MATHEMATISCHE ZEITSCHRIFT

64. BAND, 2. HEFT

(ABGESCHLOSSEN AM 14. FEBRUAR 1956)

BERLIN · GÖTTINGEN · HEIDELBERG
SPRINGER - VERLAG
1956

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.

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 irgendmöglich, 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.

Springer-Verlag OHG — Berlin W 35, Reichpietschufer 20. — Heidelberg, Neuenheimer Landstraße 24. — Göttingen, Weender Straße 60.

64. Band **Inhalt** 2. Heft

Seite

Zeller, K., Über den perfekten Teil von Wirkfeldern 123
Karzel, H., Über eine Anordnungsbeziehung am Dreieck 131
Huppert, B., Über die Auflösbarkeit faktorisierbarer Gruppen. III 138
Putnam, C. R., A Note on Inverses of Differential Operators 149
Jurkat, W., und A. Peyerimhoff, Lokalisation bei absoluter Cesàro-Summierbarkeit von Potenzreihen und trigonometrischen Reihen. II. 151
Ribenboim, P., Sur une note de Nagata relative à un problème de Krull. 159
Behrens, E.-A., Zur additiven Idealtheorie in nichtassoziativen Ringen 169
Gaier, D., Über die Äquivalenz der $|B_k|$-Verfahren 183
Groot, J. de, A System of Continuous, Mutually Non-differentiable Functions. . . 192
Witt, E., Die Unterringe der freien Lieschen Ringe 195
Ebel, I., Analytische Bestimmung der Darstellungsanzahlen natürlicher Zahlen durch spezielle ternäre quadratische Formen mit Kongruenzbedingungen 217

ZELLER, K.
Math. Zeitschr. Bd. 64, S. 123—130 (1956)

Über den perfekten Teil von Wirkfeldern

Von

KARL ZELLER

1. Einleitung

Wir betrachten Limitierungsverfahren der Form $\lim_n \sum_k a_{nk} x_k$ und verwenden Definitionen, Bezeichnungen und Ergebnisse einer früheren Arbeit des Verfassers [1951], die mit AELV zitiert wird. Das Wirkfeld $\mathfrak{A}$ eines solchen Verfahrens läßt sich in natürlicher Weise als F-Raum („FK-Raum") auffassen. Ist A permanent oder konvergenztreu, enthält also $\mathfrak{A}$ die Menge $\mathfrak{S}_C$ der konvergenten Folgen, so interessiert die abgeschlossene Hülle $\overline{\mathfrak{S}}_C$ von $\mathfrak{S}_C$ in $\mathfrak{A}$ (im Sinne der genannten F-Topologie). Ist $\overline{\mathfrak{S}}_C = \mathfrak{A}$, so heißt A perfekt. Dementsprechend nennen wir $\overline{\mathfrak{S}}_C$ auch den perfekten Teil des Wirkfeldes und verwenden für $\overline{\mathfrak{S}}_C$ auch die Bezeichnung $\mathfrak{A}_P$, wenn die Abhängigkeit von $\overline{\mathfrak{S}}_C$ von $\mathfrak{A}$ betont werden soll. Perfekte Verfahren haben besonders angenehme Eigenschaften, vor allem in bezug auf Vergleichs- und Verträglichkeitssätze. Entsprechende Eigenschaften besitzt der perfekte Teil des Wirkfeldes. Es erhebt sich daher die Frage, ob und wie man diesen Teil absondern kann. In dieser Richtung beweisen wir folgendes allgemeine Ergebnis:

Satz. *Zu jedem permanenten Matrixverfahren A gibt es ein permanentes Matrixverfahren B, dessen Wirkfeld der perfekte Teil von $\mathfrak{A}$ ist.*

B ist dann übrigens perfekt und mit A verträglich. Beim Beweis (im zweiten Abschnitt) verwenden wir unter anderem einen Gedanken von J. D. HILL. Der Beweis zeigt auch, daß man bei zeilenfinitem A die Matrix B zeilenfinit wählen kann.

Wir kommen dann im dritten Abschnitt auf Beispiele zu sprechen, in denen schon die Abtrennung des perfekten Teils gelungen ist oder bei denen der perfekte Teil gewisse ausgezeichnete Eigenschaften besitzt. Und zwar behandeln wir: Einfolgenverfahren, HUNTEMANN-Verfahren, Vergleichssätze mit Nebenbedingungen, Vergleich stetiger und unstetiger Verfahren desselben Typs, Indexverschiebung, MERCER-Sätze. Aus den Beispielen geht auch hervor, daß der perfekte Teil eine komplizierte Struktur haben kann, so daß unser Satz sicher nicht trivial ist.

Für diese Arbeit erhielt ich wertvolle Anregungen auf der Limitierungstagung in Oberwolfach (März 1955). Besonders bin ich Herrn D. GAIER und Herrn H. SALZMANN zu Dank verpflichtet.

2. Beweis des Satzes

Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß A keine leeren Spalten hat. Das Nullwirkfeld $\mathfrak{A}_0$ (die Menge der zu Null limitierten Folgen) ist dann ein FK-Raum mit den Halbnormen

$$p_{-1}(\mathfrak{x}) = \sup_{m=0,1,..}\left|\sum_{k=0}^{\infty} a_{mk}\, x_k\right|, \qquad p_n(\mathfrak{x}) = \sup_{l=0,1,..}\left|\sum_{k=0}^{l} a_{nk}\, x_k\right| \qquad (n=0,1,\ldots)$$

(AELV, Satz 5.1).

Für jedes feste $m = -1, 0, \ldots$ fassen wir ferner $\mathfrak{A}_0$ als normierten Raum $\mathfrak{A}_0^m$ mit der Norm $p_{-1}(\mathfrak{x}) + \cdots + p_m(\mathfrak{x})$ auf. Es stört dabei nicht, daß in gewissen Fällen diese Norm auch für andere Elemente als das Nullelement verschwindet. $\mathfrak{D}^m$ sei die Menge der $\mathfrak{x} \in \mathfrak{A}_0$, die in $\mathfrak{A}_0^m$ nicht Berührpunkt von $\mathfrak{S}_N$ (Menge der Nullfolgen) sind. $\mathfrak{D}^m$ ist separabel, da $\mathfrak{A}_0$ bezüglich jeder Halbnorm p_i separabel ist. Es gibt also abzählbar viele Punkte $\mathfrak{x}_i \in \mathfrak{D}^m$, die in $\mathfrak{D}^m$ dicht liegen (im Sinne der genannten Norm). Wir wählen stetige Linearformen f_i in $\mathfrak{A}_0^m$ mit

$$\begin{aligned} |f_i(\mathfrak{x})| &\leq p_{-1}(\mathfrak{x}) + \cdots + p_m(\mathfrak{x}) && (\mathfrak{x} \in \mathfrak{A}_0^m),\\ f_i(\mathfrak{x}) &= 0 && (\mathfrak{x} \in \mathfrak{A}_0^m,\ \mathfrak{x} \notin \mathfrak{D}^m),\\ f_i(\mathfrak{x}_i) &= \text{Abstand von } \mathfrak{x}_i \text{ zu } \mathfrak{S}_N \text{ in } \mathfrak{A}_0^m. \end{aligned}$$

Aus den f_i bilden wir eine Folge g_j, in der jedes f_i und jedes $-f_i$ unendlich oft vorkommt. $\lim_j g_j(\mathfrak{x})$ existiert genau dann, wenn $\mathfrak{x}\,(\in \mathfrak{A}_0)$ nicht zu $\mathfrak{D}^m$ gehört (vgl. HILL [1950]).

Dies führen wir für jedes m durch. Die so erhaltenen Linearformen ordnen wir zu einer Folge h_j an. Ist $\mathfrak{D}$ die Menge der $\mathfrak{x}$, die im F-Raum $\mathfrak{A}_0$ nicht Berührpunkt von $\mathfrak{S}_N$ sind ($\mathfrak{D}$ also das Komplement von $\overline{\mathfrak{S}}_N$), so gilt $\mathfrak{D} = \bigcup \mathfrak{D}^m$ (vgl. AELV, S. 469). Somit gilt folgendes:

$$h_j(\mathfrak{x}) = 0 \qquad (\mathfrak{x} \notin \mathfrak{D},\ \mathfrak{x} \in \mathfrak{A}_0,\ j = 0, 1, \ldots),$$
$$h_i(\mathfrak{x}) \text{ divergiert } (\mathfrak{x} \in \mathfrak{D}).$$

Jedes $h(\mathfrak{x})$ gestattet eine Zerlegung (AELV, S. 468)

$$h(\mathfrak{x}) = h^{\wedge}(\mathfrak{x}) + h^{\vee}(\mathfrak{x})$$

mit

$$|h^{\wedge}(\mathfrak{x})| \leq p_{-1}(\mathfrak{x}), \qquad |h^{\vee}(\mathfrak{x})| \leq p_0(\mathfrak{x}) + \cdots + p_m(\mathfrak{x}).$$

Nach AELV, S. 476, gelten Darstellungen

$$h^{\wedge}(\mathfrak{x}) = \sum_{n=0}^{\infty} \beta_n\, y_n \quad \text{mit} \quad \sum |\beta_n| \leq 1,$$

$$h^{\vee}(\mathfrak{x}) = \sum_{k=0}^{\infty} \alpha_k\, x_k.$$

Wegen $h(\mathfrak{x}) = 0$ für $\mathfrak{x} \notin \mathfrak{D}$ ist

$$\sum\nolimits_n \beta_n\, a_{nk} + \alpha_k = 0 \qquad (k = 0, 1, \ldots),$$

somit, da A beschränkte Zeilennormen, etwa $\leq K$ hat,

$$\sum |\alpha_k| \leq K.$$

Wir approximieren $h(\mathfrak{x})$ durch

$$C(\mathfrak{x}) = \sum_{n=0}^{m} \beta_n y_n + \sum_{k=0}^{\infty} \alpha_k x_k = \sum_{k=0}^{\infty} \gamma_k x_k,$$

wobei wir $m = m(j)$ so wählen, daß $h_j(\mathfrak{x}) - C_j(\mathfrak{x}) \to 0$ geht für jedes $\mathfrak{x} \in \mathfrak{A}_0$. Aus dem Voranstehenden folgt

$$\sum |\gamma_k| \leq 2K.$$

Die Folge $C_j(\mathfrak{x})$ konvergiert nun für $\mathfrak{x} \in \mathfrak{A}_0$, $\mathfrak{x} \notin \mathfrak{D}$, und divergiert für $\mathfrak{x} \in \mathfrak{D}$.

Die gesuchte Matrix B erhalten wir durch die Bedingungen

$$\mathfrak{b}_{2n} = \mathfrak{a}_n$$
$$\mathfrak{b}_{2n+1} = \mathfrak{c}_n + \Theta_n \mathfrak{a}_n,$$

wo $\mathfrak{a}_n$ bzw. $\mathfrak{b}_n$ die Zeilen von A bzw. B sind, und die Zeilen $\mathfrak{c}_n$ aus den Koeffizienten der Linearformen $C_n(\mathfrak{x})$ gebildet werden; ferner wählen wir dabei die Θ_n so, daß die Zeilensummen der Matrix B gegen Eins streben. Die Θ_n bilden eine beschränkte Zahlenfolge, weil die Zeilensummen von A gegen Eins streben und weil unabhängig von n für jede Linearform $C_n(\mathfrak{x})$ die Ungleichung $\sum |\gamma_k| \leq 2K$ gilt.

Man sieht: B limitiert die Folge 1, 1, ... zum Werte Eins (weil die Zeilensummen gegen Eins streben); B limitiert nur Folgen, die $\mathfrak{A}$ angehören (wegen der Zeilen $\mathfrak{a}_n$); ist $\mathfrak{x} \in \mathfrak{A}_0$, $\mathfrak{x} \notin \mathfrak{D}$, so wird $\mathfrak{x}$ limitiert zum Werte Null (weil dann $C_n(\mathfrak{x}) \to 0$ geht, und weil die Θ_n beschränkt sind, so daß der Beitrag von $\Theta_n \mathfrak{a}_n$ ebenso wie der von $\mathfrak{a}_n$ gegen Null geht); ist $\mathfrak{x} \in \mathfrak{D}$, so wird $\mathfrak{x}$ nicht limitiert (da wieder der Beitrag von $\Theta_n \mathfrak{a}_n$ gegen Null geht, wogegen $C_n(\mathfrak{x})$ divergiert). Da jedes $\mathfrak{x} \in \mathfrak{S}_N$ zwar $\mathfrak{A}_0$, aber nicht $\mathfrak{D}$ angehört, wird insbesondere jedes solche $\mathfrak{x}$ von B limitiert (zu Null). Aus diesen Bemerkungen liest man die Permanenz von B und die übrigen behaupteten Eigenschaften ab.

Als weiteres Ergebnis aus unserem Ideenkreis sei genannt: Es gibt ein konvergenzgleiches Matrixverfahren, das gewisse unbeschränkte Folgen in beschränkte transformiert. Dies widerlegt Vermutung 1 (d) aus Wilansky-Zeller [1955]. Der Beweis erfolgt am leichtesten mit Einfolgenverfahren, für Verallgemeinerungen zieht man die eben beschriebene Methode heran.

Vielleicht führt beim Beweis des Satzes auch die vom Verfasser [1953, S. 272—274], [1954, S. 345] angewandte Methode zum Ziel.

Allgemeiner kann man fragen, welche separablen FK-Räume als Wirkfelder eines Matrixverfahrens dargestellt werden können. Dies ist noch nicht geklärt. Eine Einschränkung ergibt sich schon dadurch, daß der Dual eines Wirkfeldes separabel ist.

3. Beispiele

a) Einfolgenverfahren. Im Rahmen der Untersuchung des perfekten Teils eines Wirkfeldes, also der abgeschlossenen Hülle von $\mathfrak{S}_C$ im F-Raum $\mathfrak{A}$, interessieren die beiden möglichen Extremfälle, nämlich $\overline{\mathfrak{S}}_C = \mathfrak{A}$ (perfektes Verfahren, s. oben) und $\overline{\mathfrak{S}}_C = \mathfrak{S}_C$. Letzteres tritt auch bei nicht konvergenzgleichen Verfahren, also bei $\mathfrak{A} \neq \mathfrak{S}_C$, auf; die Abspaltung des perfekten Teiles ist dann trivial. Die einfachsten Beispiele werden gegeben durch die „Einfolgenverfahren", die im wesentlichen nur eine divergente Folge d_k limitieren, was genauer heißen soll, daß das Wirkfeld aus den Folgen der Form $a \cdot d_k +$ konvergente Folge besteht (MAZUR [1928], DAREVSKY [1946]). Jedoch gibt es auch kompliziertere Verfahren mit $\overline{\mathfrak{S}}_C = \mathfrak{S}_C$, wie folgende Ergebnisse von WILANSKY-ZELLER [1955] zeigen:

Sind endlich viele Folgen gegeben, die über der Menge der beschränkten Folgen linear unabhängig sind, so existiert ein permanentes Verfahren, das im wesentlichen nur diese Folgen limitiert. Sind abzählbar viele Folgen mit derselben Unabhängigkeitseigenschaft gegeben, so existiert ein permanentes Verfahren, das diese Folgen, aber keine beschränkt-divergenten Folgen limitiert. Ein konvergenztreues Verfahren limitiert genau dann keine beschränkt-divergente Folge, wenn der perfekte Teil des Wirkfeldes gleich $\mathfrak{S}_C$ ist.

Das letztgenannte Ergebnis zeigt, daß die vorher konstruierten Verfahren minimalen perfekten Teil besitzen; außerdem ist es z.B. für den Beweis von Lückenumkehrsätzen wichtig. Das erste Resultat ermöglicht, Wirkfelder um wenige Folgen zu vergrößern, wobei der perfekte Teil ungeändert bleibt. Das zweite zeigt, daß der perfekte Teil von unendlichem Defekt im Wirkfeld sein kann. Allgemeiner kann auch bei Verfahren mit $\overline{\mathfrak{S}}_C \neq \mathfrak{S}_C$ der perfekte Teil unendlichen Defekt haben; und eben hier tritt die Hauptschwierigkeit bei der Abtrennung des perfekten Teils auf. Ist dieser hingegen von endlichem Defekt, so kann die Isolierung einfacher als im allgemeinen Satz durchgeführt werden.

Einfolgenverfahren gestatten die Aufstellung von „Gegenbeispielen" bei Fragen über Verträglichkeit, Vergleich, Indexverschiebung, Umkehrbedingungen usw. Einfache Beispiele von Einfolgenverfahren stellen die Matrizen

$$\begin{pmatrix} a_0 & & & 0 \\ b_1 & a_1 & & \\ & b_2 & a_2 & \\ 0 & & & \ddots \end{pmatrix}$$

mit $\lim (a_k + b_k) = 1$, $\overline{\lim}\, |a_k| < \underline{\lim}\, |b_k| < \infty$ dar; durch Produktbildung von n Matrizen erhält man „n-Folgenverfahren" (ZELLER [1950], [1953]). Dies leitet zu den HUNTEMANN-Verfahren über, bei denen solche Matrizen auftreten.

b) HUNTEMANN-Verfahren. So nennen wir die Verfahren, die den Matrizen der Form $b_{nk} = a_{n-k}$ $(k \leq n)$, $b_{nk} = 0$ sonst, zugeordnet sind. (HUNTEMANN [1938] und andere Autoren betrachten allerdings nur den Fall, daß fast alle a_p verschwinden.) Wir stellen zunächst einige Grundeigenschaften dieser Verfahren zusammen (vgl. SILVERMAN-SZÁSZ [1944]).

Die HUNTEMANN-Verfahren bilden ein System vertauschbarer Matrizen, das ein gewisses Gegenstück zu dem der HAUSDORFF-Verfahren darstellt. Vertauschbarkeit mit der Summationsmatrix S ($n+1$ Einsen in der n-ten Zeile) bewirkt, daß RR- und FF-Form gleich sind, und daß absolute Permanenz gleichbedeutend mit gewöhnlicher Permanenz ist. Indexverschiebung ist ohne weiteres möglich. Jedem Verfahren wird die (unter Umständen formale) Potenzreihe $a(z) = \sum a_k z^k$ zugeordnet. Das Produkt zweier Matrizen entspricht dem CAUCHY-Produkt der Potenzreihen. Nullstellen und Singularitäten von $a(z)$ sind entscheidend für die Wirksamkeit des Verfahrens. Einer Funktion $a(z) = (z - z_0)$ entspricht ein Verfahren, das für $|z_0| < 1$ Einfolgenverfahren, für $|z_0| > 1$ konvergenzgleich, und für $|z_0| = 1$ perfekt mit leicht zu überschauendem Wirkfeld ist.

Produkt- und Partialbruchzerlegung gestatten nun oft eine einfache Darstellung des Wirkfeldes und die Abspaltung des perfekten Teils. Für den Fall, daß $a(z)$ ein Polynom ohne Nullstellen vom Betrag Eins ist, erhält man ein „n-Folgenverfahren" (PETERSEN [1952]). Aber auch bei Polynomen mit Nullstellen auf dem Einheitskreis hat das Wirkfeld noch einen einfachen Aufbau, insbesondere kann man den perfekten Teil erhalten, indem man das zu dem Polynom mit den betreffenden Nullstellen vom Betrag Eins gehörige Verfahren bildet. Die Zerlegung geht teilweise auch für Nichtpolynome $a(z)$. Schwierigkeiten bereitet allerdings die Möglichkeit unendlich vieler Nullstellen im Einheitskreis, was auch bei permanenten Verfahren $\left(\sum |a_k| < \infty,\ \sum a_k = 1\right)$ vorkommen kann; man erhält dann wieder ein Verfahren, dessen perfekter Teil unendlichen Defekt besitzt. Überhaupt ist der Zusammenhang zwischen wesentlichen Singularitäten von $a(z)$ und dem Wirkfeld des Verfahrens noch nicht geklärt.

Noch einige Bemerkungen am Rande. Die von HUNTEMANN [1938] durchgeführte Summierung von Potenzreihen meromorpher Funktionen $f(z)$ läßt sich in diesem Zusammenhang auch leicht erklären: Soll etwa $f(z)$ im Punkte 1 summiert werden, so wählt man ein Polynom $a(z)$ mit $a(1) = 1$, so daß $a(z) f(z)$ in $|z| \leq 1$ regulär ist. Das zu $a(z)$ gehörige Verfahren führt die gewünschte Summierung durch. — Allgemeiner kann man Verfahren der Form $D_1 H D_2$ (D_i = Diagonalmatrizen, H = HUNTEMANN-Matrix) betrachten; damit gelangt man zu Anwendungen auf NÖRLUND-Verfahren, unter anderem zu naheliegenden Verallgemeinerungen des Vergleichssatzes von RIESZ [1923]. — So wie bei HUNTEMANN-Verfahren die Nullstellen von Polynomen wichtig sind, spielen bei anderen Verfahren die Nullstellen von LAPLACE-, FOURIER- oder MELLIN-Transformierten eine Rolle. — Man vergleiche auch die Untersuchungen über Summengleichungen, bei denen man ähnliche Ergebnisse wie die obigen für HUNTEMANN-Verfahren erhalten hat; s. etwa PAASCHE [1954].

c) Vergleichssätze mit Nebenbedingungen. Für manche Verfahren A und B sind Aussagen folgender Form bekannt: A und B sind gleich stark bezüglich aller Folgen s_k mit $s_k = o(d_k)$. Die vorausgegangenen Resultate können die Vermutung erwecken, daß dann A und B im perfekten Teil übereinstimmen, wenn nur d_k genügend rasch wächst. Man erhält jedoch nur schwache Ergebnisse in dieser Richtung, etwa: Gilt für das Verfahren A die „beste Größenordnungsbedingung" $s_k = o(d_k)$ und stimmen A und B für $s_k = O(d_k)$ überein, so haben beide Wirkfelder denselben perfekten Teil. — Daß sich allgemein nicht mehr aussagen läßt, zeigen die verschieden starken perfekten Verfahren C_1 und ZC_1 (C_1 = CEÀSRO-Verfahren, Z = Zweierverfahren), die innerhalb der von C_1 gegebenen Größenordnung $s_k = o(k)$ gleich stark sind. — Die Frage nach besseren Aussagen unter Einschränkungen über die zugelassenen Matrizen bleibt offen.

