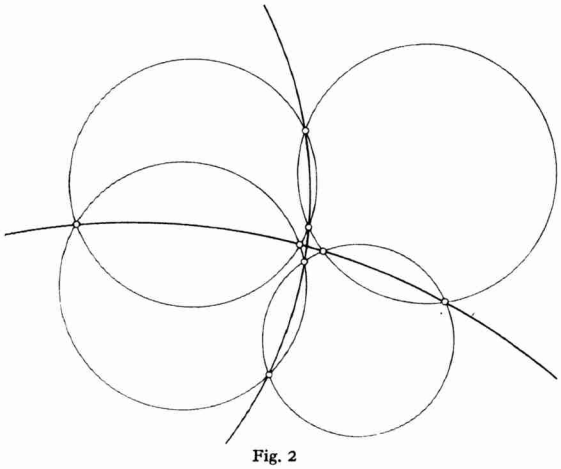

Fig. 2

schiedene Punkte, von denen je zwei gemeinsam auf mindestens einem Kreise liegen. Es seien $AA'BB'$, $AA'C_1C_1'$, $AA'C_2C_2'$, $BB'C_1C_1'$, $BB'C_2C_2'$ *konzyklische Punktequadrupel, nicht aber* $AA'BC_1$, $AA'BC_2$, $AA'C_1C_2$. *Dann ist auch das Punktequadrupel* $C_1C_1'C_2C_2'$ *konzyklisch.*

Zunächst sei gezeigt, daß es keine ähnlich einfache Identität wie (M) gibt, die den Büschelsatz beweist:

Satz 2. *Es sei* $\Omega(\mathfrak{R})$ *die Menge aller geordneten, eigentlichen Punkte-8-tupel*

$$\sigma^{(8)} = (A, B, C_1, C_2, A', B', C_1', C_2')$$

über $\mathfrak{R}$. *Es gibt dann keinen Ausdruck* Φ, *der durch endlich-oftmaliges Ausführen der Operationen Addition, Subtraktion, Multiplikation aus*

$$\begin{bmatrix} A & A' \\ B' & B \end{bmatrix}, \ldots^{9}), \quad \begin{bmatrix} A & A' \\ C_1' & C_1 \end{bmatrix}, \ldots, \quad \begin{bmatrix} A & A' \\ C_2' & C_2 \end{bmatrix}, \ldots, \quad \begin{bmatrix} B & B' \\ C_1' & C_1 \end{bmatrix}, \ldots, \quad \begin{bmatrix} B & B' \\ C_2' & C_2 \end{bmatrix}, \ldots$$

[8]) Formuliert nach VAN DER WAERDEN, SMID [4].

[9]) Mit den Punkten ... sind jeweils die permutierten Doppelverhältnisse des zuvor angeschriebenen Doppelverhältnisses gemeint. Man beachte dabei die Identitäten (3).

zusammengesetzt ist und der für jedes $\sigma^{(8)}$ *— unabhängig von* $\mathfrak{R}$ *— mit einem Doppelverhältnis* $\begin{bmatrix} C_1 & C_1' \\ C_2' & C_2 \end{bmatrix}, \ldots$ *übereinstimmt.*

Beweis. Angenommen, es gäbe doch einen Ausdruck Φ, der für alle $\sigma^{(8)} \in \Omega(\mathfrak{R})$ — unabhängig von $\mathfrak{R}$ — ein Doppelverhältnis $\begin{bmatrix} C_1 & C_1' \\ C_2' & C_2 \end{bmatrix}, \ldots$ ergäbe. Wir nehmen für $\mathfrak{R}$ speziell den Körper der reellen Zahlen und für $\mathfrak{R}$ den der rationalen her. Nimmt man dann acht verschiedene reelle Zahlen $A, B, C_1, C_2, A', B', C_1', C_2'$ so, daß

$$\begin{bmatrix} A & A' \\ B' & B \end{bmatrix}, \ldots, \quad \begin{bmatrix} A & A' \\ C_1' & C_1 \end{bmatrix}, \ldots, \quad \begin{bmatrix} A & A' \\ C_2' & C_2 \end{bmatrix}, \ldots, \quad \begin{bmatrix} B & B' \\ C_1' & C_1, \end{bmatrix}, \ldots, \quad \begin{bmatrix} B & B' \\ C_2' & C_2 \end{bmatrix}, \ldots$$

rationale Größen sind, so müßte — gemäß dem Aufbau von Φ — auch $\begin{bmatrix} C_1 & C_1' \\ C_2' & C_2 \end{bmatrix}, \ldots$ rational sein. Dies ist aber nicht immer der Fall, wie das folgende Beispiel zeigt: Sei

$$A = 0, \quad B = \frac{1}{2}, \quad C_1 = \frac{2+3\sqrt{2}}{7}, \quad C_2 = \frac{1+\sqrt{3}}{2}, \quad A' = -1, \quad B' = 2,$$