Trotzdem wird man bei bekannten Vergleichssätzen mit Nebenbedingungen untersuchen, ob die betreffenden Verfahren denselben perfekten Teil haben. Dies führt uns zum Vergleich von stetigen und unstetigen Verfahren desselben Typs, bei denen ja oft Einschließungssätze des genannten Typs vorliegen.

d) Stetige und unstetige Verfahren. Die Wirkfelder von Matrixverfahren a_{xk} mit stetigem Parameter x (etwa für $x \to \infty$) sind meistens auch FK-Räume, so daß in solchen Wirkfeldern (etwa beim RIESZ-, ABEL-, BOREL-Verfahren) der perfekte Teil ebenfalls erklärt ist. Varianten dieser Verfahren ergeben sich, wenn man x nicht stetig, sondern nur durch eine gewisse Folge x_n gegen den Grenzwert gehen läßt. Wir unterscheiden zwei Hauptfälle: Für eine genügend dichte Wahl der x_n sind das stetige und das unstetige Verfahren äquivalent; oder dies tritt für keine Folge $\{x_n\}$ ein.

Der erste Fall liegt z.B. bei den RIESZ-Mitteln $R(\lambda, p)$ vor und bietet den Vorteil, daß man nur noch gewöhnliche Matrixverfahren a_{nk} (die man für verschiedene Wahl der x_n erhält) vergleichen muß, da das stetige Verfahren eben durch ein gewöhnliches dargestellt wird. Nähere Untersuchungen galten vor allem den Mitteln $R(n, p)$ mit $x_n = n$ (RIESZ [1923], AGNEW [1933], COOKE [1950]). Die Resultate beruhen großenteils darauf, daß man die Vermittlungsmatrix zwischen den C_p-Mitteln σ_n [C_p ist ja $R(n, p)$ äquivalent] und den unstetigen RIESZ-Mitteln („R_p^*-Mitteln") τ_n, also zwischen

$$\sigma_n = \binom{n+p}{n}^{-1} \sum_{k=0}^{n} \binom{n-k+p}{n-k} u_k \quad \text{und} \quad \tau_n = \sum_{k=0}^{n} \left(\frac{n+1-k}{n+1}\right)^p u_k$$

fast ohne Rechnung bestimmen kann. Und zwar erhält man eine Matrix der Form DHD^*, wo die D Diagonalmatrizen sind und H ein HUNTEMANN-Verfahren ist, das für $p = 1, 2, 3, \ldots$ bzw. zu den Polynomen

$$1,\ 1+z,\ 1+4z+z^2,\ 1+11z+11z^2+z^3,\ 1+26z+66z^2+26z^3+z^4,$$
$$1+57z+302z^2+302z^3+57z^4+z^5, \text{ usw.}$$

gehört. Herr PEYERIMHOFF hat neuerdings die Nullstellen mehrerer solcher Polynome bestimmt und damit näheren Aufschluß über das Verhältnis von

C_p und R_p^* gewonnen (RIESZ beschränkte sich auf die Fälle $p=1, 2, 3$). Da die Koeffizienten dieser Polynome sich leicht explizit darstellen lassen, besteht die Hoffnung auf einen Überblick über die Nullstellen aller dieser Polynome. Soweit man bis jetzt sieht, stimmen der perfekte Teil von C_p und R_p^* für ungerades p überein, für gerades p nicht. Analog kann man andere Varianten der RIESZ-Mittel behandeln, z.B. die R_p^{**}-Mittel, die man erhält, indem man in der Summe für τ_n das letzte Glied ($k=n$) wegläßt. Man erhält die Polynome (für $p=1, 2, \ldots$)

$$2-z,\ 4-3z+z^2,\ 8-5z+4z^2-z^3,\ 16+z+11z^2-5z^3+z^4, \text{ usw.}$$

In den bisher bekannten Fällen sind R_p^{**} und C_p äquivalent, woraus sofort die Äquivalenz von R_p^* und C_p für $u_k=o(k^p)$ folgt. Letzteres kann man auch wie oben bei ZC_1 einsehen.

Im zweiten Hauptfall (s. oben), der z.B. beim BOREL-Verfahren eintritt, treten noch schwierigere Probleme auf. Ein erster Ansatzpunkt ist die Frage, ob eine Folge, die beim Grenzübergang $x_n \to \infty$ limitiert wird, dargestellt werden kann als Summe zweier Folgen, von denen die eine beim Grenzübergang $x \to \infty$ limitiert wird, während die Transformierte der andern in allen x_n verschwindet. Näheres über unstetige BOREL-Verfahren findet man bei GAIER [1955].

Die Untersuchung des BOREL-Verfahrens führt uns weiter zu Fragen der Indexverschiebung.

e) Indexverschiebung. Beim BOREL-Verfahren wurde festgestellt (GAIER [1954], ZELLER [1954]), daß die Folgen s_k mit $s_k=O(R^k)$ (R beliebig) Indexverschiebung gestatten und dem perfekten Teil angehören. Beim TAYLOR-Verfahren (MEYER-KÖNIG/ZELLER [1954]) wird der perfekte Teil von allen regulär summierbaren Folgen gebildet. Indexverschiebung ist nur bei gewissen singulär summierbaren Folgen (also Folgen, die nicht dem perfekten Teil angehören) nicht gestattet. Diese Folgen können überdies noch näher durch eine HUNTEMANN-Transformation charakterisiert werden (s. in der genannten Arbeit auf S. 350), die für $0<\alpha<1/2$ ein Einfolgenverfahren ist. Dies und die Resultate von AGRANOVIC [1954] deuten auf einen Zusammenhang zwischen Perfektheit und Indexverschiebung hin. Allerdings dürfte dieser Zusammenhang kein ganz einfacher sein, da es perfekte Verfahren gibt, die Indexverschiebung nicht allgemein gestatten.

f) Sonstiges. Bei MERCER-Sätzen mit Parameter (z.B. HARDY [1949], Satz 52) treten ebenfalls Einfolgenverfahren auf.

Zusammenfassend können wir feststellen: Wenn auch nichtperfekte Verfahren, insbesondere Einfolgenverfahren, für die Limitierung nicht besonders geeignet erscheinen, so stößt man doch bei allen möglichen Problemen auf solche Verfahren. Es lohnt sich daher, ihre Eigenschaften näher zu untersuchen und insbesondere den perfekten Teil des Wirkfeldes abzuspalten. Diese Abtrennung wird zwar allgemein durch unseren Satz geliefert. Für spezielle Verfahren müssen jedoch immer Einzeluntersuchungen durchgeführt werden, sei es um die im Satz gebrauchten Linearformen zu bestimmen, sei es um die Abtrennung auf einfacherem Wege durchzuführen. Ist der perfekte Teil isoliert, so erhebt sich die Frage, ob er günstigere Eigenschaften (etwa bezüglich Indexverschiebung) als das ganze Wirkfeld hat. Besonders lohnend erscheint die Untersuchung der perfekten Teile zweier Verfahren, für die bereits ein Einschließungssatz mit Zusatzbedingungen bekannt ist; gelegentlich werden diese Verfahren denselben perfekten Teil besitzen.

Literatur

(F = Fortschritte der Mathematik, R = Mathematical Reviews, Z = Zentralblatt für Mathematik.)

Agnew, R. P.: On Riesz and Cesàro methods of summability. Trans. Amer. Math. Soc. **35**, 532—548 (1933). F **59**, 971; Z **6**, 345. — Agranovic, M. S.: On consistency of some methods of summation. Uspehy Matem. Nauk **9** (61), 242 (1954). — Cooke, R. G.: Infinite Matrices and Sequence Spaces. London 1950. 347 S. R **12**, 694; Z **40**, 25. — Darevsky, V.: On intrinsically perfect methods of summation. Bull. Acad. Sci. URSS., Sér. Math. **10**, 97—104 (1946). R **7**, 517. — Gaier, D.: Zur Frage der Indexverschiebung beim Borel-Verfahren. Math. Z. **58**, 453—455 (1953). R **15**, 214; Z **50**, 284. — On modified Borel methods. Proc. Amer. Math. Soc. **1955**. — Hardy, G. H.: Divergent Series. Oxford 1949. 396 S. R **11**, 25; Z **32**, 58. — Hill, J. D.: Summability methods weaker than convergence. Amer. J. Math. **72**, 621—623 (1950). R **12**, 20; Z **38**, 213. — Huntemann, H.: Über den Wert der Reihenentwicklung meromorpher Funktionen bei linearen Summierungsverfahren. Dtsch. Math. **3**, 390—402 (1938). F **64**, 1003; Z **19**, 162. — Mazur, S.: Über lineare Limitierungsverfahren. Math. Z. **28**, 599—611 (1928). F **54**, 235. — Meyer-König, W., u. K. Zeller: Über das Taylorsche Summierungsverfahren. Math. Z. **60**, 348—352 (1954). R **16**, 28. — Paasche, I.: Über das Verhalten der Integrale homogener und inhomogener Summengleichungen im Unendlichen. München u. Düsseldorf 1954. 59 S. — Petersen, G. M.: A note on divergent series. Canad. J. Math. **4**, 445—454 (1952). R **14**, 368; Z **47**, 299. — Riesz, M.: Sur l'équivalence de certaines méthodes de sommation. Proc. Lond. Math. Soc. (2) **22**, 412—419 (1923). F **50**, 154. — Silverman, L. L., and O. Szász: On a class of Nörlund matrices. Ann. of Math. (2) **45**, 347—357 (1944). R **5**, 236. — Wilansky, A., and K. Zeller: Summability of bounded divergent sequences; topological methods. Trans. Amer. Math. Soc. **1955**. — Zeller, K.: Allgemeine Eigenschaften von Matrixtransformationen. Diss. Tübingen 1950. — Allgemeine Eigenschaften von Limitierungsverfahren. Math. Z. **53**, 463—487 (1951). R **12**, 604. — Merkwürdigkeiten bei Matrixverfahren; Einfolgenverfahren. Arch. Math. **4**, 1—5 (1953). R **14**, 866. — Über die Darstellbarkeit von Limitierungsverfahren mittels Matrixtransformationen. Math. Z. **59**, 271—277 (1953). R **15**, 618. — Matrixtransformationen von Folgenräumen. Univ. Roma. Ist. Naz. Alta Mat. Rend. Mat. e Appl. (5) **12** (1953), 340—346 (1954). R **15**, 618.

Tübingen, Mathematisches Institut der Universität

(Eingegangen am 18. April 1955)

KARZEL, H.
Math. Zeitschr. Bd. 64, S. 131—137 (1956)

Über eine Anordnungsbeziehung am Dreieck

Herrn E. SPERNER zum 50. Geburtstag am 9. Dezember 1955

Von
HELMUT KARZEL

Die von E. SPERNER [2][1]) eingeführten *Ordnungsfunktionen* haben sich in der Geometrie bei der Untersuchung von Anordnungsfragen als sehr nützlich erwiesen. Unter einer *Ordnungsfunktion* versteht man in einer ebenen Geometrie *jede eindeutige Funktion* $h(\alpha)$, *die jedem Elementepaar* α (= Punkt), h (= Gerade) *der Geometrie einen der Werte* $0, +1, -1$ *so zuordnet, daß der Wert* 0 *genau dann angenommen wird, wenn das betreffende Elementepaar inzidiert.* Wie SPERNER [2] gezeigt hat, entspricht *jeder* Ordnungsfunktion eine gemischte *Zwischen-* und *Trennbeziehung* der Geometrie[2]) und umgekehrt läßt sich jede Zwischen- und Trennbeziehung, sofern sie gewissen Bedingungen genügt, durch eine geeignete Ordnungsfunktion beschreiben. Ist jedoch $h(\alpha)$ eine beliebige Ordnungsfunktion, so weisen die durch sie erklärten Anordnungsbeziehungen noch wenige der von einer geometrischen Anordnung gewohnten Eigenschaften auf. So läßt sich mit einer beliebigen Ordnungsfunktion weder ein Zwischen- noch Trennbegriff für Punkte allein oder Geraden allein erklären. Dies ist erst dann gewährleistet, wenn die Ordnungsfunktion der sog. *Geradenrelation* genügt, d.h. der Forderung: *Sind* α, β, γ *drei beliebige voneinander verschiedene Punkte einer Geraden* k *und* g, h *zwei beliebige Geraden* $\neq k$, *die mit* γ *inzidieren, so soll stets* $g(\alpha)\, g(\beta)\, h(\alpha)\, h(\beta) = 1$ *gelten.* — Aus diesem Grunde gebraucht SPERNER fast ausschließlich Ordnungsfunktionen, die der Geradenrelation genügen.

Ist nun $h(\alpha)$ eine beliebige Ordnungsfunktion, die der Geradenrelation genügt, so läßt sich folgende Anordnungsaussage an jedem Dreieck machen: *Sind* α, β, γ *drei beliebige Punkte in allgemeiner Lage und* a, b, c *drei Geraden, so daß die Schnittpunkte* (a, b), (b, c), (a, c)[3]) *jeweils mit den Dreiecksseiten* (α, β), (β, γ), (α, γ) *inzidieren, ohne mit einem der Punkte* α, β, γ *zusammen-*

[1]) Die Zahlen in eckigen Klammern verweisen auf die Nummern des Literaturverzeichnisses auf S. 137.

[2]) Ist $h(\alpha)$ eine Ordnungsfunktion, so läßt sich nämlich erklären: Die Gerade h liegt genau dann *zwischen* den Punkten α, β, wenn $h(\alpha)\, h(\beta) = -1$ gilt, und der Punkt α liegt genau dann *zwischen* den Geraden g, h, wenn $g(\alpha)\, h(\alpha) = -1$ gilt. Zwei Geraden g, h und zwei Punkte α, β *trennen* sich, wenn $g(\alpha)\, g(\beta)\, h(\alpha)\, h(\beta) = -1$ gilt.

[3]) Sind $a \neq b$ zwei Geraden bzw. $\alpha \neq \beta$ zwei Punkte, so soll mit (a, b) stets der Schnittpunkt der Geraden a, b bzw. mit (α, β) die Verbindungsgerade der Punkte α, β bezeichnet werden.

zufallen (s. Fig. 1), *so gilt die folgende Relation:*

$$a(\beta)\,a(\gamma)\,b(\alpha)\,b(\gamma)\,c(\alpha)\,c(\beta)=1,$$

die wir die *Dreiecksrelation* nennen wollen.

Diese Dreiecksrelation läßt sich aus folgenden Gleichungen, die auf Grund der Geradenrelation gelten, durch Multiplizieren sofort ausrechnen [man beachte hierbei, daß für nichtinzidente Elementepaare stets $(h(\alpha))^2=1$ ist]:

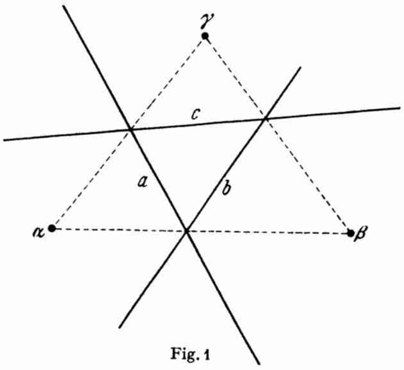

Fig. 1

$$a(\alpha)\,a(\gamma)\,c(\alpha)\,c(\gamma)=1$$
$$a(\alpha)\,a(\beta)\,b(\alpha)\,b(\beta)=1$$
$$b(\beta)\,b(\gamma)\,c(\beta)\,c(\gamma)=1.$$

Herrn SPERNER verdanke ich die folgende Frage, die in dieser Note untersucht werden soll:

Genügt umgekehrt eine Ordnungsfunktion, die die Dreiecksrelation erfüllt, der Geradenrelation?

Wir werden sehen, daß diese Frage unter gewissen zusätzlichen Voraussetzungen positiv zu beantworten ist (s. Satz).

Voraussetzungen

Die Geometrie sei eine *projektive Ebene Π*, in der der *kleine* Satz von DESARGUES gilt[4]) und in der jede Gerade mit mindestens vier verschiedenen Punkten inzidiert, d. h. die kleinste projektive Ebene, die bekanntlich aus genau sieben Punkten und sieben Geraden besteht, wird ausgeschlossen[5]).

Bezüglich einer festen Ordnungsfunktion $h(\alpha)$ definieren wir: *Genau dann, wenn α, β, γ drei voneinander verschiedene Punkte einer Geraden k sind und wenn für alle mit γ inzidierenden Geradenpaare $g, h \neq k$ die Geradenrelation $g(\alpha)\,g(\beta)\,h(\alpha)\,h(\beta)=1$ erfüllt ist, wird der Term $[\alpha,\beta|\gamma]$ erklärt, und zwar als 1, wenn $g(\alpha)\,g(\beta)=1$ und als -1, wenn $g(\alpha)\,g(\beta)=-1$ ist, wobei $g\neq k=(\alpha,\beta)$ eine beliebige mit γ inzidierende Gerade ist.*

Wir nennen daher den Term $[\alpha,\beta|\gamma]$ auch *Zwischensymbol*, da man erklären kann: γ liegt zwischen bzw. nicht zwischen α,β, wenn $[\alpha,\beta|\gamma]=-1$ bzw. $=+1$ ist. Dual ist der Term $[g,h|k]$ für drei voneinander verschiedene Geraden eines Punktes erklärt. — Ist $h(\alpha)$ eine beliebige Ordnungsfunktion,

---

[4]) Unter dem *kleinen* Satz von DESARGUES versteht man bekanntlich die Aussage: *Sind α,β,γ und α',β',γ' zwei perspektiv liegende Dreiecke mit dem Zentrum ζ und schneiden sich zwei der entsprechenden Seitenpaare (α,β), (α',β'); (α,γ), (α',γ') und (β,γ), (β',γ') auf einer Geraden durch ζ, so auch das dritte Seitenpaar.*

[5]) Für diese Geometrie gilt nämlich: Ist α,β,γ ein Dreieck, so gibt es genau eine Gerade, die mit keinem der Punkte α,β,γ inzidiert. Die Dreiecksrelation ist daher für jede Ordnungsfunktion dieser Geometrie, d.h. auch für solche, die nicht der Geradenrelation genügen, trivialerweise erfüllt. (Der Satz läßt sich für diese Geometrie nicht beweisen.)

so braucht es weder drei Punkte α, β, γ mit $[\alpha, \beta | \gamma]$ noch drei Geraden g, h, k mit $[g, h | k]$ zu geben.

Wie man leicht nachrechnet, gilt für Zwischensymbole folgende Regel:

$$[\alpha, \beta | \gamma] \cdot [\alpha, \delta | \gamma] = [\beta, \delta | \gamma], \tag{1}$$

$$[g, h | k] \cdot [g, j | k] = [h, j | k], \tag{2}$$

d.h. mit $[\alpha, \beta | \gamma]$, $[\alpha, \delta | \gamma]$ stehen auch die Punkte β, γ, δ in der Beziehung $[\beta, \delta | \gamma]$ und mit $[g, h | k]$, $[g, j | k]$ auch $[h, j | k]$.

Jetzt kann man folgenden Satz aussprechen, der eine Antwort auf die oben gestellte Frage geben soll:

Satz. *Eine Ordnungsfunktion $h(\alpha)$, die der Dreiecksrelation genügt, erfüllt die Geradenrelation, wenn es mindestens drei Punkte $\alpha_1, \alpha_2, \alpha_3$ mit $[\alpha_1, \alpha_2 | \alpha_3]$ oder wenn es mindestens drei Geraden a_1, a_2, a_3 mit $[a_1, a_2 | a_3]$ gibt.*

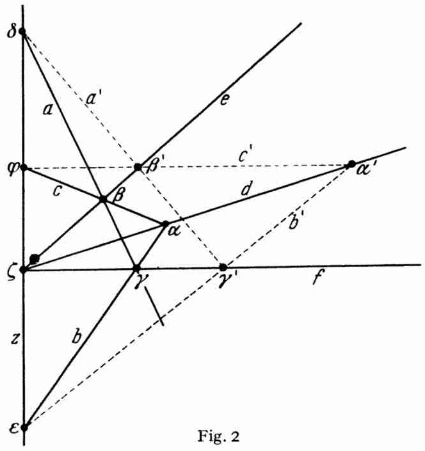

Fig. 2

Für den Beweis dieses Satzes genügt es, zu zeigen, daß für alle Punktetripel α, β, γ, deren Punkte voneinander verschieden sind und die auf einer Geraden liegen, $[\alpha, \beta | \gamma]$ gilt oder daß für alle Geradentripel g, h, k, deren Geraden voneinander verschieden sind und mit einem Punkt inzidieren, $[g, h | k]$ gilt. — Zuvor beweisen wir zwei Hilfssätze. Setzt man für eine feste Ordnungsfunktion $h(\alpha)$ die Dreiecksrelation voraus, so lassen sich folgende Anordnungsaussagen beweisen:

Hilfssatz 1. *Sind in einem vollständigen Viereck $\zeta, \alpha, \beta, \gamma$ jeweils a, b, c, d, e, f die Verbindungsgeraden von (β, γ), (α, γ), (α, β), (ζ, α), (ζ, β), (ζ, γ) und sind $\delta, \varepsilon, \varphi$ jeweils die Schnittpunkte einer beliebigen mit ζ inzidierenden Geraden $z \neq d, e, f$ mit a, b, c* (s. Fig. 2), *so folgt aus der Gültigkeit einer der Beziehungen $[\varepsilon, \varphi | \delta]$, $[e, f | d]$ stets die andere.*

Beweis. Wendet man auf das Dreieck $\alpha, \varepsilon, \varphi$ hinsichtlich der Geraden a, e, f die Dreiecksrelation an, so folgt

$$a(\varepsilon)\, a(\varphi)\, e(\alpha)\, e(\varphi)\, f(\alpha)\, f(\varepsilon) = 1\,. \tag{3}$$

α' sei ein beliebiger von ζ und α verschiedener Punkt der Geraden d. Dann bezeichnen wir mit b' und c' die Verbindungsgeraden (α', ε) und (α', φ) und mit β', γ' die Schnittpunkte (c', e) und (b', f). Nach dem kleinen Satz von Desargues geht dann die Verbindungsgerade a' von (β', γ') durch δ. Wendet man jetzt die Dreiecksrelation auf das Dreieck $\alpha', \varepsilon, \varphi$ hinsichtlich der Geraden a', e, f an, so erhält man

$$a'(\varepsilon)\, a'(\varphi)\, e(\alpha')\, e(\varphi)\, f(\alpha')\, f(\varepsilon) = 1\,. \tag{4}$$

Durch Multiplikation von (3) und (4) und Umformung ergibt sich

(5) $$a(\varepsilon)\, a(\varphi)\, a'(\varepsilon)\, a'(\varphi) = e(\alpha)\, e(\alpha')\, f(\alpha)\, f(\alpha').$$

Ist $[\varepsilon, \varphi | \delta]$, so besagt die Anordnungsaussage (5) unter Beachtung, daß sowohl α als auch α' zwei beliebige von ζ verschiedene Punkte von d sein dürfen, daß auch $[e, f | d]$ gilt. — Um auch aus der zweiten Beziehung die erste zu erhalten, gehen wir diesmal von einer beliebigen mit δ inzidierenden Geraden $a' \neq a, z$ aus. β', γ' seien hier die Schnittpunkte (a', e) und (a', f) und α' der Schnittpunkt der Verbindungsgeraden (β', φ) und (γ', ε). Nach dem kleinen Satz von DESARGUES inzidiert α' mit d. Daher gilt auch (4) und weiterhin (5). Da diesmal a und a' zwei beliebige von z verschiedene und mit δ inzidierende Geraden sein dürfen, folgt $[\varepsilon, \varphi | \delta]$ aus $[e, f | d]$. Damit ist Hilfssatz 1 bewiesen.

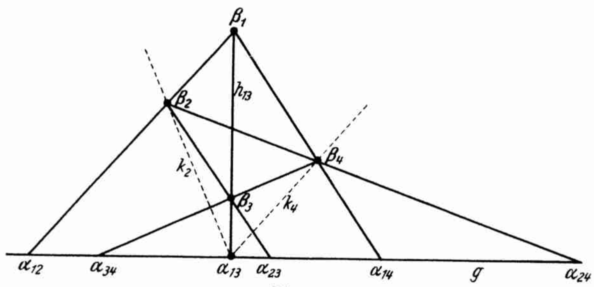

Fig. 3

Bevor wir Hilfssatz 2 formulieren, erklären wir: Unter einem *Hessenbergwurf*[6]) für Punkte soll jedes Punktesechstupel $\alpha_{ik}\, (k > i = 1, 2, 3, 4)$ verstanden werden, das von einem *vollständigen Viereck* $\beta_1, \beta_2, \beta_3, \beta_4$ auf einer Geraden g, die mit keinem β_i $(i = 1, 2, 3, 4)$ inzidiert, ausgeschnitten wird. Dabei soll α_{ik} stets der Schnittpunkt der Verbindungsgeraden (β_i, β_k) mit g sein.

Hilfssatz 2. *Ist α_{ik} ein Hessenbergwurf und gilt $\alpha_{13} \neq \alpha_{24}$, so folgt aus $[\alpha_{12}, \alpha_{14} | \alpha_{24}]$ stets auch $[\alpha_{34}, \alpha_{23} | \alpha_{24}]$.*

Beweis. $\beta_1, \beta_2, \beta_3, \beta_4$ sei das zum Hessenbergwurf α_{ik} gehörige vollständige Viereck (Fig. 3). Mit h_{ik} $(i < k)$ sei die Verbindungsgerade (β_i, β_k) bezeichnet und mit k_2, k_4 die Verbindungsgeraden (α_{13}, β_2) und (α_{13}, β_4). Wendet man jetzt einmal Hilfssatz 1 hinsichtlich des Vierecks $\alpha_{13}, \beta_1, \beta_2, \beta_4$ an, so folgt aus $[\alpha_{12}, \alpha_{14} | \alpha_{24}]$ die Beziehung $[k_2, k_4 | k_{13}]$, und zum andern folgt hinsichtlich des Vierecks $\alpha_{13}, \beta_3, \beta_2, \beta_4$ aus $[k_2, k_4 | k_{13}]$ die Beziehung $[\alpha_{34}, \alpha_{23} | \alpha_{24}]$, womit Hilfssatz 2 bewiesen ist.

Um den Satz nunmehr zu beweisen, setzten wir die Existenz von drei Geraden e, f, d voraus mit $[e, f | d]$. Mit ζ bezeichnen wir ihren Schnittpunkt. Sodann werde durch ζ eine beliebige Gerade $z \neq e, f, d$ gelegt und auf ihr ein beliebiger Punkt $\delta \neq \zeta$ gewählt. Unser erstes Ziel ist es, zu zeigen, daß für

[6]) HESSENBERG hat als erster diese Punkte-Sechstupel benutzt (vgl. [*1*]). In dem Lehrbuch von VEBLEN-YOUNG: „*Projective geometry* I" wird ein derartiges Sechstupel als *quadrangular set* bezeichnet.

alle mit z inzidierenden Punktepaare $\varepsilon, \varphi \neq \delta$ die Beziehung $[\varepsilon, \varphi | \delta]$ gilt. — $a \neq z$ sei eine beliebig gewählte Gerade durch δ, und β, γ seien ihre Schnittpunkte mit e und f. Wählt man auf d einen beliebigen von ζ und dem Schnittpunkt (a, d) verschiedenen Punkt α, so kann man von α aus die Punkte $\beta = (a, e)$, $\gamma = (a, f)$ auf die Gerade z projezieren und erhält die Projektionspunkte φ, ε (s. Fig. 2). Da hinsichtlich des Vierecks $\zeta, \alpha, \beta, \gamma$ die Voraussetzungen von Hilfssatz 1 erfüllt sind, folgt nunmehr für die Punkte ε, φ aus $[e, f | d]$ die Beziehung $[\varepsilon, \varphi | \delta]$. Damit ist die Existenz eines Punktepaares ε, φ mit $[\varepsilon, \varphi | \delta]$ nachgewiesen. — Dual ergibt sich aus der Existenz von $\varepsilon, \varphi, \delta$ mit $[\varepsilon, \varphi | \delta]$: Ist $\xi \neq \varepsilon, \varphi, \delta$ ein beliebiger Punkt von z, so gibt

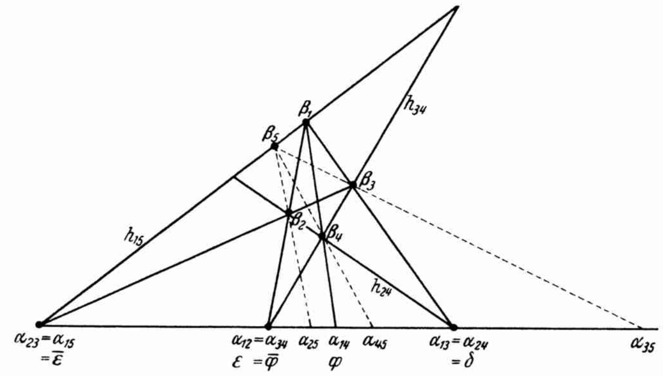

Fig. 4

es mindestens drei voneinander verschiedene mit ξ inzidierende Geraden $p, m, n \neq z$ mit $[m, n | p]$.

Jetzt sei $\bar{\varepsilon}, \bar{\varphi}$ ein beliebiges Punktepaar der Geraden z, von dem wir nur voraussetzen, daß $\bar{\varepsilon} \neq \bar{\varphi}$ und daß weder $\bar{\varepsilon}$ noch $\bar{\varphi}$ mit δ zusammenfallen. Wir setzen: $\delta = \alpha_{24}$, $\varepsilon = \alpha_{12}$, $\varphi = \alpha_{14}$, $\bar{\varepsilon} = \alpha_{23}$, $\bar{\varphi} = \alpha_{34}$, falls $\bar{\varepsilon} \neq \varepsilon$ und $\bar{\varphi} \neq \varphi$, und $\bar{\varepsilon} = \alpha_{34}$, $\bar{\varphi} = \alpha_{23}$, falls $\bar{\varepsilon} = \varepsilon$ oder $\bar{\varphi} = \varphi$.

Dann ist sicher stets $\alpha_{ik} \neq \alpha_{lm}$, wenn von den vier Zahlen i, k, l, m genau zwei übereinstimmen. Bekanntlich läßt sich daher ein sechster Punkt α_{13} so bestimmen, daß die α_{ik} einen Hessenbergwurf bilden[7]). — Ist nun $\alpha_{13} \neq \alpha_{24}$ ($= \delta$), so gilt nach Hilfssatz 2 mit $[\varepsilon, \varphi | \delta] = [\alpha_{12}, \alpha_{14} | \alpha_{24}]$ auch $[\alpha_{23}, \alpha_{34} | \alpha_{24}] = [\bar{\varepsilon}, \bar{\varphi} | \delta]$. — Sollte $\alpha_{13} = \alpha_{24}$ sein, so können wir wegen der Regel (1) ohne Beschränkung der Allgemeinheit zusätzlich $\alpha_{12} = \alpha_{34}$ voraussetzen. (Durch diese Voraussetzung bleiben uns einige Fallunterscheidungen erspart.) Hier sind zwei Fälle zu unterscheiden:

1. Jede Gerade inzidiert mit mindestens *fünf* verschiedenen Punkten. Dann läßt sich auf der Verbindungsgeraden $h_{15} = (\alpha_{23}, \beta_1)$ ein Punkt β_5 wählen, der von den Punkten $\beta_1, \alpha_{23}, (h_{24}, h_{15}), (h_{34}, h_{15})$ verschieden ist (s. Fig. 4). Das Viereck $\beta_1, \beta_2, \beta_5, \beta_4$ ist vollständig und schneidet auf z

[7]) Es läßt sich nämlich unter dieser Voraussetzung stets ein vollständiges Viereck $\beta_1, \beta_2, \beta_3, \beta_4$ angeben, so daß die Gerade $h_{ik} = (\beta_i, \beta_k)$ die Gerade z in α_{ik} für $(i, k) \neq (1, 3)$ schneidet. Vgl. hierzu [1] oder VEBLEN-YOUNG: „*Projective geometry* I" S. 47ff.

den Hessenbergwurf $\alpha_{12}, \alpha_{15}, \alpha_{14}, \alpha_{25}, \alpha_{24}, \alpha_{45}$ aus mit $\alpha_{15} = \alpha_{23} \neq \alpha_{24}$ und $[\alpha_{12}, \alpha_{14}|\alpha_{24}]$. Daher ist auch (nach Hilfssatz 2) $[\alpha_{25}, \alpha_{45}|\alpha_{24}]$. — Aber auch das Viereck $\beta_5, \beta_2, \beta_3, \beta_4$ ist vollständig. Es schneidet auf z den Hessenbergwurf $\alpha_{25}, \alpha_{35}, \alpha_{45}, \alpha_{23}, \alpha_{24}, \alpha_{34}$ aus mit $\alpha_{35} \neq \alpha_{24}$. Da $[\alpha_{25}, \alpha_{45}|\alpha_{24}]$ gilt, ist auch $[\alpha_{23}, \alpha_{34}|\alpha_{24}] = [\overline{\varepsilon}, \overline{\varphi}|\delta]$.

Von δ war nur vorausgesetzt, daß $\delta \neq \zeta$ ist. Um auch diese letzte Einschränkung aufzuheben, denken wir uns auf z ein Punktetripel $\varepsilon, \varphi, \delta$ mit $[\varepsilon, \varphi|\delta]$ gegeben. Auf Grund der Voraussetzung gibt es mindestens einen Punkt ξ auf z mit $\xi \neq \varepsilon, \varphi, \delta, \zeta$. Wie bereits oben gezeigt, existieren mindestens drei mit ξ inzidierende Geraden $m, n, p \neq z$ mit $[m, n|p]$. Geht man statt von e, f, d von diesen Geraden aus, so kann man für alle Punktepaare ε, φ mit $\varepsilon \neq \zeta$, $\varphi \neq \zeta$ die Beziehung $[\varepsilon, \varphi|\zeta]$ beweisen.

2. Jede Gerade inzidiert mit genau *vier* verschiedenen Punkten. Hier gibt es durch ζ nur eine Gerade $z \neq e, f, d$, da auch jeder Punkt mit genau vier verschiedenen Geraden inzidiert. Da es auf der Geraden z außer ζ nur noch drei weitere Punkte gibt, und da $\delta \neq \zeta$ beliebig auf z gewählt werden darf, folgen also aus $[e, f|d]$ zwangsläufig die Beziehungen $[\varepsilon, \varphi|\delta]$, $[\varepsilon, \delta|\varphi]$, $[\varphi, \delta|\varepsilon]$ und aus diesen wiederum $[e, d|f]$, $[d, f|e]$. Hieraus erkennt man sofort die Gültigkeit des

Hilfssatz 3. Inzidiert in Π jede Gerade mit genau vier verschiedenen Punkten, so gilt mit $[\alpha, \beta|\gamma]$ stets auch $[\alpha, \gamma|\beta]$, $[\beta, \gamma|\alpha]$ und mit $[a, b|c]$ stets $[a, c|b]$, $[b, c|a]$.

Um jetzt auch $[\varepsilon, \zeta|\varphi]$ zu beweisen, genügt es nach Hilfssatz 3 zu zeigen, daß $[\varepsilon, \varphi|\zeta]$ gilt. — Wir wählen in Fig. 2 auf d den vierten Punkt $\alpha' \neq \alpha, \zeta, (a, d)$. Die Verbindungsgeraden (α', β) bzw. (α', γ) müssen die Gerade z zwangsläufig in den Punkten ε bzw. φ schneiden. Wendet man die Dreiecksrelation einmal auf das Dreieck $\varepsilon, \varphi, \alpha$ und zum andern auf das Dreieck $\varepsilon, \varphi, \alpha'$ jedesmal hinsichtlich der Geraden e, f, a an, so folgt nach Umformung:

$$f(\varphi)\, e(\varepsilon) = f(\alpha)\, e(\alpha)\, a(\varepsilon)\, a(\varphi)$$

$$f(\varepsilon)\, e(\varphi) = f(\alpha')\, e(\alpha')\, a(\varepsilon)\, a(\varphi).$$

Durch Multiplikation erhält man:

$$e(\varepsilon)\, e(\varphi)\, f(\varepsilon)\, f(\varphi) = e(\alpha)\, e(\alpha')\, f(\alpha)\, f(\alpha')$$

und wegen $[e, f|d]$:

$$e(\varepsilon)\, e(\varphi)\, f(\varepsilon)\, f(\varphi) = 1.$$

Da die Beziehung $[e, f|d]$ nach Permutation der Geraden erhalten bleibt, folgt entsprechend:

$$e(\varepsilon)\, e(\varphi)\, d(\varepsilon)\, d(\varphi) = 1$$

und damit $[\varepsilon, \varphi|\zeta]$. — Nach (1) erhält man aus $[\varepsilon, \zeta|\varphi]$ und $[\varepsilon, \delta|\varphi]$ die Beziehung $[\delta, \zeta|\varphi]$ und damit (nach Hilfssatz 3) $[\zeta, \varphi|\delta]$. Ganau so folgt $[\zeta, \varepsilon|\delta]$. Aus diesen Beziehungen erkennt man auf Grund von Hilfssatz 3, daß für drei voneinander verschiedene Punkte α, β, γ von z stets $[\alpha, \beta|\gamma]$ gilt.

Damit ist in beiden Fällen gezeigt:

Sind a_1, a_2, a_3 *drei Geraden, die mit einem Punkt* ζ *inzidieren und ist* $[a_1, a_2 | a_3]$, *so gilt für alle Punktetripel* $\alpha_1, \alpha_2, \alpha_3$, *die auf einer mit* ζ *inzidierenden Geraden* $z \neq a_1, a_2, a_3$ *liegen, stets* $[\alpha_1, \alpha_2 | \alpha_3]$, *sofern die Punkte* $\alpha_1, \alpha_2, \alpha_3$ *voneinander verschieden sind.*

Vollkommen dual läßt sich beweisen:

Sind $\alpha_1, \alpha_2, \alpha_3$ *drei Punkte, die auf einer Geraden* z *liegen und ist* $[\alpha_1, \alpha_2 | \alpha_3]$, *so gilt für alle Geradentripel* a_1, a_2, a_3, *die mit einem auf* z *liegenden Punkt* $\zeta \neq \alpha_1, \alpha_2, \alpha_3$ *inzidieren, stets* $[a_1, a_2 | a_3]$, *sofern die Geraden* a_1, a_2, a_3 *voneinander verschieden sind.*

Setzt man die Existenz eines Punktetripels $\alpha_1, \alpha_2, \alpha_3$ mit $[\alpha_1, \alpha_2 | \alpha_3]$ oder die eines Geradentripels a_1, a_2, a_3 mit $[a_1, a_2 | a_3]$ voraus, so erkennt man durch Kombination dieser beiden Aussagen:

Sind α, β, γ *bzw.* a, b, c *irgend drei voneinander verschiedene Punkte bzw. Geraden, die mit einer Geraden bzw. einem Punkt inzidieren, so gilt stets* $[\alpha, \beta | \gamma]$ *bzw.* $[a, b | c]$. Damit ist gezeigt, daß die Ordnungsfunktion $h(\alpha)$ der Geradenrelation in ganz Π genügt, womit der Satz vollständig bewiesen ist.

Anmerkung

Man kann jetzt die Fragen stellen: *Läßt sich dieser Satz auch für alle nichtdesarguesschen projektiven Ebenen beweisen? — Gibt es Ordnungsfunktionen, die der Dreiecksrelation nicht aber der Geradenrelation genügen,* d.h. daß es weder drei Punkte $\alpha_1, \alpha_2, \alpha_3$ mit $[\alpha_1, \alpha_2 | \alpha_3]$ noch drei Geraden g_1, g_2, g_3 mit $[g_1, g_2 | g_3]$ gibt?

Zur ersten Frage ist zu bemerken, daß der kleine Satz von DESARGUES wesentlich zum Beweis vom Hilfssatz 1 benötigt wird. Ich sehe keine Möglichkeit, Hilfssatz 1 ohne diesen Satz zu beweisen. Hinsichtlich der zweiten Frage vermute ich, daß sie positiv zu beantworten ist. Doch dürfte die Angabe eines solchen Beispiels nicht ganz einfach sein.

Literatur

[*1*] HESSENBERG, G.: Über einen geometrischen Kalkül. Acta Math. **29**, 1—23 (1905). — [*2*] SPERNER, E.: Die Ordnungsfunktion einer Geometrie. Math. Ann. **121**, 107 bis 130 (1949). — [*3*] SPERNER, E.: Beziehungen zwischen geometrischer und algebraischer Anordnung. Sitzungsber. Heidelberg. Akad. Wiss. **1949**, 10. Abh.