$$C_1' = \frac{2-3\sqrt{2}}{7}, \quad C_2' = \frac{4-6\sqrt{3}}{23}.$$

Dann sind die Größen

$$\begin{bmatrix} A & A' \\ B' & B \end{bmatrix} = \frac{1}{2}, \begin{bmatrix} A & A' \\ C_1' & C_1 \end{bmatrix} = -1, \begin{bmatrix} A & A' \\ C_2' & C_2 \end{bmatrix} = -\frac{3}{2}, \begin{bmatrix} B & B' \\ C_1' & C_1 \end{bmatrix} = -1, \begin{bmatrix} B & B' \\ C_2' & C_2 \end{bmatrix} = -4$$

rational; hingegen ist

$$\begin{bmatrix} C_1 & C_1' \\ C_2' & C_2 \end{bmatrix} = 49 - 20\sqrt{6}$$

irrational.

6. Den weiteren Erörterungen stellen wir die folgenden Hilfssätze voran:

HILFSSATZ 1. *Ist* $A, A', B, B', C_1, C_1', C_2, C_2'$ *ein eigentliches Punkte-8-tupel, so gilt*

$$\begin{bmatrix} C_1 & C_2' \\ C_1' & C_2 \end{bmatrix} = m \begin{bmatrix} A' & C_1' \\ A & C_1 \end{bmatrix} \begin{bmatrix} A' & C_2 \\ A & C_2' \end{bmatrix},$$

wenn gesetzt ist

$$m = 1 - \frac{1}{b_2}\left(b_1 \frac{\gamma_2}{\gamma_1} + b_2 \frac{\gamma_1}{\gamma_2}\right) + \frac{b_1}{b_2},$$

$$b_i = \begin{bmatrix} A' & A \\ C_i & C_i' \end{bmatrix} \begin{bmatrix} A' & A \\ B' & B \end{bmatrix}, \quad i = 1, 2,$$

$$\gamma_i = \begin{bmatrix} A' & A \\ C_i & B \end{bmatrix}, \quad i = 1, 2.$$

Beweis. Es ist

$$m=\left(1-\frac{\gamma_1}{\gamma_2}\right)+\frac{b_1}{b_2}\left(1-\frac{\gamma_2}{\gamma_1}\right)$$

und weiter mit

$$\frac{b_1}{b_2}=\begin{bmatrix}A' & A\\ C_1 & C_1'\end{bmatrix}\begin{bmatrix}A' & A\\ C_2' & C_2\end{bmatrix},$$

$$1-\frac{\gamma_1}{\gamma_2}=1-\begin{bmatrix}A' & A\\ C_1 & B\end{bmatrix}\begin{bmatrix}A' & A\\ B & C_2\end{bmatrix}=1-\begin{bmatrix}A' & A\\ C_1 & C_2\end{bmatrix}=\begin{bmatrix}A' & C_2\\ C_1 & A\end{bmatrix}$$

und entsprechend

$$1-\frac{\gamma_2}{\gamma_1}=\begin{bmatrix}A' & C_1\\ C_2 & A\end{bmatrix}$$

gilt

$$m=\begin{bmatrix}A' & C_2\\ C_1 & A\end{bmatrix}+\begin{bmatrix}A' & A\\ C_1 & C_1'\end{bmatrix}\begin{bmatrix}A' & A\\ C_2' & C_2\end{bmatrix}\begin{bmatrix}A' & C_1\\ C_2 & A\end{bmatrix}.$$

Nun ist

$$\begin{bmatrix}A' & C_2\\ C_1 & A\end{bmatrix}\begin{bmatrix}A' & C_1'\\ A & C_1\end{bmatrix}\begin{bmatrix}A' & C_2\\ A & C_2'\end{bmatrix}\begin{bmatrix}C_1 & C_2'\\ C_2 & C_1'\end{bmatrix}=\begin{bmatrix}A' & C_1'\\ A & C_1\end{bmatrix}\begin{bmatrix}A' & C_2\\ C_1 & C_2'\end{bmatrix}\begin{bmatrix}C_1 & C_2'\\ C_2 & C_1'\end{bmatrix}$$

$$=\begin{bmatrix}A' & C_1'\\ A & C_1\end{bmatrix}\begin{bmatrix}C_1 & C_2'\\ A' & C_2\end{bmatrix}\begin{bmatrix}C_1 & C_2'\\ C_2 & C_1'\end{bmatrix}=\begin{bmatrix}A' & C_1'\\ A & C_1\end{bmatrix}\begin{bmatrix}C_1 & C_2'\\ A' & C_1'\end{bmatrix}$$