Hamburg, Mathematisches Seminar der Universität

(Eingegangen am 23. April 1955)

Huppert, B.
Math. Zeitschr. Bd. 64, S. 138—148 (1956)

Über die Auflösbarkeit faktorisierbarer Gruppen. III

Von

Bertram Huppert

In Teil II[1]) war unter anderem folgender Satz bewiesen worden (Satz 4): *Die Gruppe $\mathfrak{L}$ habe einen zyklischen Normalteiler vom Index 2. Dann ist jedes Produkt $\mathfrak{G}=\mathfrak{L}\mathfrak{N}$ von $\mathfrak{L}$ mit einer nilpotenten Gruppe $\mathfrak{N}$ auflösbar.*

Wird der Index 2 durch eine Primzahl $q>2$ ersetzt, so gilt der Satz nicht mehr. Denn die einfache Gruppe der Ordnung 168 erlaubt eine Zerlegung $\mathfrak{G}_{168}=\mathfrak{L}\mathfrak{N}$, wobei $\mathfrak{L}$ eine nichtabelsche Gruppe der Ordnung 21 ist (also einen zyklischen Normalteiler vom Index 3 besitzt) und $\mathfrak{N}$ eine Diedergruppe der Ordnung 8 ist. Unter spezielleren Voraussetzungen ist die einfache Gruppe $\mathfrak{G}_{168}$ in gewissem Sinne das einzige nicht auflösbare Beispiel; denn es gilt[2])

Satz 6. *Sei $\mathfrak{L}$ eine Gruppe der Ordnung pq, wobei p und q Primzahlen sind, $\mathfrak{N}$ eine nilpotente Gruppe. Gibt es keine Untergruppe $\mathfrak{U}$ von $\mathfrak{G}=\mathfrak{L}\mathfrak{N}$, die sich homomorph auf die einfache $\mathfrak{G}_{168}$ abbilden läßt, so ist $\mathfrak{G}$ auflösbar.*

In Satz 4 dürfen wir den Faktor $\mathfrak{L}$ etwas allgemeiner wählen, wenn wir $\mathfrak{N}$ spezialisieren:

Satz 7. *$\mathfrak{L}$ besitze einen zyklischen Normalteiler vom Primzahlindex q. Ist $\mathfrak{A}$ abelsch, so ist $\mathfrak{G}=\mathfrak{L}\mathfrak{A}$ auflösbar.*

Aber auch bei abelschem zweiten Faktor kann $\mathfrak{L}$ nicht durch eine beliebige metazyklische Gruppe (zyklischer Normalteiler mit zyklischer Faktorgruppe) ersetzt werden ohne die Auflösbarkeit zu verletzen. Denn die symmetrische Gruppe $\mathfrak{S}_5$ gestattet eine Zerlegung $\mathfrak{S}_5=\mathfrak{L}\mathfrak{Z}$, wobei $\mathfrak{L}$ der Normalisator einer 5-Sylowgruppe ist (und einen zyklischen Normalteiler der Ordnung 5 mit zyklischer Faktorgruppe der Ordnung 4 besitzt), während $\mathfrak{Z}$ eine zyklische Gruppe der Ordnung 6 ist. Wieder ist unter speziellen Voraussetzungen die $\mathfrak{S}_5$ das einzige Gegenbeispiel:

Satz 8. *$\mathfrak{L}$ habe einen zyklischen Normalteiler $\mathfrak{Z}_p$ der Ordnung $p>2$ (p Primzahl), $\mathfrak{L}/\mathfrak{Z}_p$ sei zyklisch von der Ordnung 4. Ist $\mathfrak{A}$ abelsch und hat $\mathfrak{G}=\mathfrak{L}\mathfrak{A}$ keine Untergruppe $\mathfrak{U}$, die sich homomorph auf die symmetrische Gruppe $\mathfrak{S}_5$ abbilden läßt, so ist $\mathfrak{G}$ auflösbar.*

Bezeichnungen. $(\mathfrak{G})=$ Ordnung von $\mathfrak{G}$; $\mathfrak{U}\leq\mathfrak{G}$ bedeutet: $\mathfrak{U}$ ist Untergruppe von $\mathfrak{G}$, wobei auch $\mathfrak{U}=\mathfrak{G}$ zugelassen ist; $\mathfrak{U}<\mathfrak{G}$: $\mathfrak{U}$ ist Untergruppe von $\mathfrak{G}$, aber $\mathfrak{U}\neq\mathfrak{G}$[3]); $\mathfrak{U}\trianglelefteq\mathfrak{G}$: $\mathfrak{U}$ ist Normalteiler von $\mathfrak{G}$; $\mathfrak{U}\triangleleft\mathfrak{G}$: $\mathfrak{U}$ ist Normalteiler von $\mathfrak{G}$ und $\mathfrak{U}\neq\mathfrak{G}$; $\mathfrak{G}_p=p$-Sylow-Gruppe von $\mathfrak{G}$; ${}_p\mathfrak{G}=p$-Sylow-

[1]) Siehe Literatur [5] und [7], zitiert als I und II.
[2]) Wir numerieren die Sätze durchlaufend weiter.
[3]) Abweichend von I und II.

Komplement von $\mathfrak{G}$ (s. P. HALL [4]); $\mathfrak{Z}(\mathfrak{G})$ = Zentrum von $\mathfrak{G}$; $\mathfrak{G}'$ = Kommutatorgruppe von $\mathfrak{G}$; $\mathfrak{G}'(p) = p$-Kommutatorgruppe von $\mathfrak{G}$ (s. ZASSENHAUS [16], S. 122); $\mathfrak{N}(\mathfrak{U})$ = Normalisator der Untergruppe $\mathfrak{U}$ von $\mathfrak{G}$; $\mathfrak{C}(\mathfrak{U})$ = Zentralisator der Untergruppe $\mathfrak{U}$ von $\mathfrak{G}$; $\mathfrak{U}^X = X^{-1}\mathfrak{U}X$; ist p Primzahl und $p^\alpha \mid m$, aber $p^{\alpha+1} \nmid m$, so schreiben wir $p^\alpha \top m$.

Beweis von Satz 6 durch Induktion nach $(\mathfrak{G})$. Die Voraussetzung, daß sich keine Untergruppe von $\mathfrak{G}$ homomorph auf die einfache $\mathfrak{G}_{168}$ abbilden läßt, überträgt sich auf Untergruppen und Faktorgruppen von $\mathfrak{G}$. Ein homomorphes Bild $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ hat entweder wieder eine Produktzerlegung des gleichen Typs wie $\mathfrak{G}$ (falls $\overline{\mathfrak{L}} \cong \mathfrak{L}$) oder ist nach ITÔ [8] auflösbar (falls $\overline{\mathfrak{L}}$ zyklisch ist). Somit genügt der Nachweis eines von $\mathfrak{E}$ verschiedenen auflösbaren Normalteilers von $\mathfrak{G}$.

Sei $\mathfrak{L}' \neq \mathfrak{E}$; sonst ist $\mathfrak{G}$ nach ITÔ [8] auflösbar. Insbesondere dürfen wir daher $p \neq q$ annehmen. Sei etwa $p > q$, also bekanntlich $\mathfrak{L}_p = \mathfrak{Z}_p \lhd \mathfrak{L}$.

a) Sei zunächst $\mathfrak{N}$ eine maximale Untergruppe von $\mathfrak{G}$, r eine Primzahl mit $r \mid (\mathfrak{N})$ und $p \neq r \neq q$; gibt es kein solches r, so ist $(\mathfrak{G}) = p^\alpha q^\beta$ und $\mathfrak{G}$ ist nach einem bekannten Satz von BURNSIDE auflösbar (s. SPEISER [12], S. 193). $\mathfrak{G}_r = \mathfrak{N}_r$ ist eine r-SYLOW-Gruppe von $\mathfrak{G}$. Schließen wir den trivialen Fall $\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_r)) = \mathfrak{G}$ aus, so ist $\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_r)) = \mathfrak{N}$. Ist $\mathfrak{G}$ r-normal, so gilt nach GRÜN (s. ZASSENHAUS [16], S. 135)

$$\mathfrak{E} \neq \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_r))/\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_r))'(r) \cong \mathfrak{G}/\mathfrak{G}'(r).$$

Wegen $r \nmid (\mathfrak{L})$ liegt $\mathfrak{L}$ in $\mathfrak{G}'(r)$. Dann haben wir $\mathfrak{G}'(r) = \mathfrak{L}\overline{\mathfrak{N}}$ mit $\overline{\mathfrak{N}} < \mathfrak{N}$ und $\mathfrak{G}'(r)$ ist nach unserer Induktionsannahme auflösbar.

Ist $\mathfrak{G}$ nicht r-normal, so existiert ein Element $X \in \mathfrak{G}$, $X \notin \mathfrak{N}$ mit $\mathfrak{Z}(\mathfrak{G}_r) < \mathfrak{G}_r^X$, $\mathfrak{Z}(\mathfrak{G}_r) \neq \mathfrak{Z}(\mathfrak{G}_r^X)$. Dann bekommen wir $\mathfrak{N} = \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_r)) \geqq \{\mathfrak{N}, {}_r\mathfrak{N}^X\}$. Also ist ${}_r\mathfrak{N} = {}_r\mathfrak{N}^X$. Nun folgt $\mathfrak{N}({}_r\mathfrak{N}) \geqq \{\mathfrak{N}, X\} = \mathfrak{G}$. Ist ${}_r\mathfrak{N} \neq \mathfrak{E}$, so haben wir damit einen auflösbaren, von $\mathfrak{E}$ verschiedenen Normalteiler von $\mathfrak{G}$ gefunden. Ist aber ${}_r\mathfrak{N} = \mathfrak{E}$, d.h. $(\mathfrak{N}) = r^\varrho$, so folgt $(\mathfrak{G}) = pqr^\varrho$. Ist $\mathfrak{G}$ nicht auflösbar, so hat ein nicht auflösbarer Kompositionsfaktor $\mathfrak{U}/\mathfrak{V}$ von $\mathfrak{G}$ notwendig eine Ordnung der Gestalt pqr^τ. Sei $\mathfrak{G} \rhd \mathfrak{U}_1 \rhd \mathfrak{U}_2 \rhd \cdots \rhd \mathfrak{U}_j \rhd \mathfrak{U}$ der Ausschnitt einer Kompositionsreihe von $\mathfrak{G}$ bis $\mathfrak{U}$. Wegen $(\mathfrak{U}/\mathfrak{V}) = pqr^\tau$ und $(\mathfrak{G}) = pqr^\varrho$ sind die Indizes in dem angegebenen Abschnitt Potenzen von r. Aus $r \nmid (\mathfrak{L}) = pq$ folgt nun schrittweise $\mathfrak{L} \leqq \mathfrak{U}_1$, $\mathfrak{L} \leqq \mathfrak{U}_2, \ldots, \mathfrak{L} \leqq \mathfrak{U}$. Somit hat $\mathfrak{U}$ die Gestalt $\mathfrak{U} = \mathfrak{L}\tilde{\mathfrak{N}}$ mit $\tilde{\mathfrak{N}} \leqq \mathfrak{N}$. Dann erlaubt $\mathfrak{U}/\mathfrak{V}$ die Zerlegung $\mathfrak{U}/\mathfrak{V} = \overline{\mathfrak{L}}\overline{\mathfrak{N}}$ mit $\overline{\mathfrak{L}} \cong \mathfrak{L}$ und nilpotentem $\overline{\mathfrak{N}}$. Nach BRAUER und TUAN [1] sind die einfache Gruppe $\mathfrak{G}_{168}$ und die alternierende Gruppe $\mathfrak{A}_5$ die einzigen einfachen, nichtauflösbaren Gruppen mit Ordnungen der Gestalt pqr^τ. Die $\mathfrak{A}_5$ erlaubt aber keine Zerlegung der Gestalt $\overline{\mathfrak{L}}\overline{\mathfrak{N}}$. Daher folgt $\mathfrak{U}/\mathfrak{V} \cong \mathfrak{G}_{168}$, was aber durch die Voraussetzung ausgeschlossen ist. Also muß $\mathfrak{G}$ in diesem Falle auflösbar sein.

b) Sei nun weiterhin $\mathfrak{N}$ nicht maximale Untergruppe von $\mathfrak{G}$. Ferner können wir annehmen, daß $\mathfrak{N} \cap \mathfrak{L} = \mathfrak{E}$ gilt; andernfalls würde nämlich $\mathfrak{G}$ eine Zerlegung $\mathfrak{G} = \mathfrak{Z}\mathfrak{N}$ mit einer zyklischen Untergruppe $\mathfrak{Z}$ von $\mathfrak{L}$ zulassen und wäre nach ITÔ [8] auflösbar. Sei $\mathfrak{J}$ eine maximale, $\mathfrak{N}$ umfassende Untergruppe von $\mathfrak{G}$. Dann ist $(\mathfrak{J}) = p(\mathfrak{N})$ oder $(\mathfrak{J}) = q(\mathfrak{N})$.

Gibt es ein $\mathfrak{J}$ mit $(\mathfrak{J}) = p(\mathfrak{N})$, so hat $\mathfrak{J}$ die Gestalt $\mathfrak{J} = \mathfrak{Z}_p\mathfrak{N}$ mit einer zyklischen Untergruppe $\mathfrak{Z}_p$ von $\mathfrak{L}$. Nach ITÔ [8] ist $\mathfrak{J}$ auflösbar. Wir stellen nun $\mathfrak{G}$ dar als Permutationsgruppe der Nebenklassen von $\mathfrak{J}$. Dabei werde $\mathfrak{G}$ auf die Permutationsgruppe $\overline{\mathfrak{G}}$ vom Grade q abgebildet. Es ist $(\overline{\mathfrak{G}}) \mid q!$. Wegen $p > q$ folgt $p \nmid (\overline{\mathfrak{G}})$. Also ist die homomorphe Abbildung von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$ nicht treu, vielmehr wird ein in $\mathfrak{J}$ liegender, von $\mathfrak{E}$ verschiedener Normalteiler $\mathfrak{K}$ von $\mathfrak{G}$ auf $\mathfrak{E}$ abgebildet. Als Untergruppe von $\mathfrak{J}$ ist $\mathfrak{K}$ auflösbar, womit wir einen auflösbaren Normalteiler $\neq \mathfrak{E}$ nachgewiesen haben. Weiterhin dürfen wir also annehmen, daß jede maximale Untergruppe $\mathfrak{J}$ von $\mathfrak{G}$, welche $\mathfrak{N}$ umfaßt, die Ordnung $(\mathfrak{J}) = q(\mathfrak{N})$ hat und sich als Produkt $\mathfrak{J} = \mathfrak{Z}_q\mathfrak{N}$ mit einer zyklischen Untergruppe $\mathfrak{Z}_q$ von $\mathfrak{L}$ der Ordnung q schreiben läßt. Alle diese $\mathfrak{J}$ sind nach ITÔ [8] auflösbar.

c) Sei $p \mid (\mathfrak{N})$. Dann gilt $\mathfrak{N}(\mathfrak{N}_p) \geqq \mathfrak{N}$. Da $\mathfrak{N}_p$ keine p-SYLOW-Gruppe von $\mathfrak{G}$ ist, folgt nach einem bekannten Satz (ZASSENHAUS [16], S. 105, Satz 10) $p \mid (\mathfrak{N}(\mathfrak{N}_p)/\mathfrak{N}_p)$. Mithin kann $\mathfrak{N}(\mathfrak{N}_p)$ in keiner der maximalen Untergruppen $\mathfrak{J} = \mathfrak{Z}_q\mathfrak{N}$ liegen, muß also mit $\mathfrak{G}$ übereinstimmen. Dann liefert uns $\mathfrak{N}_p$ den gesuchten Normalteiler von $\mathfrak{G}$. Wir können daher in der Folge annehmen, daß $p \nmid (\mathfrak{N})$.

d) $\mathfrak{G}_q = \mathfrak{J}_q = \mathfrak{Z}_q\mathfrak{N}_q$ ist für jedes $\mathfrak{J}$ eine q-SYLOW-Gruppe von $\mathfrak{G}$ (s. WIELANDT [15], S. 3). Ist $\mathfrak{N}_q \neq \mathfrak{E}$, so liegt $\mathfrak{D} = \mathfrak{Z}(\mathfrak{G}_q) \cap \mathfrak{N}_q$ in $\mathfrak{Z}(\mathfrak{J})$. Nun ist $\mathfrak{N}_q$ maximal in $\mathfrak{G}_q$, daher $\mathfrak{N}_q \triangleleft \mathfrak{G}_q$ und dann bekanntlich $\mathfrak{D} = \mathfrak{Z}(\mathfrak{G}_q) \cap \mathfrak{N}_q \neq \mathfrak{E}$. Wegen $(\mathfrak{G}:\mathfrak{J}) = p$ ist die Anzahl der Konjugierten eines Elementes $D \neq E$ von $\mathfrak{D}$ ein Teiler von p. Nach einem bekannten Satz von BURNSIDE (SPEISER [12], S. 193, Satz 169) ist dann $\mathfrak{G}$ nicht einfach. Sei $\mathfrak{K}$ ein minimaler, von $\mathfrak{E}$ verschiedener Normalteiler von $\mathfrak{G}$. Ist $\mathfrak{K}\mathfrak{N} \neq \mathfrak{G}$, so hat $\mathfrak{K}\mathfrak{N}$ die Gestalt $\mathfrak{N}\overline{\mathfrak{L}}$ mit $\overline{\mathfrak{L}} \leqq \mathfrak{L}$. Wegen $\mathfrak{G} \neq \mathfrak{K}\mathfrak{N}$ ist $\overline{\mathfrak{L}} \neq \mathfrak{L}$, daher $\overline{\mathfrak{L}}$ zyklisch und $\mathfrak{N}\overline{\mathfrak{L}}$ nach ITÔ [8] auflösbar. Als Untergruppe von $\mathfrak{N}\overline{\mathfrak{L}}$ ist dann auch $\mathfrak{K}$ auflösbar. Sei also $\mathfrak{K}\mathfrak{N} = \mathfrak{G}$. In gleicher Weise können wir annehmen, daß auch $\mathfrak{K}\mathfrak{L} = \mathfrak{G}$ gilt; sonst wäre $\mathfrak{K}\mathfrak{L} = \overline{\mathfrak{N}}\mathfrak{L}$ mit $\overline{\mathfrak{N}} < \mathfrak{N}$ nach unserer Induktionsannahme auflösbar und $\mathfrak{K}$ ebenfalls. Aus $\mathfrak{K}\mathfrak{N} = \mathfrak{G}$ und $\mathfrak{K}\mathfrak{L} = \mathfrak{G}$ folgt nun $(\mathfrak{G}/\mathfrak{K}) \mid (\mathfrak{N})$ und $(\mathfrak{G}/\mathfrak{K}) \mid (\mathfrak{L})$, also $(\mathfrak{G}/\mathfrak{K}) = q$. Sicher ist dann $p \mid (\mathfrak{K})$. Da $\mathfrak{K}$ als minimaler Normalteiler ein direktes Produkt von isomorphen einfachen Gruppen ist, aber $p \top (\mathfrak{K})$ gilt, so ist $\mathfrak{K}$ selbst einfach. Aus $\mathfrak{G} = \mathfrak{Z}_p\mathfrak{J}$ ergibt sich nun $\mathfrak{K} = \mathfrak{Z}_p\overline{\mathfrak{J}}$ mit $(\mathfrak{J}/\overline{\mathfrak{J}}) = q$. Ist $\overline{\mathfrak{J}} \leqq \mathfrak{N}$, so ist $\mathfrak{K}$ nach unserer Induktionsannahme auflösbar und wir sind fertig. Ist aber $\overline{\mathfrak{J}} \nleqq \mathfrak{N}$, so folgt $\overline{\mathfrak{J}}\mathfrak{N} = \mathfrak{J}$, also $(\mathfrak{J}:\mathfrak{N}) = q = (\overline{\mathfrak{J}}:\overline{\mathfrak{J}} \cap \mathfrak{N})$. Sicher ist $\mathfrak{N} \neq \overline{\mathfrak{J}} \cap \mathfrak{N}$, denn sonst wäre $\mathfrak{N} \leqq \overline{\mathfrak{J}} \leqq \mathfrak{K}$, daher $\mathfrak{K} = \mathfrak{K}\mathfrak{N} = \mathfrak{G}$, im Widerspruch zur Nichteinfachheit von $\mathfrak{G}$. Wir setzen $\overline{\mathfrak{J}} \cap \mathfrak{N} = \overline{\mathfrak{N}}$. Wäre $\overline{\mathfrak{N}}_q \neq \mathfrak{E}$, so würde wie oben aus dem Satz von BURNSIDE folgen, daß $\mathfrak{K}$ nicht einfach ist, im Gegensatz zu unserer Annahme. Daher ist notwendig $\overline{\mathfrak{N}}_q = \mathfrak{E}$, also $q^2 \nmid (\mathfrak{N})$ und dann $q^3 \nmid (\mathfrak{G})$. Insbesondere ist $\mathfrak{G}_q$ abelsch. Dies trifft auch dann zu, wenn $q \nmid (\mathfrak{N})$. Daher können wir weiterhin annehmen, daß $\mathfrak{G}_q$ abelsch und dann $\mathfrak{G}$ q-normal ist (s. ZASSENHAUS [16], S. 135).

e) Für eine geeignete, in einem $\mathfrak{J} = \mathfrak{Z}_q\mathfrak{N}$ liegende q-SYLOW-Gruppe $\mathfrak{G}_q$ von $\mathfrak{G}$ gilt $\mathfrak{G}_q = \mathfrak{Z}_q \times \mathfrak{N}_q$, wobei eventuell $\mathfrak{N}_q = \mathfrak{E}$ sein kann (s. WIELANDT [15], S. 3). Sei nun $\mathfrak{L} = \mathfrak{Z}_p\mathfrak{Z}_q$, wobei $\mathfrak{Z}_p$ und $\mathfrak{Z}_q$ bzw. von Z_p und Z_q erzeugt werden mögen. Ferner sei $X \in \mathfrak{N}(\mathfrak{G}_q)$. Wegen $\mathfrak{G} = \mathfrak{L}\mathfrak{N}$ hat X die Gestalt $X = Z_q^\beta Z_p^\alpha N$ mit einem $N \in \mathfrak{N}$ und geeigneten α, β. Dann haben wir

$$\mathfrak{Z}_q^X = \mathfrak{Z}_q^{Z_p^\alpha N} \leq \mathfrak{G}_q \leq \mathfrak{J}, \quad \text{daher} \quad \mathfrak{Z}_q^{Z_p^\alpha} \leq \mathfrak{J}^{N^{-1}} = \mathfrak{J}$$

und dann

$$\mathfrak{Z}_q^{Z_p^\alpha} \leq \mathfrak{L} \cap \mathfrak{J} = \mathfrak{Z}_q.$$

Da $\mathfrak{Z}_q$ in $\mathfrak{L}$ eigener Normalisator ist (was aus $\mathfrak{Z}_p \triangleleft \mathfrak{L}$ und $\mathfrak{L}' \neq \mathfrak{E}$ sofort folgt), erhalten wir $Z_p^\alpha = E$. Somit liegt X in $\mathfrak{J}$ und es ergibt sich $\mathfrak{N}(\mathfrak{G}_q) \leq \mathfrak{J}$. Wegen $\mathfrak{Z}_q \leq \mathfrak{N}(\mathfrak{G}_q) \leq \mathfrak{Z}_q \mathfrak{N} = \mathfrak{J}$ hat $\mathfrak{N}(\mathfrak{G}_q)$ die Gestalt $\mathfrak{N}(\mathfrak{G}_q) = \mathfrak{Z}_q \hat{\mathfrak{N}}$ mit $\hat{\mathfrak{N}} \leq \mathfrak{N}$. Ist $\mathfrak{N} \triangleleft \mathfrak{J}$, so folgt $\hat{\mathfrak{N}} \triangleleft \mathfrak{N}(\mathfrak{G}_q)$, und dann ist eine von $\mathfrak{E}$ verschiedene q-Faktorgruppe in $\mathfrak{N}(\mathfrak{G}_q)$ abspaltbar. Nach GRÜN (ZASSENHAUS [*16*], S. 135) folgt wegen der q-Normalität von $\mathfrak{G}$, daß $\mathfrak{G}'(q) \neq \mathfrak{G}$. Sicher ist $\mathfrak{G}'(q) \geq \{\mathfrak{Z}_p, {}_q\mathfrak{N}\}$. Ferner haben wir $\mathfrak{G}'(q)_q = \mathfrak{G}'(q) \cap \mathfrak{G}_q \leq \mathfrak{G}'(q) \cap \mathfrak{N}(\mathfrak{G}_q)$. Offenbar ist

$$\mathfrak{G}'(q) \cap \mathfrak{N}(\mathfrak{G}_q) \geq \mathfrak{N}(\mathfrak{G}_q)'(q).$$

Es gilt aber sogar das Gleichheitszeichen; denn nach GRÜN ist wegen $\mathfrak{G}_q = \mathfrak{Z}(\mathfrak{G}_q)$

$$\mathfrak{G}/\mathfrak{G}'(q) \cong \mathfrak{N}(\mathfrak{G}_q)/\mathfrak{N}(\mathfrak{G}_q)'(q)$$

und andererseits

$$\mathfrak{G}/\mathfrak{G}'(q) = \mathfrak{N}(\mathfrak{G}_q)\,\mathfrak{G}'(q)/\mathfrak{G}'(q) \cong \mathfrak{N}(\mathfrak{G}_q)/\mathfrak{G}'(q) \cap \mathfrak{N}(\mathfrak{G}_q).$$

Daraus folgt $\big(\mathfrak{N}(\mathfrak{G}_q)'(q)\big) = \big(\mathfrak{G}'(q) \cap \mathfrak{N}(\mathfrak{G}_q)\big)$ und dann wegen der obigen Ungleichung die Gleichung. Aus $\hat{\mathfrak{N}} \triangleleft \mathfrak{N}(\mathfrak{G}_q)$ erhalten wir $\mathfrak{N}(\mathfrak{G}_q)'(q) \leq \mathfrak{N}$. Nun bekommen wir schließlich $\mathfrak{G}'(q) = \mathfrak{Z}_p\, {}_q\mathfrak{N}\, \mathfrak{G}'(q)_q = \mathfrak{Z}_p \hat{\mathfrak{N}}$ mit $\hat{\mathfrak{N}} < \mathfrak{N}$. Nach ITÔ [*8*] ist dann $\mathfrak{G}'(q)$ auflösbar. Weiter können wir daher annehmen, daß $\mathfrak{N}$ in keiner der maximalen Untergruppen $\mathfrak{J} = \mathfrak{Z}_q \mathfrak{N}$ invariant ist.

f) Nun stellen wir eine beliebige, $\mathfrak{N}$ umfassende maximale Untergruppe $\mathfrak{J} = \mathfrak{Z}_q \mathfrak{N}$ von $\mathfrak{G}$ dar als Permutationsgruppe $\mathfrak{J}^*$ der Nebenklassen nach $\mathfrak{N}$, also vom Grad q. Da $\mathfrak{J}$ auflösbar ist, gibt es ein $\mathfrak{R}$ mit $\mathfrak{R} \triangleleft \mathfrak{J}$, $\mathfrak{R} < \mathfrak{N}$ und $(\mathfrak{J}/\mathfrak{R}) = qs$ mit $s \mid q-1$; denn bekanntlich haben die transitiven, auflösbaren Permutationsgruppen vom Primzahlgrad q stets eine Ordnung, welche $q(q-1)$ teilt (PERRON [*10*], S. 151). Es ist sicher $s \neq 1$, da sonst $\mathfrak{N} \triangleleft \mathfrak{J}$ gelten würde. Daher gibt es eine Primzahl r mit $r \mid s$ und $r \mid (\mathfrak{N})$. Da sich in $\mathfrak{J}^*$ stets eine zyklische Faktorgruppe der Ordnung s abspalten läßt, ist $\mathfrak{J}^{*\prime}(r) \neq \mathfrak{J}^*$ und dann auch $\mathfrak{J}'(r) \neq \mathfrak{J}$. Wegen $r < q < p$ haben wir für $\mathfrak{G}_r = \mathfrak{N}_r$ nun $\mathfrak{N}\big(\mathfrak{Z}(\mathfrak{G}_r)\big) = \mathfrak{N}$ oder $\mathfrak{N}\big(\mathfrak{Z}(\mathfrak{G}_r)\big) = \mathfrak{J}$, also in jedem Falle $\mathfrak{N}\big(\mathfrak{Z}(\mathfrak{G}_r)\big)'(r) \neq \mathfrak{N}\big(\mathfrak{Z}(\mathfrak{G}_r)\big)$. Ist $\mathfrak{G}$ r-normal, so sind wir wieder fertig; nach GRÜN ist dann nämlich $\mathfrak{G}'(r) \neq \mathfrak{G}$, und $\mathfrak{G}'(r) \geq \mathfrak{L}$ sichert mit Hilfe der Induktionsannahme die Auflösbarkeit von $\mathfrak{G}'(r)$.

g) Nun sei $\mathfrak{G}$ nicht r-normal und $\mathfrak{N}\big(\mathfrak{Z}(\mathfrak{G}_r)\big) = \mathfrak{N}$ für $\mathfrak{G}_r = \mathfrak{N}_r$. Dann gibt es ein $X \in \mathfrak{G}$, $X \notin \mathfrak{N}$ mit $\mathfrak{Z}(\mathfrak{G}_r) \leq \mathfrak{N}^X$, aber $\mathfrak{Z}(\mathfrak{G}_r) \neq \mathfrak{Z}(\mathfrak{G}_r^X)$. Es folgt $\mathfrak{N} = \mathfrak{N}\big(\mathfrak{Z}(\mathfrak{G}_r)\big) \geq \{\mathfrak{N}, {}_r\mathfrak{N}^X\}$. Ist $(\mathfrak{N}) = r^\varrho$, so können wir wie unter a) schließen. Sei daher $(\mathfrak{N}) \neq r^\varrho$, also ${}_r\mathfrak{N} \neq \mathfrak{E}$. Aus $\mathfrak{N}\big(\mathfrak{Z}(\mathfrak{G}_r)\big) = \mathfrak{N} = \{\mathfrak{N}, {}_r\mathfrak{N}^X\}$ folgt jetzt ${}_r\mathfrak{N}^X = {}_r\mathfrak{N}$, somit $\mathfrak{N}({}_r\mathfrak{N}) \geq \{\mathfrak{N}, X\} > \mathfrak{N}$. Schließen wir den trivialen Fall $\mathfrak{N}({}_r\mathfrak{N}) = \mathfrak{G}$

aus, so ist $\mathfrak{N}({}_r\mathfrak{N})$ eine Gruppe $\mathfrak{J} = \mathfrak{Z}_q \mathfrak{N}$. Mit ${}_r\mathfrak{N} \lhd \mathfrak{J}$ ergibt sich $\mathfrak{C}({}_r\mathfrak{N}) \trianglelefteq \mathfrak{N}({}_r\mathfrak{N}) = \mathfrak{J}$. Wir setzen $\mathfrak{Z}({}_r\mathfrak{N}) = \mathfrak{A}$. Dann ist $\mathfrak{A}$ charakteristisch in ${}_r\mathfrak{N}$, also $\mathfrak{A} \lhd \mathfrak{J}$ wegen ${}_r\mathfrak{N} \lhd \mathfrak{J}$. Ferner ist $\mathfrak{C}(\mathfrak{A}) \geqq \mathfrak{N}$. Aus $\mathfrak{C}(\mathfrak{A}) \trianglelefteq \mathfrak{N}(\mathfrak{A}) = \mathfrak{J}$ folgt nun wegen $\mathfrak{N} \ntriangleleft \mathfrak{J}$ die Aussage $\mathfrak{C}(\mathfrak{A}) = \mathfrak{J}$, d.h. $\mathfrak{A} \leqq \mathfrak{Z}(\mathfrak{J})$. Wie unter b) schließen wir nun mit Hilfe des Satzes von BURNSIDE auf die Existenz eines Normalteilers $\mathfrak{K}$ mit $(\mathfrak{G}/\mathfrak{K}) = q$ und wie dort können wir annehmen, daß $\mathfrak{K}$ einfach ist. Wieder hat $\mathfrak{K}$ die Gestalt $\mathfrak{K} = \mathfrak{Z}_p \overline{\mathfrak{J}}$ mit $\mathfrak{J} > \overline{\mathfrak{J}} > \overline{\mathfrak{J}} \cap \mathfrak{N} \geqq_q \mathfrak{N}$ und $(\mathfrak{J}/\overline{\mathfrak{J}}) = (\overline{\mathfrak{J}} : \overline{\mathfrak{J}} \cap \mathfrak{N}) = q$.

Gibt es eine Primzahl s mit $s \mid (\mathfrak{N})$ und $q \neq s \neq r$, so ist $\mathfrak{E} < \mathfrak{Z}(\mathfrak{N}_s) \leqq \mathfrak{Z}({}_r\mathfrak{N}) = \mathfrak{A}$ und wegen $\mathfrak{A} \leqq \mathfrak{Z}(\mathfrak{J})$ folgt $\mathfrak{Z}(\mathfrak{N}_s) \leqq \mathfrak{Z}(\overline{\mathfrak{J}})$. Dann kann aber $\mathfrak{K}$ nach dem schon mehrfach benutzten Satz von BURNSIDE nicht einfach sein, im Widerspruch zu unserer Annahme. Somit ist wegen $q^2 \nmid (\mathfrak{N})$ also $(\mathfrak{N}) \mid q r^\varrho$ und dann $(\mathfrak{G}) \mid p q^2 r^\varrho$. Aus $(\mathfrak{G}/\mathfrak{K}) = q$ folgt $(\mathfrak{K}) \mid p q r^\varrho$. Der schon benutzte Satz von BRAUER und TUAN liefert wegen der Einfachheit von $\mathfrak{K}$ nun $\mathfrak{K} \cong \mathfrak{A}_5$ oder $\mathfrak{K} \cong \mathfrak{G}_{168}$. Der zweite Fall ist durch unsere Voraussetzung ausgeschlossen. Der erste Fall erfordert $p = 5$ und $q \mid p - 1$, also $q = 2$. Dann wäre aber $\mathfrak{G}$ nach II, Satz 4 auflösbar, im Widerspruch zu $\mathfrak{K} \cong \mathfrak{A}_5$.

h) Sei schließlich $\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_r))$ eine der maximalen Untergruppen $\mathfrak{J}$ von $\mathfrak{G}$. Für $\mathfrak{G}_r = \mathfrak{N}_r$ ist dann $\mathfrak{N} \leqq \mathfrak{C}(\mathfrak{Z}(\mathfrak{G}_r)) \trianglelefteq \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_r)) = \mathfrak{J}$. Wegen $\mathfrak{N} \ntriangleleft \mathfrak{J}$ folgt daraus $\mathfrak{C}(\mathfrak{Z}(\mathfrak{G}_r)) = \mathfrak{J}$, d.h. $\mathfrak{Z}(\mathfrak{G}_r) \leqq \mathfrak{Z}(\mathfrak{J})$. Wie früher können wir wegen $(\mathfrak{G} : \mathfrak{J}) = p$ den Satz von BURNSIDE anwenden und erhalten einen Normalteiler $\mathfrak{K}$ von $\mathfrak{G}$ mit $(\mathfrak{G}/\mathfrak{K}) = q$. Wieder kann $\mathfrak{K}$ als einfach angenommen werden. Sicher gilt $\mathfrak{K} \geqq_q \mathfrak{N} \geqq \mathfrak{Z}(\mathfrak{G}_r)$ und $\mathfrak{K} = \mathfrak{Z}_p \overline{\mathfrak{J}}$ mit $(\mathfrak{J}/\overline{\mathfrak{J}}) = q$. Aus $\mathfrak{Z}(\mathfrak{G}_r) \leqq \overline{\mathfrak{J}}$ und $\mathfrak{Z}(\mathfrak{G}_r) \leqq \mathfrak{Z}(\mathfrak{J})$ folgt $\mathfrak{Z}(\mathfrak{G}_r) \leqq \mathfrak{Z}(\overline{\mathfrak{J}})$. Dann kann aber (wieder nach dem BURNSIDEschen Satz) $\mathfrak{K}$ nicht einfach sein, entgegen unserer Annahme.

Damit ist der Beweis von Satz 6 abgeschlossen.

Beweis von Satz 7 durch Induktion nach $(\mathfrak{G})$. Wiederum genügt der Nachweis eines von $\mathfrak{E}$ verschiedenen auflösbaren Normalteilers von $\mathfrak{G}$.

a) Ist $\mathfrak{D} = \mathfrak{L} \cap \mathfrak{A} \neq \mathfrak{E}$, so haben wir $\mathfrak{D} \trianglelefteq \mathfrak{A}$. Dann existiert ein $\mathfrak{K} \lhd \mathfrak{G}$ mit $\mathfrak{D} \leqq \mathfrak{K} \leqq \mathfrak{L}$ (s. ORE [*9*], S. 436 oder SZÉP-RÉDEI [*13*]). Als Untergruppe von $\mathfrak{L}$ ist $\mathfrak{K}$ auflösbar. Wir können daher weiterhin annehmen, daß $\mathfrak{L} \cap \mathfrak{A} = \mathfrak{E}$.

b) Ist $\mathfrak{L}$ nicht maximale Untergruppe von $\mathfrak{G}$, so gibt es eine maximale Untergruppe $\mathfrak{L}\mathfrak{A}_1$ von $\mathfrak{G}$ mit $\mathfrak{E} < \mathfrak{A}_1 < \mathfrak{A}$. Es folgt $\mathfrak{G} = \{\mathfrak{L}\mathfrak{A}_1\}\mathfrak{A}$ und $\mathfrak{L}\mathfrak{A}_1 \cap \mathfrak{A} = \mathfrak{A}_1 \lhd \mathfrak{A}$. Nach [*9*] oder [*13*] existiert dann ein $\mathfrak{K} \lhd \mathfrak{G}$ mit $\mathfrak{A}_1 \leqq \mathfrak{K} \leqq \mathfrak{L}\mathfrak{A}_1$. Unsere Induktionsannahme sagt uns, daß $\mathfrak{L}\mathfrak{A}_1$ auflösbar ist. Dann ist auch $\mathfrak{K}$ auflösbar, und wir sind fertig. Weiter sei also $\mathfrak{L}$ eine maximale Untergruppe von $\mathfrak{G}$.

c) Ist $\mathfrak{A}$ eine maximale Untergruppe von $\mathfrak{G}$, so ist $\mathfrak{G}$ auflösbar (s. HUPPERT [*6*], S. 412, Satz 2). Wir können daher annehmen, daß es $\mathfrak{A}$ echt umfassende maximale Untergruppen $\mathfrak{J}$ von $\mathfrak{G}$ gibt. Dann ist $\mathfrak{J} = \mathfrak{A}\overline{\mathfrak{L}}$ mit $\mathfrak{E} < \overline{\mathfrak{L}} < \mathfrak{L}$. Gibt es einen Normalteiler $\mathfrak{N}$ von $\mathfrak{L}$ mit $\mathfrak{N} \leqq \overline{\mathfrak{L}}$, so existiert nach [*9*] oder [*13*] ein $\mathfrak{K} \lhd \mathfrak{G}$ mit $\mathfrak{N} \leqq \mathfrak{K} \leqq \mathfrak{A}\overline{\mathfrak{L}}$. Dann sind wir wieder fertig. Wir können also voraussetzen, daß $\overline{\mathfrak{L}}$ keinen Normalteiler von $\mathfrak{L}$ enthält. Ist $\mathfrak{Z}_n$ der in $\mathfrak{L}$ nach Voraussetzung enthaltene zyklische Normalteiler vom Index q und der

Ordnung n, so gilt insbesondere $\mathfrak{Z}_n \cap \overline{\mathfrak{L}} = \mathfrak{E}$. Dann hat $\overline{\mathfrak{L}}$ notwendig die Ordnung q und ist Vertretergruppe zu $\mathfrak{Z}_n$ in $\mathfrak{L}$, d.h. es gilt $\mathfrak{Z}_n \overline{\mathfrak{L}} = \mathfrak{L}$ und $\mathfrak{Z}_n \cap \overline{\mathfrak{L}} = \mathfrak{E}$. Wir bezeichnen $\overline{\mathfrak{L}}$ weiterhin mit $\mathfrak{Z}_q$. Jede $\mathfrak{A}$ umfassende, maximale Untergruppe $\mathfrak{J}$ von $\mathfrak{G}$ hat also die Gestalt $\mathfrak{J} = \mathfrak{A}\mathfrak{Z}_q$ mit geeignetem $\mathfrak{Z}_q < \mathfrak{L}$.

Ist $p \mid (\mathfrak{A})$, $p \mid n$ und $p \neq q$, so betrachten wir den Normalisator der p-SYLOW-Gruppe von $\mathfrak{Z}_n$. Dieser enthält $\mathfrak{L}$; seine Ordnung ist aber wegen $p \mid (\mathfrak{A})$ noch durch mindestens eine weitere Potenz von p teilbar. Da $\mathfrak{L}$ maximale Untergruppe von $\mathfrak{G}$ ist, folgt die Invarianz der p-SYLOW-Gruppe von $\mathfrak{Z}_n$ in $\mathfrak{G}$. In Zukunft können wir also annehmen, daß $(\mathfrak{A})$ und n nur die Primzahl q als gemeinsamen Primteiler besitzen.

d) Wir stellen eine beliebige der maximalen Untergruppen $\mathfrak{J} = \mathfrak{A}\mathfrak{Z}_q$ dar als transitive Permutationsgruppe der Nebenklassen nach $\mathfrak{A}$, also vom Grad q. Dabei wird eine in $\mathfrak{J}$ invariante Untergruppe $\overline{\mathfrak{A}}$ von $\mathfrak{A}$ auf $\mathfrak{E}$ abgebildet. $\mathfrak{J}/\overline{\mathfrak{A}}$ ist isomorph zu einer transitiven und auflösbaren Permutationsgruppe vom Primzahlgrad q (auflösbar nach ITÔ [*8*]).

Ist $(\mathfrak{J}/\overline{\mathfrak{A}}) = qs$ mit $s \neq 1$, so gilt $s \mid q-1$. Ist r eine Primzahl mit $r \mid s$, so haben wir $\mathfrak{J}'(r) \neq \mathfrak{J}$. Nun ist $r \mid (\mathfrak{A})$ und $r \neq q$, also $r \nmid n$. Daher ist $\mathfrak{A}_r$ eine r-SYLOW-Gruppe $\mathfrak{G}_r$ von $\mathfrak{G}$ und $\mathfrak{G}$ ist r-normal. Wegen $\mathfrak{A} \leq \mathfrak{N}(\mathfrak{G}_r) \leq \mathfrak{J}$ gilt $\mathfrak{N}(\mathfrak{G}_r) = \mathfrak{A}$ oder $\mathfrak{N}(\mathfrak{G}_r) = \mathfrak{J}$. In $\mathfrak{N}(\mathfrak{G}_r)$ läßt sich somit in jedem Falle eine von $\mathfrak{E}$ verschiedene r-Faktorgruppe abspalten. Aus dem Satz von GRÜN folgt nun $\mathfrak{G}'(r) \neq \mathfrak{G}$. Wegen $r \nmid n$ und $r \neq q$ haben wir $\mathfrak{L} \leq \mathfrak{G}'(r)$, also $\mathfrak{G}'(r) = \mathfrak{L}\widetilde{\mathfrak{A}}$ mit $\widetilde{\mathfrak{A}} < \mathfrak{A}$, und $\mathfrak{G}'(r)$ ist nach unserer Induktionsannahme auflösbar.

e) Nun sei $(\mathfrak{J}/\overline{\mathfrak{A}}) = q$, also $\overline{\mathfrak{A}} = \mathfrak{A} \lhd \mathfrak{J}$ für alle $\mathfrak{J}$. Gibt es eine Primzahl r mit $r \mid (\mathfrak{A})$, $r \neq q$ und $\mathfrak{J}'(r) \neq \mathfrak{J}$, so folgt wegen der r-Normalität von $\mathfrak{G}$ wie eben $\mathfrak{G}'(r) \neq \mathfrak{G}$ und dann die Auflösbarkeit von $\mathfrak{G}$. Wir dürfen daher annehmen, daß $(\mathfrak{J}/\mathfrak{J}') = q^\tau$. Das q-SYLOW-Komplement ${}_q\mathfrak{A}$ von $\mathfrak{A}$ liegt dann in $\mathfrak{J}'$. Wegen $\mathfrak{A} \lhd \mathfrak{J}$ ist ${}_q\mathfrak{A}$ ein Normalteiler von $\mathfrak{J}$, dessen Index und Ordnung teilerfremd sind. Nach ZASSENHAUS ([*16*], S. 136) ist dann ${}_q\mathfrak{A} = \mathfrak{J}' \cap {}_q\mathfrak{A} \times \mathfrak{Z}(\mathfrak{J}) \cap {}_q\mathfrak{A}$, woraus $\mathfrak{Z}(\mathfrak{J}) \cap {}_q\mathfrak{A} = \mathfrak{E}$ folgt.

f) Sei nun $q \mid n$. Wir stellen $\mathfrak{G}$ dar als Permutationsgruppe $\mathfrak{G}^*$ der Nebenklassen nach einer der maximalen Untergruppen $\mathfrak{J}$, also vom Grad n, und können annehmen, daß diese Darstellung treu ist; andernfalls hätten wir nämlich einen in $\mathfrak{J}$ liegenden, daher auflösbaren Normalteiler von $\mathfrak{G}$ aufgefunden. Bei unserer Darstellung wird die Gruppe $\mathfrak{Z}_n$ regulär dargestellt. Da $\mathfrak{J}$ eine maximale Untergruppe von $\mathfrak{G}$ ist, ist diese Darstellung primitiv. Nach einem Satz von SCHUR [*11*] ist eine primitive Permutationsgruppe, deren Grad keine Primzahl ist und welche einen Vollzyklus (d.h. eine reguläre zyklische Untergruppe) enthält, zweifach transitiv. Alle diese Voraussetzungen sind in unserem Falle erfüllt, sofern n keine Primzahl ist. Ist aber n Primzahl, so ist nach einem Satz von BURNSIDE ([*2*], S. 341) $\mathfrak{G}^*$ zweifach transitiv oder auflösbar. Wir können also in jedem Falle annehmen, daß $\mathfrak{G}^*$ zweifach transitiv ist.