$$=\begin{bmatrix}A' & C_1'\\ A & C_1\end{bmatrix}\begin{bmatrix}A' & C_1'\\ C_1 & C_2'\end{bmatrix}=\begin{bmatrix}A' & C_1'\\ A & C_2'\end{bmatrix};$$

weiterhin ergibt explizites Anschreiben

$$\begin{bmatrix}A' & A\\ C_1 & C_1'\end{bmatrix}\begin{bmatrix}A' & A\\ C_2' & C_2\end{bmatrix}\begin{bmatrix}A' & C_1\\ C_2 & A\end{bmatrix}\begin{bmatrix}A' & C_1'\\ A & C_1\end{bmatrix}\begin{bmatrix}A' & C_2\\ A & C_2'\end{bmatrix}\begin{bmatrix}C_1 & C_2'\\ C_2 & C_1'\end{bmatrix}=\begin{bmatrix}A' & C_2'\\ A & C_1'\end{bmatrix}.$$

Damit ist

$$m\begin{bmatrix}A' & C_1'\\ A & C_1\end{bmatrix}\begin{bmatrix}A' & C_2\\ A & C_2'\end{bmatrix}\begin{bmatrix}C_1 & C_2'\\ C_2 & C_1'\end{bmatrix}=\begin{bmatrix}A' & C_1'\\ A & C_2'\end{bmatrix}+\begin{bmatrix}A' & C_2'\\ A & C_1'\end{bmatrix}=1$$

nach (3), was die Behauptung unmittelbar ergibt.

HILFSSATZ 2. *Ist $\gamma\in\mathfrak{r}-\mathfrak{R}$ und hat $\gamma^2+a\gamma+b=0$ eine Lösung $a, b\in\mathfrak{R}$, so ist diese Lösung eindeutig bestimmt. Ferner ist $b\neq 0$. [Ist genau in dieser Weise einem $\gamma\in\mathfrak{r}-\mathfrak{R}$ eindeutig ein — geordnetes — Paar (a, b) von Elementen aus $\mathfrak{R}$ zugeordnet, so schreiben wir $\gamma\to(a, b)$.]*

Beweis. Hätte man noch $\gamma^2+a'\gamma+b'=0$ für $(a', b')\neq(a, b)$ und $a', b'\in\mathfrak{R}$, so wäre $(a-a')\gamma=(b'-b)$ und also doch $(a', b')=(a, b)$ wegen $\gamma\notin\mathfrak{R}$. — Wäre nun $b=0$, so würde $\gamma(\gamma+a)=0$ wegen $\gamma\in\mathfrak{r}$ ergeben $\gamma=-a\in\mathfrak{R}$.

HILFSSATZ 3. *Ist A, A', B, B', C, C' ein eigentliches Punkte-6-tupel und gilt*

$$\begin{bmatrix}A' & A\\ B & B'\end{bmatrix},\ \begin{bmatrix}A' & A\\ C & C'\end{bmatrix},\ \begin{bmatrix}B' & B\\ C & C'\end{bmatrix}\in\mathfrak{R}$$

und ferner

$$\gamma \equiv \begin{bmatrix} A' & A \\ C & B \end{bmatrix} \notin \mathfrak{R},$$

so genügt γ einer Gleichung

$$\gamma^2 + a\gamma + b = 0$$

mit Größen a, b aus $\mathfrak{R}$. Insbesondere ist $b = \begin{bmatrix} A' & A \\ B' & B \end{bmatrix}\begin{bmatrix} A' & A \\ C & C' \end{bmatrix}$.

Beweis. Es ist

$$\begin{bmatrix} A' & A \\ C' & B' \end{bmatrix} = \begin{bmatrix} A' & A \\ B & B' \end{bmatrix}\begin{bmatrix} A' & A \\ C & B \end{bmatrix}\begin{bmatrix} A' & A \\ C' & C \end{bmatrix} = u\gamma, \quad u \in \mathfrak{R}^*,$$

wenn $u = \begin{bmatrix} A' & A \\ B & B' \end{bmatrix}\begin{bmatrix} A' & A \\ C' & C \end{bmatrix}$ gesetzt ist.

Weiterhin erkennt man vermittels expliziten Anschreibens

$$\begin{bmatrix} A' & B' \\ C' & A \end{bmatrix} = \begin{bmatrix} C' & A \\ A' & C \end{bmatrix}\begin{bmatrix} B' & C \\ B & C' \end{bmatrix}\begin{bmatrix} A' & B' \\ B & A \end{bmatrix}\begin{bmatrix} A' & C \\ A & B \end{bmatrix} = v\begin{bmatrix} A' & C \\ A & B \end{bmatrix}$$

mit einer Größe $v \in \mathfrak{R}^*$.