$\mathfrak{J}$ wird dargestellt durch eine Permutationsgruppe, welche eine Ziffer fest läßt, die übrigen $q-1$ Ziffern aber noch transitiv permutiert. Sei $\widetilde{\mathfrak{J}}$ diejenige

Untergruppe von $\mathfrak{J}$, welche noch eine weitere (beliebige, aber fest gewählte) Ziffer fest läßt. Dann gilt $(\mathfrak{J}:\bar{\mathfrak{J}}) = n-1$ und wegen $q \mid n$ sicher $q \nmid (\mathfrak{J}:\bar{\mathfrak{J}})$. Insbesondere können wir daher $\bar{\mathfrak{J}}$ noch so wählen, daß $\mathfrak{Z}_q \leq \bar{\mathfrak{J}}$ (gemeint ist natürlich das $\mathfrak{Z}_q$ mit $\mathfrak{J} = \mathfrak{Z}_q\mathfrak{A}$), also $\bar{\mathfrak{J}}$ die Gestalt $\bar{\mathfrak{J}} = \mathfrak{Z}_q\bar{\mathfrak{A}}$ mit geeignetem $\bar{\mathfrak{A}} < \mathfrak{A}$ hat. Da $\bar{\mathfrak{J}}$ in den $n-1$ Ziffern transitiv ist, enthält $\bar{\mathfrak{J}}$ keinen von $\mathfrak{E}$ verschiedenen Normalteiler von $\mathfrak{J}$. Wegen $\mathfrak{A} \lhd \mathfrak{J}$ gilt nun aber $\bar{\mathfrak{A}} \lhd \mathfrak{Z}_q\bar{\mathfrak{A}} = \bar{\mathfrak{J}}$. Daher folgt $\mathfrak{N}(\bar{\mathfrak{A}}) \geq \{\mathfrak{A}, \mathfrak{Z}_q\} = \mathfrak{J}$. Daraus ergibt sich $\bar{\mathfrak{A}} = \mathfrak{E}$ und dann $\bar{\mathfrak{J}} = \mathfrak{Z}_q$ und $(\mathfrak{A}) = n-1$. Sei nun r ein Primteiler von n mit $r \neq q$; gibt es kein solches r, so ist $\mathfrak{L}$ eine q-Gruppe und $\mathfrak{G}$ ist nach ITô [8] als Produkt einer abelschen Gruppe mit einer q-Gruppe $\mathfrak{L}$ auflösbar. Übergehen wir den trivialen Fall $\mathfrak{N}(\mathfrak{G}_r) = \mathfrak{G}$, so ist $\mathfrak{N}(\mathfrak{G}_r) = \mathfrak{L}$, sofern wir $\mathfrak{G}_r \leq \mathfrak{Z}_n$ wählen, was wegen $r \nmid (\mathfrak{A})$ geht. Nach einem Satz von SYLOW (SPEISER [12], S. 70, Satz 82) folgt $(\mathfrak{G}:\mathfrak{L}) = (\mathfrak{A}) = n-1 \equiv 1(r)$. Daraus erhalten wir $r \mid n-2$ und wegen $r \mid n$ schließlich $r = 2$. Nun haben wir wegen $q \neq r = 2$ die Beziehungen $n = 2^\alpha q^\beta$ und $(\mathfrak{G}) = n(n-1)q$. Daher ist $\mathfrak{G}_2 = \mathfrak{L}_2$ zyklisch, also bekanntlich (ZASSENHAUS [16], S. 133) $\mathfrak{G}/\mathfrak{G}'(2) \cong \mathfrak{G}_2$. Nach ITô [8] ist $\mathfrak{G}'(2) = \mathfrak{L}_q\mathfrak{A}$ auflösbar, womit wir fertig sind. Im folgenden dürfen wir daher annehmen, daß $q \nmid n$ gilt.

g) Wegen $q \nmid n$ ist eine beliebige q-SYLOW-Gruppe $\mathfrak{J}_q$ von $\mathfrak{J}$ auch q-SYLOW-Gruppe $\mathfrak{G}_q$ von $\mathfrak{G}$. Aus $\mathfrak{A} \lhd \mathfrak{J}$ und dem Ergebnis unter e) folgt $\mathfrak{N}(\mathfrak{G}_q) \cap {}_q\mathfrak{A} \leq \mathfrak{Z}(\mathfrak{J}) \cap {}_q\mathfrak{A} = \mathfrak{E}$. Daher ist $\mathfrak{G}_q$ in $\mathfrak{J}$ eigener Normalisator.

Wie unter e) folgt wegen $q \nmid n$ durch Anwendung des Satzes von ZASSENHAUS (diesmal mit $\mathfrak{Z}_n$ an Stelle von ${}_q\mathfrak{A}$ und $\mathfrak{L}$ an Stelle von $\mathfrak{J}$) die Beziehung $\mathfrak{Z}_n = \mathfrak{L}' \times \mathfrak{Z}(\mathfrak{L})$. Ist $\mathfrak{Z}(\mathfrak{L}) \neq \mathfrak{E}$, so gibt es eine Primzahl r mit $r \mid (\mathfrak{Z}(\mathfrak{L}))$. Dann ist $\mathfrak{L}'(r) \neq \mathfrak{L}$.

Schließen wir den trivialen Fall $\mathfrak{N}(\mathfrak{G}_r) = \mathfrak{G}$ aus, so dürfen wir mit $\mathfrak{G}_r = \mathfrak{L}_r$ annehmen, daß $\mathfrak{N}(\mathfrak{G}_r) = \mathfrak{L}$. Da $\mathfrak{G}_r$ abelsch ist, folgt nun nach GRÜN $\mathfrak{G}'(r) \neq \mathfrak{G}$. Wegen $\mathfrak{A} \leq \mathfrak{G}'(r)$ hat $\mathfrak{G}'(r)$ die Gestalt $\mathfrak{G}'(r) = \mathfrak{A}\tilde{\mathfrak{L}}$ und ist nach unserer Induktionsannahme oder nach ITô [8] (falls $\tilde{\mathfrak{L}}$ abelsch ist) auflösbar. Weiterhin können wir daher $\mathfrak{Z}(\mathfrak{L}) = \mathfrak{E}$ annehmen.

h) Sei $\mathfrak{G}_q = \mathfrak{Z}_q\mathfrak{A}_q$ und $X \in \mathfrak{N}(\mathfrak{G}_q)$. Dann hat X die Gestalt $X = Z_q^\alpha Z_n^\beta A$ mit $A \in \mathfrak{A}$ und geeigneten α, β. Nun erhalten wir

$$\mathfrak{Z}_q^X = \mathfrak{Z}_q^{Z_n^\beta A} \leq \mathfrak{A}\mathfrak{Z}_q, \quad \text{also} \quad \mathfrak{Z}_q^{Z_n^\beta} \leq \{\mathfrak{A}\mathfrak{Z}_q\}^{A^{-1}} \cap \mathfrak{L} = \mathfrak{A}\mathfrak{Z}_q \cap \mathfrak{L} = \mathfrak{Z}_q.$$

Somit ist $\mathfrak{Z}_q^{Z_n^\beta} = \mathfrak{Z}_q$, daher $Z_n^\beta \in \mathfrak{Z}(\mathfrak{L})$ und dann nach g) $Z_n^\beta = E$. Demnach liegt $\mathfrak{N}(\mathfrak{G}_q)$ in $\mathfrak{J}$ und nach obigem ist dann sogar $\mathfrak{N}(\mathfrak{G}_q) = \mathfrak{G}_q$. Ist $\mathfrak{G}_q$ abelsch und dann $\mathfrak{G}$ q-normal, so gilt nach GRÜN $\mathfrak{G}/\mathfrak{G}'(q) \cong \mathfrak{G}_q$. Dann folgt wegen $\mathfrak{Z}_n \leq \mathfrak{G}'(q)$ und ${}_q\mathfrak{A} \leq \mathfrak{G}'(q)$ sofort $\mathfrak{G}'(q) = \mathfrak{Z}_n\,{}_q\mathfrak{A}$ und $\mathfrak{G}'(q)$ ist nach ITô [8] auflösbar.

Ist aber $\mathfrak{G}_q' \neq \mathfrak{E}$, so liegt wegen $\mathfrak{A}_q \lhd \mathfrak{G}_q$ sicher $\mathfrak{Z}(\mathfrak{G}_q)$ in $\mathfrak{A}_q$. Dann haben wir $\mathfrak{A} \leq \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))$, also unter Ausschluß des trivialen Falles $\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q)) = \mathfrak{G}$ entweder $\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q)) = \mathfrak{A}$ oder $\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q)) = \mathfrak{J}$. Jedenfalls ist dann in $\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))$ eine von $\mathfrak{E}$ verschiedene q-Faktorgruppe abspaltbar. Ist $\mathfrak{G}$ q-normal, so liefert der GRÜNsche Satz uns $\mathfrak{G}'(q) \neq \mathfrak{G}$. Sicher ist $\mathfrak{Z}_n \leq \mathfrak{G}'(q)$ und ${}_q\mathfrak{A} \leq \mathfrak{G}'(q)$. Ferner haben wir ähnlich wie im Beweis von Satz 6, e) die Beziehungen

$$\mathfrak{G}'(q)_q = \mathfrak{G}'(q) \cap \mathfrak{G}_q \leq \mathfrak{G}'(q) \cap \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q)) = \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))'(q) \leq \mathfrak{A};$$

denn offenbar ist $\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))'(q) \leq \mathfrak{G}'(q) \cap \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))$ und es gilt sogar das Gleichheitszeichen, denn

$$\mathfrak{G}/\mathfrak{G}'(q) \cong \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))/\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))'(q) \qquad \text{(nach GRÜN)}$$

und

$$\mathfrak{G}/\mathfrak{G}'(q) = \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))\,\mathfrak{G}'(q)/\mathfrak{G}'(q) \cong \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))/\mathfrak{G}'(q) \cap \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q)),$$

woraus $(\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q))'(q)) = (\mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q)) \cap \mathfrak{G}'(q))$ folgt. Damit erhalten wir nun $\mathfrak{G}'(q) = \mathfrak{Z}_{n\,q}\mathfrak{A}\,\mathfrak{G}'(q)_q = \mathfrak{Z}_n\overline{\mathfrak{A}}$ mit geeignetem $\overline{\mathfrak{A}} < \mathfrak{A}$. Nach ITÔ [8] ist dann $\mathfrak{G}'(q)$ auflösbar. Weiterhin können wir also voraussetzen, daß $\mathfrak{G}$ nicht q-normal ist.

i) Da $\mathfrak{G}$ nicht q-normal ist, ist insbesondere $\mathfrak{G}_q' \neq \mathfrak{E}$ und dann wie unter h) $\mathfrak{Z}(\mathfrak{G}_q) \leq \mathfrak{A}_q$. In e) hatten wir gezeigt, daß $\mathfrak{Z}(\mathfrak{J}) \cap {}_q\mathfrak{A} = \mathfrak{E}$ ist. Damit ergibt sich nun $\mathfrak{Z}(\mathfrak{G}_q) = \mathfrak{Z}(\mathfrak{J})$.

Da $\mathfrak{G}$ nicht q-normal ist, gibt es ein Element $X \in \mathfrak{G}$ mit $\mathfrak{Z}(\mathfrak{G}_q)^X \leq \mathfrak{G}_q < \mathfrak{J}$, aber $\mathfrak{Z}(\mathfrak{G}_q)^X \neq \mathfrak{Z}(\mathfrak{G}_q)$. Wegen $\mathfrak{Z}(\mathfrak{G}_q) = \mathfrak{Z}(\mathfrak{J})$ ist sicher $X \notin \mathfrak{J}$, daher $\mathfrak{J}^X \neq \mathfrak{J}$, wenn wir den trivialen Fall $\mathfrak{J} \lhd \mathfrak{G}$ übergehen. Sei nun $(\mathfrak{Z}(\mathfrak{G}_q)) > q$. Aus $\mathfrak{Z}(\mathfrak{G}_q)^X \leq \mathfrak{G}_q$ folgt dann $\mathfrak{Z}(\mathfrak{G}_q)^X \cap \mathfrak{A}_q = \mathfrak{D} \neq \mathfrak{E}$ und $\mathfrak{N}(\mathfrak{D}) \geq \{\mathfrak{A}, \mathfrak{J}^X\}$. Wir dürfen annehmen, daß $\{\mathfrak{A}, \mathfrak{A}^X\} = \mathfrak{G}$: ist nämlich ${}_q\mathfrak{A}^X = {}_q\mathfrak{A}$, so folgt $\mathfrak{N}({}_q\mathfrak{A}) \geq \{\mathfrak{J}, X\} = \mathfrak{G}$ und wir sind für ${}_q\mathfrak{A} \neq \mathfrak{E}$ fertig; ist aber ${}_q\mathfrak{A}^X \neq {}_q\mathfrak{A}$, so besitzt $\{\mathfrak{A}, \mathfrak{A}^X\}$ mindestens zwei verschiedene Untergruppen der Ordnung $({}_q\mathfrak{A})$, kann daher mit keiner der maximalen Obergruppen $\mathfrak{J}$ von $\mathfrak{A}$ übereinstimmen, ist folglich gleich $\mathfrak{G}$; für ${}_q\mathfrak{A} = \mathfrak{E}$ schließlich ist $(\mathfrak{J}) = q^\gamma$ und $\mathfrak{G}$ nach ITÔ [8] auflösbar. Aus $\mathfrak{N}(\mathfrak{D}) \geq \{\mathfrak{A}, \mathfrak{J}^X\} \geq \{\mathfrak{A}, \mathfrak{A}^X\} = \mathfrak{G}$ erhalten wir nun $\mathfrak{D} \lhd \mathfrak{G}$. Im folgenden kann daher $(\mathfrak{Z}(\mathfrak{G}_q)) = q$ angenommen werden.

j) Sei X wie unter i) bestimmt und $\mathfrak{F} = \mathfrak{J} \cap \mathfrak{J}^X$. Ferner sei p eine Primzahl mit $p \mid (\mathfrak{F})$ und $p \neq q$. Dann ist $\mathfrak{N}(\mathfrak{F}_p) \geq \{\mathfrak{A}, \mathfrak{A}^X\} = \mathfrak{G}$ und wir sind fertig. Also können wir annehmen, daß $(\mathfrak{F}) = q^\varphi$. Weiter haben wir $(\mathfrak{F}/\mathfrak{F} \cap \mathfrak{A}_q) \mid q$ und ebenso $(\mathfrak{F}/\mathfrak{F} \cap \mathfrak{A}_q^X) \mid q$, woraus sich $(\mathfrak{F}/\mathfrak{F} \cap \mathfrak{A}_q \cap \mathfrak{A}_q^X) \mid q^2$ ergibt. Wir können annehmen, daß $\mathfrak{A}_q \cap \mathfrak{A}_q^X = \mathfrak{E}$ ist; sonst wäre nämlich $\mathfrak{N}(\mathfrak{A}_q \cap \mathfrak{A}_q^X) \geq \{\mathfrak{A}, \mathfrak{A}^X\} = \mathfrak{G}$. Daher ist $(\mathfrak{F}) \mid q^2$.

Ist $\mathfrak{H} = \mathfrak{Z}(\mathfrak{G}_q)^X \cap \mathfrak{A} \neq \mathfrak{E}$, so erhalten wir $\mathfrak{N}(\mathfrak{H}) \geq \{\mathfrak{A}, \mathfrak{J}^X\} \geq \{\mathfrak{A}, \mathfrak{A}^X\} = \mathfrak{G}$. Daher sei $\mathfrak{Z}(\mathfrak{G}_q)^X \cap \mathfrak{A} = \mathfrak{E}$ und dann wegen $\mathfrak{Z}(\mathfrak{G}_q)^X \leq \mathfrak{J}$ notwendig $\mathfrak{J} = \mathfrak{Z}(\mathfrak{G}_q)^X \mathfrak{A}$. Wegen $\mathfrak{Z}(\mathfrak{G}_q)^X \leq \mathfrak{G}_q$ ist ferner $\mathfrak{J}^X = \mathfrak{C}(\mathfrak{Z}(\mathfrak{G}_q)^X) \geq \mathfrak{Z}(\mathfrak{G}_q)$. Damit bekommen wir $\mathfrak{Z}(\mathfrak{G}_q) \leq \mathfrak{J} \cap \mathfrak{J}^X$ und dann $\mathfrak{F} = \mathfrak{J} \cap \mathfrak{J}^X \geq \mathfrak{Z}(\mathfrak{G}_q) \times \mathfrak{Z}(\mathfrak{G}_q)^X$ [wegen $\mathfrak{Z}(\mathfrak{G}_q) \neq \mathfrak{Z}(\mathfrak{G}_q)^X$ und $(\mathfrak{Z}(\mathfrak{G}_q)) = q$ tritt wirklich das direkte Produkt von $\mathfrak{Z}(\mathfrak{G}_q)$ und $\mathfrak{Z}(\mathfrak{G}_q)^X$ auf!]. Mit Hilfe von $(\mathfrak{F}) \mid q^2$ ergibt sich nun $\mathfrak{F} = \mathfrak{Z}(\mathfrak{G}_q) \times \mathfrak{Z}(\mathfrak{G}_q)^X$. Wegen $\mathfrak{G}_q' \neq \mathfrak{E}$ ist sicher $\mathfrak{F} \neq \mathfrak{G}_q$. Ferner ist $\mathfrak{C}(\mathfrak{F}) \leq \mathfrak{C}(\mathfrak{Z}(\mathfrak{G}_q)) = \mathfrak{J}$ und $\mathfrak{C}(\mathfrak{F}) \leq \mathfrak{C}(\mathfrak{Z}(\mathfrak{G}_q)^X) = \mathfrak{J}^X$, mithin $\mathfrak{C}(\mathfrak{F}) \leq \mathfrak{J} \cap \mathfrak{J}^X = \mathfrak{F}$. Die Faktorgruppe $\mathfrak{N}(\mathfrak{F})/\mathfrak{C}(\mathfrak{F}) = \mathfrak{N}(\mathfrak{F})/\mathfrak{F}$ ist daher isomorph zu einer Gruppe von Automorphismen von $\mathfrak{F}$, also isomorph zu einer Untergruppe der linearen Gruppe $GL(2, q)$ in zwei Dimensionen mod q. Wegen $\mathfrak{F} \neq \mathfrak{G}_q$ gibt es nun eine Untergruppe $\mathfrak{U}$ von $\mathfrak{G}_q$ mit $\mathfrak{F} \lhd \mathfrak{U}$ und $(\mathfrak{U}/\mathfrak{F}) = q$, ebenso gibt es eine Untergruppe $\mathfrak{V}$ von $\mathfrak{G}_q^X$ mit $\mathfrak{F} \lhd \mathfrak{V}$ und $(\mathfrak{V}/\mathfrak{F}) = q$. Wegen $\mathfrak{F} = \mathfrak{J} \cap \mathfrak{J}^X$ ist $\mathfrak{U} \neq \mathfrak{V}$. Daher besitzt $\mathfrak{N}(\mathfrak{F})/\mathfrak{F}$, dessen Ordnung nicht durch q^2 teilbar ist [als Untergruppe von $GL(2, q)$] bekanntlich mindestens $q+1$ q-SYLOW-Gruppen. Aber die volle lineare Gruppe $GL(2, q)$ besitzt nur $q+1$ q-SYLOW-Gruppen, und diese erzeugen die unimodulare Gruppe $SL(2, q)$. Wir haben damit gezeigt, daß $\mathfrak{N}(\mathfrak{F})$ bei Transformation auf $\mathfrak{F}$ sicher diejenigen Automorphismen bewirkt, welche linearen Abbildungen aus $SL(2, q)$ entsprechen.