Addiert man die beiden Gleichungen auf und beachtet man dabei (3), sowie

$$\begin{bmatrix} A' & C \\ B & A \end{bmatrix} = 1 - \begin{bmatrix} A' & A \\ B & C \end{bmatrix} = 1 - \frac{1}{\gamma}, \quad \text{d.h.} \quad \begin{bmatrix} A' & C \\ A & B \end{bmatrix} = \frac{1}{1 - \frac{1}{\gamma}}$$

(da A', C, B, A ein eigentliches Punktequadrupel ist, sind die Größen

$$\gamma = \begin{bmatrix} A' & A \\ C & B \end{bmatrix}, \quad 1 - \frac{1}{\gamma} = \begin{bmatrix} A' & C \\ B & A \end{bmatrix}$$

regulär), so ist

$$1 = u\gamma + v \cdot \frac{1}{1 - \frac{1}{\gamma}}$$

bzw. weiter

$$\gamma^2 + \frac{v - u - 1}{u}\gamma + \frac{1}{u} = 0$$

wegen $u \neq 0$.

Wegen Hilfssatz 2 sind die Größen

$$\frac{v - u - 1}{u} \quad \text{und} \quad b = \frac{1}{u} = \begin{bmatrix} A' & A \\ B' & B \end{bmatrix}\begin{bmatrix} A' & A \\ C & C' \end{bmatrix}$$

eindeutig bestimmt.

Hilfssatz 4. *Es besitze $\mathfrak{R}$ einen involutorischen Automorphismus $a \to \bar{a}$, der genau die Elemente von $\mathfrak{R}$ als Fixpunkte besitzt. Ist dann γ ein Element aus*

$\mathfrak{r}-\mathfrak{K}$, *so gilt*

$$\gamma \to (-\gamma-\bar{\gamma}, \gamma\bar{\gamma}).$$

Sind γ_1, γ_2 *Elemente aus* $\mathfrak{r}-\mathfrak{K}$ *und ist* $\gamma_i \to (a_i, b_i)$, $i=1, 2$, *so gilt*

$$b_1\frac{\gamma_2}{\gamma_1}+b_2\frac{\gamma_1}{\gamma_2}\in\mathfrak{K}.$$

Beweis. Sei $\gamma\in\mathfrak{r}-\mathfrak{K}$ und sei $a=-(\gamma+\bar{\gamma})$, $b=\gamma\bar{\gamma}$. Wegen $a=\bar{a}$, $b=\bar{b}$ ist $a, b\in\mathfrak{K}$. Wegen Hilfssatz 2 und $\gamma^2-(\gamma+\bar{\gamma})\gamma+\gamma\bar{\gamma}=0$ ist dann $\gamma\to(-\gamma-\bar{\gamma}, \gamma\bar{\gamma})$. Ist nun $\gamma_1, \gamma_2\in\mathfrak{r}-\mathfrak{K}$, so gilt mit dem gerade Bewiesenen

$$b_1\frac{\gamma_2}{\gamma_1}+b_2\frac{\gamma_1}{\gamma_2}=\bar{\gamma}_1\gamma_2+\bar{\gamma}_2\gamma_1.$$

Wegen $\overline{\bar{\gamma}_1\gamma_2+\bar{\gamma}_2\gamma_1}=\bar{\gamma}_1\gamma_2+\bar{\gamma}_2\gamma_1$ ist alles bewiesen. Genau so einfach zeigt man

HILFSSATZ 5. *Es sei* $\mathfrak{K}$ *von Charakteristik* 2. *Gilt dann* $\gamma^2\in\mathfrak{K}$ *für jedes* $\gamma\in\mathfrak{R}$, *so hat man für jedes Element* $\gamma\in\mathfrak{r}-\mathfrak{K}$, $\gamma\to(0, \gamma^2)$. *Sind* γ_1, γ_2 *Elemente aus* $\mathfrak{r}-\mathfrak{K}$ *und ist* $\gamma_i\to(a_i, b_i)$, $i=1, 2$, *so gilt* $b_1\frac{\gamma_2}{\gamma_1}+b_2\frac{\gamma_1}{\gamma_2}=0$.

7. Nicht in allen Geometrien $(\mathfrak{K}, \mathfrak{R})$ gilt der Büschelsatz: dies zeigte der Beweis von Satz 2, wenn man für $\mathfrak{K}$ den Körper der rationalen und für $\mathfrak{R}$ den der reellen Zahlen nimmt. Gezeigt wurde dies auch bereits in [*1*], wo allerdings in der Diskussion ein weiterer Punkt ∞ auftrat[10]). Bevor wir nun die Geometrien $(\mathfrak{K}, \mathfrak{R})$ kennzeichnen, in denen der Büschelsatz gilt, wenden wir uns dem Sonderfall zu, daß $\mathfrak{R}$ zusätzlich (neben den in dieser Arbeit stets gemachten Voraussetzungen) ein hyperkomplexes System vom Rang 2 über $\mathfrak{K}$ ist. Dieser Sonderfall umfaßt die Möbius-, die Laguerre-Geometrie und auch die von HOFFMAN [*2*] untersuchten Geometrien neben unendlich vielen weiteren, paarweise nichtisomorphen, Geometrien.

Satz 3. *Die Geometrien* $(\mathfrak{K}, \mathfrak{R})$, *für die zusätzlich* $(\mathfrak{R}:\mathfrak{K})=2$ *ist, genügen dem Büschelsatz.*

Beweis. Es seien $A, B, C_1, C_2, A', B', C_1', C_2'$ acht verschiedene Punkte, von denen je zwei konzyklisch sind. Nach (2) liegt also ein eigentliches Punkte-8-tupel vor. Sind dann $AA'BB'$, $AA'C_1C_1'$, $AA'C_2C_2'$, $BB'C_1C_1'$, $BB'C_2C_2'$ konzyklische Punktequadrupel, nicht aber $AA'BC_1$, $AA'BC_2$, $AA'C_1C_2$, so ist zu zeigen, daß auch $C_1C_1'C_2C_2'$ ein konzyklisches Punktequadrupel ist. Zunächst ist $\gamma_i\equiv\begin{bmatrix}A' & A\\ C_i & B\end{bmatrix}\notin\mathfrak{K}$, da sonst die Kreise $(A'AB)$, $(A'AC_i)$ übereinstimmten. Hilfssatz 3 angewandt auf die eigentlichen Punkte-6-tupel A, A', B, B', C_i, C_i', $i=1, 2$, erkennt man, daß gilt $\gamma_i\to(a_i, b_i)$ für ein gewisses $a_i\in\mathfrak{K}$ und für $b_i=\begin{bmatrix}A' & A\\ B' & B\end{bmatrix}\begin{bmatrix}A' & A\\ C_i & C_i'\end{bmatrix}\in\mathfrak{K}$. — Sei nun $1, \vartheta$ eine Basis von $\mathfrak{R}$ über $\mathfrak{K}$. Dann ist $\vartheta^2=r+s\vartheta$ für Größen $r, s\in\mathfrak{K}$. Hat man nun nicht

[10]) In [*1*] waren für $\mathfrak{R}$ nur kommutative Körper zugelassen. Dadurch fielen die Geometrien $(\mathfrak{K}, \mathfrak{R})$ mit „Laguerre-Charakter" heraus nach Satz 1.

gleichzeitig $s=0$ und Charakteristik $\mathfrak{K}=2$, so ist

$$p+q\vartheta \to p+q(s-\vartheta)$$

ein involutorischer Automorphismus von $\mathfrak{R}$, der genau die Elemente von $\mathfrak{K}$ festläßt. Ist gleichzeitig Charakteristik $\mathfrak{K}=2$ und $s=0$, so gilt für jedes $\gamma \in \mathfrak{R}$ sicherlich $\gamma^2 \in \mathfrak{K}$. In jedem Falle ist (vermittels der Hilfssätze 4, 5)

$$b_1 \frac{\gamma_2}{\gamma_1} + b_2 \frac{\gamma_1}{\gamma_2} \in \mathfrak{K}.$$

Dann beweist Hilfssatz 1 den Büschelsatz.

8. DEFINITION. *Das Elementepaar γ_1, γ_2 heiße speziell, wenn gilt*

(a) $\gamma_1,\ \gamma_2 \in \mathfrak{r} - \mathfrak{K}, \quad \frac{\gamma_1}{\gamma_2} \notin \mathfrak{K}.$

(b) *Es gibt Größen a_i und b_i aus $\mathfrak{K}$ mit $\gamma_i \to (a_i, b_i)$ für $i=1, 2$.*

(c) *Es gibt Größen k, ϱ mit*

c_1) $0, 1, b_1, b_2 \neq k \in \mathfrak{K}$,

c_2) $1 \neq \varrho \in \mathfrak{r}$,

c_3) $1 - \varrho\sigma \in \mathfrak{r}$ *für alle* σ *aus* $\left\{1, k, \gamma_1, \gamma_2, k\frac{\gamma_1}{b_1}, k\frac{\gamma_2}{b_2}\right\}$[11]).

c_4) *Es ist* $\gamma_1 - \gamma_2 \in \mathfrak{r}$, $\frac{\gamma_1}{b_1} - \frac{\gamma_2}{b_2} \in \mathfrak{r}$ *und weiterhin jeweils für* $i=1, 2$

$$1 - \gamma_i\sigma \in \mathfrak{r} \quad \text{für alle } \sigma \text{ aus } \left\{1, \frac{k}{b_i}, \frac{1}{k}, \frac{1}{b_i}\right\}^{12}).$$

DEFINITION. *Es sei $\mathfrak{R}$ ein kommutativer Ring und es sei $\mathfrak{K}$ ein Körper. $\mathfrak{R}$ heiße ein L-Ring in bezug auf $\mathfrak{K}$, wenn gilt*

(L_1) $\mathfrak{K} \subseteqq \mathfrak{R}$.