$\mathfrak{Z}(\mathfrak{G}_q)$ möge von C erzeugt werden, so daß C und C^X eine Basis von $\mathfrak{F}$ bilden. Nach dem eben erhaltenen Ergebnis gibt es dann ein $Y \in \mathfrak{N}(\mathfrak{F})$ mit $C^Y = C^{-1}$ und $(C^X)^Y = (C^X)^{-1}$. Es folgt nun $Y \in \mathfrak{N}(\mathfrak{Z}(\mathfrak{G}_q)) = \mathfrak{F} = \mathfrak{C}(\mathfrak{Z}(\mathfrak{G}_q))$, also $C^Y = C^{-1} = C$. Für $q > 2$ ist dies ein Widerspruch, womit wir fertig sind. Für $q = 2$ ist aber unsere Behauptung schon in II, Satz 4 enthalten.

Damit ist Satz 7 in allen Teilen bewiesen.

Beweis von Satz 8 wieder durch Induktion nach $(\mathfrak{G})$. Die Voraussetzung, daß keine Untergruppe von $\mathfrak{G}$ sich homomorph auf die symmetrische Gruppe $\mathfrak{S}_5$ abbilden läßt, überträgt sich offenbar sofort auf Untergruppen und Faktorgruppen. Ferner hat jede Faktorgruppe $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ eine Zerlegung $\overline{\mathfrak{G}} = \overline{\mathfrak{L}}\overline{\mathfrak{A}}$; dabei ist $\overline{\mathfrak{L}}$ abelsch oder es hat einen zyklischen Normalteiler vom Index 2, erfüllt also die Voraussetzungen von Satz 4, oder es hat einen zyklischen Normalteiler vom Index 4 mit zyklischer Faktorgruppe, entspricht also den Voraussetzungen von Satz 8. Daher können wir annehmen, daß jedes von $\mathfrak{G}$ verschiedene homomorphe Bild von $\mathfrak{G}$ auflösbar ist. Somit genügt der Nachweis eines von $\mathfrak{E}$ verschiedenen auflösbaren Normalteilers von $\mathfrak{G}$.

a) Zunächst läßt sich ein Teil der Schlüsse von Satz 7 ungeändert übertragen. Wie dort können wir uns darauf beschränken, daß (a) $\mathfrak{A} \cap \mathfrak{L} = \mathfrak{E}$, (b) $\mathfrak{L}$ maximale Untergruppe von $\mathfrak{G}$ ist, (c) $\mathfrak{A}$ keine maximale Untergruppe von $\mathfrak{G}$ ist. Ist $\mathfrak{Z}_p$ der zyklische Normalteiler von $\mathfrak{L}$, so können wir wie in (c) annehmen, daß für eine $\mathfrak{A}$ echt umfassende maximale Untergruppe $\mathfrak{F}$ von $\mathfrak{G}$ gilt $\mathfrak{Z}_p \cap \mathfrak{F} = \mathfrak{E}$. Dann hat $\mathfrak{F}$ die Gestalt $\mathfrak{F} = \mathfrak{A}\mathfrak{Z}$, wobei nun aber $\mathfrak{Z}$ eine zyklische Untergruppe von $\mathfrak{L}$ der Ordnung 2 oder 4 sein kann (hier tritt ein Unterschied gegenüber dem Beweis von Satz 7 auf!). Ebenso wie in c) können wir voraussetzen, daß $p \nmid (\mathfrak{A})$.

b) Sei nun zunächst $\mathfrak{F}$ von der Gestalt $\mathfrak{F} = \mathfrak{A}\mathfrak{Z}_4$ mit $(\mathfrak{Z}_4) = 4$ und $\mathfrak{L} = \mathfrak{Z}_4\mathfrak{Z}_p$. Wir stellen $\mathfrak{F}$ dar als transitive Permutationsgruppe der Nebenklassen nach $\mathfrak{A}$, also vom Grad 4. Dabei werde $\mathfrak{F}$ auf $\overline{\mathfrak{F}} \cong \mathfrak{F}/\mathfrak{M}$ mit $\mathfrak{M} \leq \mathfrak{A}$ abgebildet. Da $\mathfrak{Z}_4$ auf einen 4-Zyklus abgebildet wird, enthält $\overline{\mathfrak{F}}$ ungerade Permutationen, ist daher von der alternierenden Gruppe verschieden. Auch $\overline{\mathfrak{F}} \cong \mathfrak{S}_4$ ist ausgeschlossen, denn die Untergruppe von $\overline{\mathfrak{F}}$, welche eine bestimmte Ziffer fest läßt, ist als homomorphes Bild von $\mathfrak{A}$ abelsch, während die entsprechende Untergruppe in $\mathfrak{S}_4$ nichtabelsch ist. Daher gilt also $(\overline{\mathfrak{F}}) = 2^\varrho$ mit $\varrho \leq 3$. Der Normalteiler $\mathfrak{M}$ umfaßt somit alle $\mathfrak{A}_q$ mit $q \geq 3$. Da $\mathfrak{M}$ als Untergruppe von $\mathfrak{A}$ abelsch ist, haben wir $\mathfrak{F}_q = \mathfrak{A}_q \trianglelefteq \mathfrak{M}$ und dann auch $\mathfrak{A}_q \triangleleft \mathfrak{F}$ für $q \geq 3$. Somit ist $\mathfrak{F}$ 2-nilpotent, d.h. $\mathfrak{F}$ besitzt ein invariantes 2-SYLOW-Komplement. Ist $\mathfrak{F}'$ nilpotent, so ist $\mathfrak{G} = \mathfrak{Z}_p\mathfrak{F}$ nach II, Satz 5 auflösbar.

Es gilt $\mathfrak{A} \leq \mathfrak{C}({}_2\mathfrak{A}) \trianglelefteq \mathfrak{N}({}_2\mathfrak{A}) = \mathfrak{F}$. Ist $\mathfrak{A} = \mathfrak{C}({}_2\mathfrak{A}) \triangleleft \mathfrak{F}$, so folgt $\mathfrak{F}' \leq \mathfrak{A}$ und $\mathfrak{F}'$ ist nilpotent. Ist aber $\mathfrak{C}({}_2\mathfrak{A}) = \mathfrak{F}$, so erhalten wir $\mathfrak{F} = {}_2\mathfrak{A} \times \mathfrak{F}_2$ und sogar $\mathfrak{F}$ selbst ist nilpotent, dann $\mathfrak{F}'$ erst recht. Es bleibt der Fall zu betrachten, daß $\mathfrak{C}({}_2\mathfrak{A})$ die Gestalt $\mathfrak{A}\mathfrak{Z}_2$ mit $(\mathfrak{Z}_2) = 2$ und $\mathfrak{Z}_2 < \mathfrak{L}$ hat. Dann ist $\mathfrak{C}({}_2\mathfrak{A})$ nilpotent und wegen $(\mathfrak{J}/\mathfrak{C}({}_2\mathfrak{A})) = 2$ bekommen wir $\mathfrak{J}' \leq \mathfrak{C}({}_2\mathfrak{A})$, womit auch in diesem Falle $\mathfrak{J}'$ nilpotent ist. Damit ist unser Satz auf Satz 5 von II zurückgeführt.

c) Nun sei $(\mathfrak{J}) = 2(\mathfrak{A})$ für jede $\mathfrak{A}$ umfassende maximale Untergruppe $\mathfrak{J}$ von $\mathfrak{G}$ und dann $\mathfrak{A} \lhd \mathfrak{J}$. Ein solches $\mathfrak{J}$ hat die Gestalt $\mathfrak{J} = \mathfrak{Z}_2\mathfrak{A}$ mit $\mathfrak{Z}_2 < \mathfrak{Z}_4 < \mathfrak{L}$. Eine geeignete 2-Sylow-Gruppe von $\mathfrak{G}$ hat die Gestalt $\mathfrak{G}_2 = \tilde{\mathfrak{Z}}_4\mathfrak{A}_2$. Gibt es ein $\mathfrak{K}$ mit $\mathfrak{K} \lhd \mathfrak{G}_2$ und $\mathfrak{K} \leq \mathfrak{A}_2$, so erhalten wir $\mathfrak{N}(\mathfrak{K}) \geq \{\mathfrak{A}, \tilde{\mathfrak{Z}}_4\} = \mathfrak{G}$ und sind fertig. Daher können wir annehmen, daß $\mathfrak{A}_2$ keinen Normalteiler von $\mathfrak{G}_2$ enthält. Die Darstellung von $\mathfrak{G}_2$ als Permutationsgruppe der Nebenklassen von $\mathfrak{A}_2$ ist daher treu und vom Grad 4. Daraus folgt $(\mathfrak{G}_2) \mid 8$, also $(\mathfrak{A}_2) \mid 2$.

Sei zuerst $2 \nmid (\mathfrak{A})$. Nun stellen wir $\mathfrak{G}$ dar als Permutationsgruppe der Nebenklassen von $\mathfrak{A}$, also vom Grad $4p$. Diese Darstellung kann als treu angenommen werden, da sonst $\mathfrak{A}$ einen auflösbaren, von $\mathfrak{E}$ verschiedenen Normalteiler von $\mathfrak{G}$ enthalten würde. Bei dieser Darstellung wird $\mathfrak{L}$ regulär dargestellt. Ein erzeugendes Element Z_4 von $\mathfrak{Z}_4$ besteht daher aus p Zyklen der Länge 4, ist also ungerade. Die geraden Permutationen von $\mathfrak{G}$ bilden daher einen Normalteiler $\mathfrak{K} \neq \mathfrak{G}$. Wegen $2 \neq p$ und $2 \nmid (\mathfrak{A})$ gilt $\mathfrak{Z}_p \leq \mathfrak{K}$ und $\mathfrak{A} \leq \mathfrak{K}$, also $\mathfrak{K} = \bar{\mathfrak{L}}\mathfrak{A}$ mit $\bar{\mathfrak{L}} < \mathfrak{L}$. $\bar{\mathfrak{L}}$ hat die Ordnung $2p$, ist daher abelsch oder eine Diedergruppe. Nach Itô [8] oder II, Satz 4 folgt die Auflösbarkeit von $\mathfrak{G}$.

Nun sei $(\mathfrak{A}_2) = 2$. Wir stellen $\mathfrak{G}$ dar als Permutationsgruppe $\bar{\mathfrak{G}}$ der Nebenklassen von $\mathfrak{L}$ und können annehmen, daß diese Darstellung treu ist. Da $\mathfrak{L}$ maximale Untergruppe von $\mathfrak{G}$ ist, ist $\bar{\mathfrak{G}}$ primitiv. $\bar{\mathfrak{A}}$ ist eine reguläre abelsche Permutationsgruppe mit zyklischer 2-Sylow-Gruppe. Nach Wielandt [14] ist dann $\bar{\mathfrak{G}}$ zweifach transitiv. Mit $(\mathfrak{A}) = a$ folgt $a - 1 \mid 4p = (\mathfrak{L})$.

Andererseits ist $\mathfrak{N}(\mathfrak{G}_p) \geq \mathfrak{L}$ für $\mathfrak{G}_p = \mathfrak{Z}_p$, also unter Ausschluß des trivialen Falles $\mathfrak{N}(\mathfrak{G}_p) = \mathfrak{G}$ wegen der Maximalität von $\mathfrak{L}$ sicher $\mathfrak{N}(\mathfrak{G}_p) = \mathfrak{L}$. Ein bekannter Satz von Sylow besagt nun

$$(\mathfrak{G} : \mathfrak{N}(\mathfrak{G}_p)) = (\mathfrak{G} : \mathfrak{L}) = (\mathfrak{A}) = a \equiv 1\,(p),$$

also $p \mid a - 1 \mid 4p$. Es bleiben die Möglichkeiten $p = a - 1$, $2p = a - 1$, $4p = a - 1$. Wegen $2 \mid a$ kommt aber nur $p = a - 1$ in Frage.

Für $q \geq 3$ und $q \mid (\mathfrak{A})$ ist $\mathfrak{A}_q \trianglelefteq \mathfrak{A} \lhd \mathfrak{J}$, also $\mathfrak{A}_q \lhd \mathfrak{J}$. Unter Ausschluß von $\mathfrak{N}(\mathfrak{A}_q) = \mathfrak{G}$ folgt $\mathfrak{N}(\mathfrak{A}_q) = \mathfrak{J}$, daher wegen $\mathfrak{A}_q = \mathfrak{G}_q$ wieder nach Sylow $(\mathfrak{G} : \mathfrak{N}(\mathfrak{A}_q)) = (\mathfrak{G} : \mathfrak{J}) = 2p \equiv 1\,(q)$. Andererseits ist $q \mid a = p + 1$, daher auch $q \mid (2p - 1) + (p + 1) = 3p$, also $q = 3$ wegen $q \neq p$. Daraus bekommen wir nun $a = 3^\alpha 2$. Die gleiche Überlegung liefert uns $(\mathfrak{G} : \mathfrak{N}(\mathfrak{G}_3)) = 2p = 2(a - 1) = 2(2\,3^\alpha - 1) \equiv 1 - 3\ (3^2)$ für $\alpha > 1$. Nach Grün [3] gilt folgender Satz:

Sei $p^n \top (\mathfrak{G})$, $(\mathfrak{G} : \mathfrak{N}(\mathfrak{G}_p)) \equiv 1 + a p^m\ (p^{m+1})$ mit $(a, p) = 1$. Dann gibt es ein $\mathfrak{G}_p^T \neq \mathfrak{G}_p$ mit $(\mathfrak{G}_p \cap \mathfrak{G}_p^T) \geq p^{n-m}$.

In unserem vorliegenden Falle ist $m = 1$. Mit $\mathfrak{D} = \mathfrak{G}_3 \cap \mathfrak{G}_3^T$ erhalten wir daher $(\mathfrak{D}) \geq 3^{\alpha-1}$. Ferner ist $\mathfrak{N}(\mathfrak{D}) \geq \{\mathfrak{A}, \mathfrak{A}^T\}$. Da $\mathfrak{N}(\mathfrak{D})$ sicher die verschiedenen 3-Sylow-Gruppen $\mathfrak{A}_3$ und $\mathfrak{A}_3^T$ umfaßt, aber $\mathfrak{J}$ nur eine 3-Sylow-Gruppe hat, folgt $\mathfrak{N}(\mathfrak{D}) = \mathfrak{G}$ und wir sind fertig, falls $\alpha > 1$ ist. Ist aber $\alpha = 1$, so haben wir $a=6$, $p=5$ und $(\mathfrak{G})=120$. Dann besitzt $\mathfrak{G}$ eine treue Darstellung vom Grad 6 (Permutation der Nebenklassen von $\mathfrak{L}$), ist somit bekanntlich zur symmetrischen $\mathfrak{S}_5$ isomorph.

Literatur

[1] BRAUER, R., and H. F. TUAN: On simple groups of finite order. Bull. Amer. Math. Soc. **51**, 756—766 (1945). — [2] BURNSIDE, W.: Theory of groups of finite order, sec. edit. 1911. — [3] GRÜN, O.: Beiträge zur Gruppentheorie. III. Math. Nachr. **1**, 1—24 (1948). — [4] HALL, P.: A note on soluble groups. J. London Math. Soc. **3**, 98—105 (1928). — [5] HUPPERT, B.: Über die Auflösbarkeit faktorisierbarer Gruppen. Math. Z. **59**, 1—7 (1953). — [6] HUPPERT, B.: Normalteiler und maximale Untergruppen endlicher Gruppen. Math. Z. **60**, 409—434 (1954). — [7] HUPPERT, B., u. N. ITÔ: Über die Auflösbarkeit faktorisierbarer Gruppen. II. Math. Z. **61**, 94—99 (1954). — [8] ITÔ, N.: Remarks on factorisable groups. Acta Sci. Math. Szeged **14**, 83—84 (1951). — [9] ORE, O.: Contributions to the theory of groups of finite order. Duke Math. J. **5**, 431—460 (1938). — [10] PERRON, O.: Algebra II, 2. Aufl. 1933. — [11] SCHUR, I.: Zur Theorie der einfach transitiven Permutationsgruppen. Sitzgsber. Berl. Akad. **1933**, 598—623. — [12] SPEISER, A.: Die Theorie der Gruppen von endlicher Ordnung, 3. Aufl. 1937. — [13] SZÉP, J., u. L. RÉDEI: On factorisable groups. Acta Sci. Math. Szeged **13**, 235—238 (1950). — [14] WIELANDT, H.: Zur Theorie der einfach transitiven Permutationsgruppen. Math. Z. **40**, 582—587 (1936). — [15] WIELANDT, H.: Über das Produkt paarweise vertauschbarer nilpotenter Gruppen. Math. Z. **55**, 1—7 (1951). — [16] ZASSENHAUS, H.: Lehrbuch der Gruppentheorie, Bd. I. 1937.

Tübingen, Mathematisches Institut der Universität

(Eingegangen am 28. April 1955)

PUTNAM, C. R.
Math. Zeitschr. Bd. 64, S. 149/50 (1956)

A Note on Inverses of Differential Operators*)

By

C. R. PUTNAM

Let $q_1(t)$, $q_2(t)$ be continuous, real-valued functions on the half-line $0 \leq t < \infty$ and consider the differential operators L_1, L_2:

$$(1_1) \quad L_1 x = -x'' - q_1 x, \qquad (1_2) \quad L_2 x = -x'' - q_2 x,$$

with respective domains consisting of the functions $x = x(t)$ which satisfy a fixed boundary condition, say $x(0) = 0$, have absolutely continuous first derivatives, and, together with $L_1 x$ or $L_2 x$, are of class $L^2[0, \infty)$. Then $L_1 - L_2$, where $L_1 x - L_2 x = (q_2 - q_1) x$, has a domain $\Omega = \mathfrak{D}_{L_1} \mathfrak{D}_{L_1}$ dense on $L^2[0, \infty)$. Suppose that both L_1 and L_2 are self-adjoint (that is, of the limit-point type) and let z be any complex number not in the spectrum of L_1 or L_2 (e.g., z any non-real complex number). Then both operators $(L_k - zI)^{-1}$ are normal and bounded. If $y = (L_1 - zI)^{-1} x$ is in Ω, an application of the operator equation

$$(2) \qquad (L_1 - zI) - (L_2 - zI) = (q_2 - q_1) I \qquad (I, \text{ the identity operator}),$$

valid on Ω $(= \mathfrak{D}_{L_1 - zI} \mathfrak{D}_{L_2 - zI})$, to y, followed by an application of $(L_2 - zI)^{-1}$ to the resulting functional equation shows that the operator equation

$$(3) \qquad (L_2 - zI)^{-1} - (L_1 - zI)^{-1} = (L_2 - zI)^{-1} [(q_2 - q_1) I] (L_1 - zI)^{-1}$$

holds for all elements x in $(L_1 - zI)\Omega$.

It was pointed out in [2], p. 84, that standard theorems in the theory of operators imply that if

$$(4) \qquad |q_2(t) - q_1(t)| < \text{const},$$

so that $L_1 - L_2$ is bounded on its domain, and if (1_1) is of the limit-point type (so that L_1 is self-adjoint), then (1_2) is of the limit-point type. If (1_1) and/or (1_2) are of the limit-point type and if

$$(5) \qquad q_2(t) - q_1(t) \to 0 \quad \text{as} \quad t \to \infty,$$

then the essential (cluster) spectra S_1', S_2' of (1_1), (1_2) are identical; cf. [1], [3]. It was remarked in [2], p. 84, that this fact is a consequence of standard theorems in the theory of operators; however, the indications of the proof *loc. cit.* are incorrect. A simple proof of this fact as a consequence of the equation (3) will be given below. In fact, it will be shown that *the difference*

*) This work was supported by the National Science Foundation research grant NSF—G 481.

$(L_2 - zI)^{-1} - (L_1 - zI)^{-1}$ *is completely continuous whenever* (5) *holds* [although $(q_2 - q_1) I$ is completely continuous only when $q_1(t) \equiv q_2(t)$, that is, when $L_1 = L_2$].

In view of (5), or even (4), $\mathfrak{D}_{L_1} = \mathfrak{D}_{L_2}$, hence $\Omega = \mathfrak{D}_{L_1}$ $(= \mathfrak{D}_{L_1 - zI})$. Consequently, $(L_1 - zI)\Omega$ is the entire HILBERT space $\mathfrak{H}$: $L^2[0, \infty)$ and (3) holds for all x in H. [Of course, this last assertion holds whenever $(L_1 - zI)\Omega$ is dense, whether or not (5), or (4), is assumed.] The operator $(L_1 - zI)^{-1}$ is the integral operator belonging to a GREEN kernel $G(t, s)$ for which $\|G(t, .)\|$ is a continuous function of t. Hence if the elements $x_1(t), x_2(t), \ldots$ of $\mathfrak{H}$ tend weakly to 0 as $n \to \infty$, then the sequence of functions

$$y_n(t) = (L_1 - zI)^{-1} x_n = \int_0^\infty G(t, s)\, x_n(s)\, ds$$

is uniformly bounded on every t-interval, is such that $y_n(t) \to 0$ as $n \to \infty$ for every fixed t, and satisfies $\|y_n\| <$ const. The boundedness of $(L_k - zI)^{-1}$ and relation (5) now imply that $[(q_2 - q_1) I]\,(L_1 - zI)^{-1}$, hence $(L_2 - zI)^{-1}[(q_2 - q_1) I]\,(L_1 - zI)^{-1}$, is completely continuous. The italicized assertion now follows from (3); as a consequence, the essential spectra of $(L_k - zI)^{-1}$ are identical, and hence also $S_1' = S_2'$.