(L_2) *Das Einselement von $\mathfrak{K}$ ist auch Einselement von $\mathfrak{R}$.*

(L_3) *Für jedes spezielle Elementepaar γ_1, γ_2 gilt*

$$b_1 \frac{\gamma_2}{\gamma_1} + b_2 \frac{\gamma_1}{\gamma_2} \in \mathfrak{K}^{13}),$$

wo b_i durch $\gamma_i \to (a_i, b_i)$ festgelegt ist, $i=1, 2$.

---

[11]) Man beachte $b_i \neq 0$, $i=1, 2$, wegen Hilfssatz 2.

[12]) Ist $\mathfrak{R}$ Körper und besitzt $\mathfrak{K}$ wenigstens sechs verschiedene Elemente, so ist jedes Elementepaar γ_1, γ_2 aus $\mathfrak{R} - \mathfrak{K}$, welches (b) genügt und für das $\frac{\gamma_1}{\gamma_2} \notin \mathfrak{K}$ gilt, speziell: Man braucht nur für k irgendein Element aus $\mathfrak{K} - \{0, 1, -1, b_1, b_2\}$ zu nehmen und $k=\varrho$ zu setzen. (Dabei wird hier auch $k \neq -1$ vorausgesetzt, da sonst $1 - \varrho k = 0 \notin \mathfrak{r}$ wäre.)

[13]) Für den Sonderfall $(\mathfrak{R}:\mathfrak{K})=2$ hatte man $b_1\frac{\gamma_2}{\gamma_1} + b_2\frac{\gamma_1}{\gamma_2} \in \mathfrak{K}$ sogar für jedes Elementepaar $\gamma_1, \gamma_2 \in \mathfrak{r} - \mathfrak{K}$ mit $\gamma_i \to (a_i, b_i)$. (Hier ist also $\mathfrak{R}$ L-Ring in bezug auf $\mathfrak{K}$.) Benötigt wird die Aussage aber nur für spezielle Elementepaare.

Damit kommen wir zu

Satz 4. *Es seien $\mathfrak{R}$ ein kommutativer Ring und $\mathfrak{K}$ ein in $\mathfrak{R}$ enthaltener Körper, dessen Einselement auch Einselement von $\mathfrak{R}$ ist. Es gilt: Die Geometrie $(\mathfrak{K}, \mathfrak{R})$ genügt dann und nur dann ausnahmslos dem Büschelsatz, wenn $\mathfrak{R}$ L-Ring in bezug auf $\mathfrak{K}$ ist.*

Beweis. Sei $\mathfrak{R}$ L-Ring in bezug auf $\mathfrak{K}$ und seien $A, B, C_1, C_2, A', B', C_1', C_2'$ acht verschiedene Punkte, von denen je zwei konzyklisch sind. Nach (2) liegt damit ein eigentliches Punkte-8-tupel vor. Sind dann $AA'BB'$, $AA'C_1C_1'$, $AA'C_2C_2'$, $BB'C_1C_1'$, $BB'C_2C_2'$ konzyklische Punktequadrupel, nicht aber $AA'BC_1$, $AA'BC_2$, $AA'C_1C_2$[14]), so ist also zu zeigen, daß $C_1C_1'C_2C_2'$ ein konzyklisches Punktequadrupel ist. Man hat $\gamma_i \equiv \begin{bmatrix} A' & A \\ C_i & B \end{bmatrix} \notin \mathfrak{K}$, da die Kreise $(A'AB)$, $(A'AC_i)$ verschieden sind. Wir weisen nach, daß γ_1, γ_2 ein spezielles Elementepaar ist. (a) ist evident, weil A', A, B, C_i, $i = 1, 2$, eigentliche Punktequadrupel sind und weil $\frac{\gamma_1}{\gamma_2} = \begin{bmatrix} A' & A \\ C_1 & C_2 \end{bmatrix} \notin \mathfrak{K}$ ist. (b): Hilfssatz 3 angewandt auf die eigentlichen Punkte-6-tupel A, A', B, B', C_i, C_i', $i = 1, 2$, erkennt man, daß gilt $\gamma_i \to (a_i, b_i)$ für ein gewisses $a_i \in \mathfrak{K}$ und für

$$b_i = \begin{bmatrix} A' & A \\ B' & B \end{bmatrix} \begin{bmatrix} A' & A \\ C_i & C_i' \end{bmatrix} \in \mathfrak{K}.$$

Für (c) setze man $k = \begin{bmatrix} A' & A \\ B' & B \end{bmatrix}$ und $\varrho = \frac{A-B}{A'-B}$. Zu c_1): Für jedes eigentliche Punktequadrupel P, Q, R, S ist gewiß $\begin{bmatrix} P & Q \\ S & R \end{bmatrix} \neq 0$ wegen $\begin{bmatrix} P & Q \\ S & R \end{bmatrix} \in \mathfrak{r}$. Damit ist $k \neq 0$. Im Falle $k = 1$ wäre $0 \neq \begin{bmatrix} A' & B \\ B' & A \end{bmatrix} = 1 - \begin{bmatrix} A' & A \\ B' & B \end{bmatrix} = 1 - k = 0$. Im Falle $k = b_i = \begin{bmatrix} A' & A \\ B' & B \end{bmatrix} \begin{bmatrix} A' & A \\ C_i & C_i' \end{bmatrix}$ wäre $\begin{bmatrix} A' & A \\ C_i & C_i' \end{bmatrix} = 1$, was auf $\begin{bmatrix} A' & C_i' \\ C_i & A \end{bmatrix} = 0$ führte.

c_2): Sicherlich ist $\varrho \in \mathfrak{r}$. Im Falle $\varrho = 1$ wäre $A - B = A' - B$, d.h. $A = A'$. Es folgt c_3) aus

$$1 - \varrho = \frac{A - A'}{B - A'}, \qquad 1 - \varrho k = \frac{A' - A}{A' - B'},$$

$$1 - \varrho \gamma_i = \frac{A' - A}{A' - C_i}, \qquad 1 - \varrho k \frac{\gamma_i}{b_i} = \frac{A' - A}{A' - C_i'}.$$

c_4): Es ist

$$\gamma_1 - \gamma_2 = \gamma_1 \left(1 - \frac{\gamma_2}{\gamma_1}\right) = \gamma_1 \left(1 - \begin{bmatrix} A' & A \\ C_2 & B \end{bmatrix} \begin{bmatrix} A' & A \\ B & C_1 \end{bmatrix}\right)$$

$$= \gamma_1 \left(1 - \begin{bmatrix} A' & A \\ C_2 & C_1 \end{bmatrix}\right) = \gamma_1 \begin{bmatrix} A' & C_1 \\ C_2 & A \end{bmatrix} \in \mathfrak{r}.$$

[14]) Es wird nicht behauptet, daß es eigentliche Punkte-8-tupel mit den genannten Eigenschaften gibt.

Weiter gilt

$$\frac{\gamma_1}{b_1} - \frac{\gamma_2}{b_2} = \frac{\gamma_1}{b_1}\left(1 - \frac{b_1}{b_2}\frac{\gamma_2}{\gamma_1}\right)$$
$$= \frac{\gamma_1}{b_1}\left(1 - \begin{bmatrix} A' & A \\ C_1 & C_1' \end{bmatrix}\begin{bmatrix} A' & A \\ C_2' & C_2 \end{bmatrix}\begin{bmatrix} A' & A \\ C_2 & C_1 \end{bmatrix}\right) = \frac{\gamma_1}{b_1}\left(1 - \begin{bmatrix} A' & A \\ C_2' & C_1' \end{bmatrix}\right) = \frac{\gamma_1}{b_1}\begin{bmatrix} A' & C_1' \\ C_2' & A \end{bmatrix} \in \mathfrak{r}.$$

Schließlich ist

$$1 - \gamma_i = \begin{bmatrix} A' & B \\ C_i & A \end{bmatrix}, \quad 1 - \gamma_i \frac{k}{b_i} = 1 - \begin{bmatrix} A' & A \\ C_i & B \end{bmatrix}\begin{bmatrix} A' & A \\ C_i' & C_i \end{bmatrix} = \begin{bmatrix} A' & B \\ C_i' & A \end{bmatrix},$$
$$1 - \frac{\gamma_i}{k} = 1 - \begin{bmatrix} A' & A \\ C_i & B \end{bmatrix}\begin{bmatrix} A' & A \\ B & B' \end{bmatrix} = \begin{bmatrix} A' & B' \\ C_i & A \end{bmatrix},$$
$$1 - \frac{\gamma_i}{b_i} = 1 - \begin{bmatrix} A' & A \\ C_i & B \end{bmatrix}\begin{bmatrix} A' & A \\ B & B' \end{bmatrix}\begin{bmatrix} A' & A \\ C_i' & C_i \end{bmatrix} = \begin{bmatrix} A' & B' \\ C_i' & A \end{bmatrix}.$$

Da also γ_1, γ_2 ein spezielles Elementepaar ist und da $\mathfrak{R}$ L-Ring in bezug auf $\mathfrak{K}$ ist, hat man $b_1\frac{\gamma_2}{\gamma_1} + b_2\frac{\gamma_1}{\gamma_2} \in \mathfrak{K}$. Mit Hilfssatz 1 ist nun C_1, C_1', C_2, C_2' ein konzyklisches Punktequadrupel. Damit gilt der Büschelsatz.

Sei nun umgekehrt in der Geometrie $(\mathfrak{K}, \mathfrak{R})$ stets der Büschelsatz erfüllt. Sei γ_1, γ_2 ein spezielles Elementepaar und seien a_i, b_i, k, ϱ Größen mit den Eigenschaften (b), (c). Wir konstruieren ein eigentliches Punkte-8-tupel: Sei

$$A = 0, \quad A' = 1, \quad B = 1 - \frac{1}{1-\varrho}, \quad B' = 1 - \frac{1}{1-\varrho k},$$
$$C_i = 1 - \frac{1}{1-\varrho\gamma_i}, \quad C_i' = 1 - \frac{1}{1 - \varrho k\frac{\gamma_i}{b_i}}.$$

In der Tat sind die Differenzen je zweier verschiedener Punkte regulär, wie man (a), (b), (c) (s. Def. des speziellen Elementepaares) entnimmt. Weiter sind $AA'BB'$, $AA'C_1C_1'$, $AA'C_2C_2'$, $BB'C_1C_1'$, $BB'C_2C_2'$ konzyklische Punktequadrupel, hingegen nicht $AA'BC_1$, $AA'BC_2$, $AA'C_1C_2$:

Einmal ist

$$\begin{bmatrix} A' & A \\ B' & B \end{bmatrix} = \frac{A'-B}{A-B}\frac{A-B'}{A'-B'} = k \in \mathfrak{K}, \quad \begin{bmatrix} A' & A \\ C_i & C_i' \end{bmatrix} = \frac{A'-C_i'}{A-C_i'}\frac{A-C_i}{A'-C_i} = \frac{b_i}{k} \in \mathfrak{K},$$
$$\begin{bmatrix} B' & B \\ C_i' & C_i \end{bmatrix} = \frac{B'-C_i}{B-C_i}\frac{B-C_i'}{B'-C_i'} = \frac{-(b_i+\gamma_i^2) + \gamma_i\left(k + \frac{b_i}{k}\right)}{-(b_i+\gamma_i^2) + \gamma_i(1+b_i)} = \frac{a_i + \left(k + \frac{b_i}{k}\right)}{a_i + (1+b_i)} \in \mathfrak{K}^{15}),$$

wenn man bei der letzteren Gleichung $\gamma_i \to (a_i, b_i)$, d.h. $\gamma_i^2 + a_i\gamma_i + b_i = 0$ beachtet. Zum anderen ist

$$\begin{bmatrix} A' & A \\ C_i & B \end{bmatrix} = \frac{A'-B}{A-B}\frac{A-C_i}{A'-C_i} = \gamma_i \notin \mathfrak{K} \quad \text{und} \quad \begin{bmatrix} A' & A \\ C_1 & C_2 \end{bmatrix} = \frac{\gamma_1}{\gamma_2} \notin \mathfrak{K}$$

[15]) Man braucht sich nicht zu überzeugen, daß die benutzten Nenner regulär sind, da dort von vornherein ja nur reguläre Größen $B - C_i$, $B' - C_i'$ auftreten.

nach (a). Da der Büschelsatz gilt, muß also $C_1C_1'C_2C_2'$ ein konzyklisches Quadrupel sein. Beachtet man jetzt noch

$$\begin{bmatrix} A' & A \\ B' & B \end{bmatrix}\begin{bmatrix} A' & A \\ C_i & C_i' \end{bmatrix} = k\,\frac{b_i}{k} = b_i,$$

so folgt aus Hilfssatz 1

$$m = 1 - \frac{1}{b_2}\left(b_1\frac{\gamma_2}{\gamma_1} + b_2\frac{\gamma_1}{\gamma_2}\right) + \frac{b_1}{b_2} \in \mathfrak{R}$$

bzw. weiter, da $b_i \neq 0$ ist,

$$b_1\frac{\gamma_2}{\gamma_1} + b_2\frac{\gamma_1}{\gamma_2} \in \mathfrak{R}.$$

Damit ist also $\mathfrak{R}$ L-Ring in bezug auf $\mathfrak{K}$.

Literatur

[1] BENZ, W.: Axiomatischer Aufbau der Kreisgeometrie auf Grund von Doppelverhältnissen. J. reine angew. Math. **199**, 56–90 (1958). — [2] HOFFMAN, A. J.: Chains in the projective line. Duke Math. J. **18**, 827–830 (1951). — [3] PECZAR, L.: Über eine einheitliche Methode zum Beweis gewisser Schließungssätze. Mh. Math. **54**, 210–220 (1950). — [4] VAN DER WAERDEN, B. L., u. L. J. SMID: Eine Axiomatik der Kreisgeometrie und der Laguerre-Geometrie. Math. Ann. **110**, 753–776 (1935).

Mainz, Mathematisches Institut der Universität

(Eingegangen am 22. April 1958)