References

[1] HARTMAN, P.: On the spectra of slightly disturbed linear oscillators. Amer. J. Math. **71**, 71—79 (1949). — [2] HARTMAN, P., and A. WINTNER: On perturbations of the continuous spectrum of the harmonic oscillator. Amer. J. Math. **74**, 79—85 (1952). — [3] PUTNAM, C. R.: The comparison of spectra belonging to potentials with a bounded difference. Duke Math. J. **18**, 267—273 (1951).

Dept. of Math., Purdue University, Lafayette, Ind. (U.S.A.)

(Eingegangen am 21. Juli 1955)

JURKAT, W., u. A. PEYERIMHOFF
Math. Zeitschr. Bd. 64, S. 151—158 (1956)

Lokalisation bei absoluter Cesàro-Summierbarkeit von Potenzreihen und trigonometrischen Reihen. II*)

Von
WOLFGANG JURKAT und ALEXANDER PEYERIMHOFF

Dieser zweite Teil unserer Arbeit befaßt sich mit den Lokalisationsverhältnissen bei absoluter Summierbarkeit von FOURIER-Reihen. Während bei trigonometrischen Reihen die Summierbarkeit nach I mit dem lokalen Verhalten eines mehrfachen Integrales zusammenhängt, können wir im Spezialfall der FOURIER-Reihen die Lokalisation auch direkt auf die erzeugende Funktion beziehen. Dabei treten entscheidend gewisse Koeffizientenbedingungen auf, von deren Erfülltsein es abhängt, ob für die FOURIER-Reihen einer Klasse von Funktionen Lokalisation besteht oder nicht. Durch die Untersuchung dieser Bedingungen für zahlreiche bekannte Klassen ist es möglich, in vollständiger und einheitlicher Form die Lokalisationsverhältnisse zu beschreiben. Unsere Resultate umfassen insbesondere die vielen bisher bekannten Einzelergebnisse auf diesem Gebiet.

§ 4. Allgemeine Lokalisationssätze für FOURIER-Reihen

4.1. Nach I, Satz 2 ist die Summierbarkeit einer trigonometrischen Reihe abhängig vom lokalen Verhalten eines $(k+p+2)$-fachen Integrales und von einer Koeffizientenbedingung. Bei FOURIER-Reihen können wir auf Grund der gliedweisen Integrierbarkeit an Stelle des Integrales auch die erzeugende Funktion heranziehen und erhalten so

Satz 4. *Zwei* FOURIER-*Reihen* $f(\varphi) \sim \sum\limits_0^\infty \Re a_n e^{in\varphi}$ *und* $g(\varphi) \sim \sum\limits_0^\infty \Re b_n e^{in\varphi}$ *sind genau dann für* $|\varphi| < \varepsilon$, $0 < \varepsilon < \pi$, $|C_\alpha|$*-äquisummierbar* $(\alpha > -1)$, *wenn gilt:*

a) Für eine ganze Zahl $p \geq 0$ *ist*

$$\overline{\Delta}^p \frac{a_n - b_n}{(n+1)^\alpha} = a(1) \quad \textit{oder auch} \quad \overline{\Delta}^p (a_n - b_n) = a(n^\alpha);$$

b) es gibt eine periodische Funktion $h(\varphi)$, *die für fast alle* $|\varphi| < \varepsilon$ *mit* $f(\varphi) - g(\varphi)$ *übereinstimmt und deren* FOURIER-*Reihe für* $|\varphi| < \varepsilon$ $|C_\alpha|$*-summierbar ist.*

---

*) Der erste Teil dieser Arbeit — fortan als I zitiert — erschien in Math. Z. **60**, 255—270 (1954). Die Numerierung der Sätze, Formeln und Fußnoten erfolgt hier im Anschluß an den ersten Teil, auf den auch bezüglich der Bezeichnungen grundsätzlich verwiesen sei. [Zum Beispiel bedeutet $x_n = a(y_n)$, daß von einer Stelle ab $x_n = a_n y_n$ ist mit $\sum |a_n - a_{n-1}| < \infty$.] Das Literaturverzeichnis für den zweiten Teil befindet sich am Schluß der vorliegenden Note.

Die genauen Bedingungen für die $|C_\alpha|$-Äquisummierbarkeit der konjugierten Reihen $\sum \mathfrak{I} a_n e^{in\varphi}$ und $\sum \mathfrak{I} b_n e^{in\varphi}$ für $|\varphi| < \varepsilon$ sind:

$\bar{a}) = a)$ und

$\bar{b})$ es gibt eine periodische Funktion $h(\varphi)$, die für fast alle $|\varphi| < \varepsilon$ mit $f(\varphi) - g(\varphi)$ übereinstimmt und deren konjugierte FOURIER*-Reihe für $|\varphi| < \varepsilon$ $|C_\alpha|$-summierbar ist.*

Zusatz 1. Ersetzt man die $|C_\alpha|$-Summierbarkeit durch gewöhnliche C_α-Summierbarkeit, so bleibt Satz 4 wörtlich richtig, wenn man bei a) $=$ ā) entsprechend a durch o ersetzt.

Zusatz 2. Ersetzt man die $|C_\alpha|$-Summierbarkeit für $|\varphi| < \varepsilon$ durch gleichmäßige C_α-Summierbarkeit in jedem abgeschlossenen Teilintervall von $|\varphi| < \varepsilon$, so bleibt Satz 4 wieder wörtlich richtig, wenn man bei a) $=$ ā) entsprechend a durch o ersetzt.

4.2. *Beweis.* Die Notwendigkeit von a) $=$ ā) folgt aus I, Satz 2, und die Notwendigkeit von b) bzw. $\bar{b}$) erkennt man sofort, indem man $b(\varphi) = f(\varphi) - g(\varphi)$ setzt für $0 \leq \varphi \leq 2\pi$.

Für den hinreichenden Teil des Beweises zeigen wir durch Anwendung von I, Satz 2, daß die FOURIER-Reihen bzw. konjugierten FOURIER-Reihen von $f - g$ und h äquisummierbar sind für $|\varphi| < \varepsilon$. Ist $h(\varphi) \sim \sum \Re c_n e^{in\varphi}$, so ist zunächst wegen b) bzw. $\bar{b}$) nach Satz 2 $\bar{\Delta}^p \frac{c_n}{(n+1)^\alpha} = a(1)$ oder auch $\bar{\Delta}^p c_n = a(n^\alpha)$. Außerdem ist das $(k+p+2)$-fache Integral der FOURIER-Reihe von $(f-g) - h$ ein Polynom eines Grades $\leq k+p+1$ für $|\varphi| < \varepsilon$ (denn FOURIER-Reihen dürfen gliedweise integriert werden). Daraus folgt die behauptete Äquisummierbarkeit nach Satz 2 (beachte I, § 2.4; dort steht in der vorletzten Zeile auf S. 266 versehentlich $k+p+2$ statt $k+p+1$).

Die Zusätze von Satz 4 lassen sich ebenso auf die Zusätze von Satz 2 zurückführen.

4.3. Nach Satz 4 ist das Summierungsverhalten von FOURIER-Reihen abhängig von lokalen Eigenschaften der erzeugenden Funktion für alle FOURIER-Reihen, deren Koeffizienten eine vom Index des Verfahrens abhängige Bedingung erfüllen (Satz 4 mit $h \equiv 0$). Es erscheint nun ganz natürlich, Klassen von erzeugenden Funktionen[22]) zu betrachten, für welche die Koeffizientenbedingung wegfällt, d.h. für alle Funktionen der Klasse erfüllt ist. Naturgemäß werden solche Klassen vom Index des Verfahrens abhängen. Den einfachsten Fall bietet der Raum aller (integrierbaren und mit 2π periodischen) Funktionen, d.h. der Fall des gewöhnlichen RIEMANNschen Lokalisationssatzes für FOURIER-Reihen (daß hier die Koeffizientenbedingung wegfällt, ist gerade der Inhalt des RIEMANNschen Lemmas).

Definition. Es sei eine Funktionenklasse K vorgegeben. $|C_\alpha|$-Lokalisation für die FOURIER-Reihen (konjugierten FOURIER-Reihen) aus K an einer

[22]) Das heißt stets integrierbare und mit 2π periodische Funktionen. Wir werden dies im folgenden oft stillschweigend voraussetzen.

Stelle φ_0 bedeutet: Sind $f, g \in K$ und $0 < \varepsilon < \pi$, so hat $f(\varphi) = g(\varphi)$ für $|\varphi - \varphi_0| < \varepsilon$ stets die $|C_\alpha|$-Äquisummierbarkeit ($\alpha > -1$) der FOURIER-Reihen (konjugierten FOURIER-Reihen) von f und g an der Stelle φ_0 zur Folge.

Eine entsprechende Definition gilt für (gewöhnliche) C_α-Lokalisation (die wegen $|C_\alpha| \subseteqq C_\alpha$ stets eine Folge der $|C_\alpha|$-Lokalisation ist).

Besteht C_α-Lokalisation für die FOURIER-Reihen (konjugierten FOURIER-Reihen) aus einer Klasse K an allen Stellen φ, so folgt aus der obigen Definition sofort: Ist J ein beliebiges offenes Intervall, $f, g \in K$ und $f(\varphi) = g(\varphi)$ in J, so sind die FOURIER-Reihen (konjugierten FOURIER-Reihen) von f und g in ganz J C_α-äquisummierbar. Wenn hier sogar gleichmäßige C_α-Äquisummierbarkeit in jedem abgeschlossenen Teilintervall von J folgt, so sprechen wir von (überall) gleichmäßiger C_α-Lokalisation[23]).

Es sei K eine Funktionenklasse mit der Eigenschaft, daß die FOURIER-Koeffizienten der Funktionen aus K für ein $\beta \geqq -2$ die Bedingung $a_n = O(n^\beta)$ erfüllen. Nach Satz 4 und wegen $O(n^\beta) = o(n^\alpha)$ für $\alpha > \beta + 1$ gilt dann:

Für die FOURIER-*Reihen und konjugierten* FOURIER-*Reihen aus K liegt $|C_\alpha|$-Lokalisation überall vor für jedes $\alpha > \beta + 1$.*

Diese Tatsache kann man z. B. verwenden, um bei speziellen Reihen zu einer Aussage über Summierbarkeit zu gelangen. Betrachten wir etwa die FOURIER-Reihe $-\log\left(2 \sin \frac{\varphi}{2}\right) \sim \sum \frac{\cos n\varphi}{n}$, so ergibt sich wegen $\beta = -1$, daß die Reihe $|C_\alpha|$-summierbar ist für $\varphi \neq 0 \pmod{2\pi}$ und jedes $\alpha > 0$, denn die erzeugende Funktion ist für $\varphi \neq 0$ zweimal stetig differenzierbar. Entsprechendes gilt für die konjugierte Reihe $\sum \frac{\sin n\varphi}{n}$; übrigens hätten sich diese Tatsachen auch direkt durch Anwendung von I, Satz 1 auf $\sum \frac{z^n}{n}$ ergeben.

4.4. Wir werden im folgenden die Gültigkeit von Lokalisationssätzen gemäß unserer Definition in § 4.3 untersuchen. Um notwendige und hinreichende Bedingungen zu erhalten, werden wir nur Klassen K mit folgenden Eigenschaften betrachten: K ist nicht leer, und mit $f(\varphi) \in K$ ist auch $\lambda(\varphi) f(2\varphi) \in K$ für jede zweimal stetig differenzierbare (periodische) Funktion $\lambda(\varphi)$.

Tatsächlich wird dies nur benutzt werden für $\lambda \equiv 0$ und für eine spezielle Funktion λ mit nachstehenden Eigenschaften:

$$\lambda(\varphi) = 1 - \lambda(\varphi + \pi) \quad \text{für} \quad -\pi \leqq \varphi \leqq 0, \qquad \lambda(\varphi) = 0 \quad \text{für} \quad |\varphi| \leqq \frac{\pi}{3}.$$

Ist $f(\varphi) \sim \sum \Re a_n e^{in\varphi}$ und $f^*(\varphi) = \lambda(\varphi) f(2\varphi) \sim \sum \Re b_n e^{in\varphi}$, so gilt dann für $n \geqq 1$

$$(15) \qquad \begin{cases} b_{2n} = \dfrac{1}{\pi}\left(\displaystyle\int_{-\pi}^{0} + \int_{0}^{\pi}\right) \lambda(\varphi) f(2\varphi) e^{-2ni\varphi} d\varphi \\[2ex] \quad = \dfrac{1}{\pi} \displaystyle\int_0^\pi \big(1 - \lambda(\varphi) + \lambda(\varphi)\big) f(2\varphi) e^{-2ni\varphi} d\varphi = \dfrac{1}{2} a_n. \end{cases}$$

---

[23]) Gleichmäßige Lokalisation wird also nur für alle φ erklärt.

Für alle „zulässigen" Klassen K gilt nun

Satz 5. *Für die* FOURIER-*Reihen* $\sum \Re a_n e^{in\varphi}$ *aus einer Klasse* K *besteht genau dann* $|C_\alpha|$-*Lokalisation* ($\alpha > -1$) *für* $\varphi = 0$, *wenn für alle Reihen aus* K

$$\Re a_n = a(n^\alpha) \tag{16}$$

gilt, und $|C_\alpha|$-*Lokalisation an allen Stellen besteht genau dann, wenn für alle Reihen aus* K

$$\sum \left| \frac{a_n}{n^\alpha} \right| < \infty \tag{17}$$

gilt. Dies bleibt wörtlich richtig für Lokalisation bei konjugierten Reihen, wenn überall $\Re$ *durch* $\Im$ *ersetzt wird.*

Zusatz 1. Ersetzt man $|C_\alpha|$-Summierbarkeit durch gewöhnliche C_α-Summierbarkeit, so bleibt Satz 5 wörtlich richtig, wenn man (16) und (17) ersetzt durch

$$(16') \qquad \Re a_n = o(n^\alpha) \qquad \text{bzw.} \qquad (17') \qquad a_n = o(n^\alpha).$$

Zusatz 2. Gleichmäßige C_α-Lokalisation für die FOURIER-Reihen oder konjugierten Reihen aus K liegt genau dann vor, wenn (17') gilt, so daß gleichmäßige C_α-Lokalisation mit gewöhnlicher C_α-Lokalisation überall äquivalent ist (insbesondere also aus $|C_\alpha|$-Lokalisation überall folgt).

4.5. *Beweis.* Um die Notwendigkeit von (16) bzw. (17) zu zeigen, betrachten wir zu beliebigem $f \in K$ die Funktion $f^* = \lambda(\varphi) f(2\varphi)$. Da $f^* = 0$ ist für $|\varphi| \leq \frac{\pi}{3}$, so haben wir wegen der Lokalisation für $\varphi = 0$ bzw. $|\varphi| < \frac{\pi}{3}$ $|C_\alpha|$-Summierbarkeit, insbesondere nach I, Hilfssatz 6 oder 8

$$\Re b_n = a(n^\alpha) \qquad \text{bzw.} \qquad \sum \frac{|b_n|}{n^\alpha} < \infty.$$

Wegen (15) ergibt sich daraus (16) bzw. (17).

Daß (17) auch hinreichend ist, folgt unmittelbar aus Satz 4 (vgl. I, § 2.4). Um diesen Satz auch bei (16) anwenden zu können, betrachten wir statt $f(\varphi) \sim \sum \Re a_n e^{in\varphi} \in K$ die FOURIER-Reihe

$$f_1(\varphi) = \tfrac{1}{2}\big(f(\varphi) + f(-\varphi)\big) \sim \sum \Re a_n \cos n\varphi.$$

Im Falle der konjugierten Reihen schließt man ganz entsprechend [natürlich gilt I, Hilfssatz 8 auch für die konjugierten Reihen; an Stelle von f_1 ist jetzt $f_2 = \frac{1}{2}\big(f(\varphi) - f(-\varphi)\big)$ zu betrachten].

Bei Zusatz 1 schließt man analog. Zusatz 2 schließlich folgt durch Kombination von Zusatz 1 und Satz 4.

Wie der Beweis zeigt, wird die Einschränkung auf zulässige Klassen nur für den notwendigen Teil des Satzes gebraucht, während der hinreichende Teil für jede Klasse gilt.

§ 5. Spezielle Lokalisationssätze für FOURIER-Reihen

Im folgenden werden wir für einige bekannte Funktionenklassen das Lokalisationsverhalten der FOURIER-Reihen bzw. konjugierten Reihen auf Grund von Satz 5 bestimmen. Alle auftretenden Klassen werden zulässig in dem eingeführten Sinne sein. Es wird kein Punkt φ bevorzugt werden, so daß also Lokalisation stets Lokalisation überall bedeutet und zwischen gewöhnlicher und gleichmäßiger C_α-Lokalisation kein Unterschied besteht. Wir werden somit nur die Bedingungen (17) und (17′) zu betrachten haben, die für FOURIER-Reihen und konjugierte FOURIER-Reihen gleich lauten. Aus diesem Grund können wir die kurze Aussage „eine Klasse K besitzt $|C_\alpha|$-Lokalisation (bzw. C_α-Lokalisation)“ verwenden und verstehen darunter Lokalisation (überall) für FOURIER-Reihen und konjugierte FOURIER-Reihen.

5.1. Wir betrachten zunächst die Räume L, L^p $(p>1)$, B und C [24]).

Satz 6. *Jede Klasse K zwischen L und C, $L \supseteqq K \supseteqq C$, besitzt C_α-Lokalisation für $\alpha \geqq 0$ und nicht für $\alpha < 0$* [25]).

Zum *Beweis* genügt es zu bemerken, daß (17′) für L und $\alpha \geqq 0$ erfüllt ist (RIEMANNsches Lemma), während (17′) für C und $\alpha < 0$ nicht gilt (vgl. TS, § 2.9.2).

5.2. Satz 7. *Die Klasse L besitzt $|C_\alpha|$-Lokalisation für $\alpha > 1$ und nicht für $\alpha \leqq 1$* [26]).

Zum *Beweis* genügt es zu bemerken, daß (17) für $\alpha > 1$ erfüllt ist (RIEMANNsches Lemma), während die FOURIER-Reihe $\sum \Re \frac{e^{in\varphi}}{\log n}$ ein Gegenbeispiel für $\alpha \leqq 1$ darstellt (vgl. TS, § 5.12).

5.3. Satz 8. *Die Klasse L^p $(1 < p \leqq 2)$ besitzt $|C_\alpha|$-Lokalisation für $\alpha > \frac{1}{p}$ und nicht für $\alpha \leqq \frac{1}{p}$* [27]).

Beweis. Mit $\frac{1}{p} + \frac{1}{q} = 1$ ist $\sum \left|\frac{a_n}{n^\alpha}\right| \leqq (\sum |a_n|^q)^{1/q} (\sum n^{-\alpha p})^{1/p}$, so daß für $\alpha > \frac{1}{p}$ nach der Ungleichung von HAUSDORFF-YOUNG die Bedingung (17) erfüllt ist. Ein Gegenbeispiel im anderen Fall wird gegeben durch $\sum \Re \frac{e^{in\varphi}}{n^{1-\frac{1}{p}} \log n}$,

24) Dabei ist B der Raum der meßbaren und beschränkten Funktionen und C der Raum der stetigen Funktionen.

25) Für $K = L$ vgl. ZYGMUND [1926], BOSANQUET-OFFORD [1935] und BHATNAGAR [1938]; ferner ZYGMUND [1935] (fortan als TS zitiert).

26) Lokalisation für $\alpha > 1$ (als lokales Summierbarkeitskriterium) bei BOSANQUET [1936] und SUNOUCHI [1949]. Nichtlokalisation für $\alpha = 1$ bei FOÀ [1938], BOSANQUET-KESTELMAN [1939] und RANDELS [1940].

27) Lokale Summierbarkeitskriterien bei FOÀ [1940] (falsche Aussage für $p > 2$ berichtigt bei FOÀ [1941]) und TSUCHIKURA [1953], [1954] (falsche Aussage für $p > 2$ in der ersten Note ist berichtigt in der zweiten). Nichtlokalisation für $\alpha \leqq \frac{1}{p}$ bei FOÀ [1940], [1942], YANO [1953], TSUCHIKURA [1954].

denn dies ist die FOURIER-Reihe einer Funktion aus L_p (vgl. TS, § 9.501 oder § 5.221).

5.4. Satz 9. *Die Klassen L^p $(p \geqq 2)$, B und C, allgemeiner alle Klassen K mit $L^2 \supseteqq K \supseteqq C$, besitzen $|C_\alpha|$-Lokalisation für $\alpha > \frac{1}{2}$ und nicht für $\alpha \leqq \frac{1}{2}$* [28]).

Beweis. Lokalisation für $\alpha > \frac{1}{2}$ folgt nach Satz 8 für alle Unterklassen von L^2. Nichtlokalisation für $\alpha \leqq \frac{1}{2}$ folgt aus der Tatsache, daß es zu jeder (reellen) Folge c_n mit $\sum c_n^2 = \infty$, insbesondere also zu $c_n = \frac{1}{\sqrt{n}}$, eine stetige Funktion gibt, für deren FOURIER-Koeffizienten a_n die Beziehung $\sum |a_n c_n| = \infty$ gilt [29]).

5.5. Im folgenden betrachten wir Klassen, die aus den bisher untersuchten Räumen sozusagen durch Integration hervorgegangen sind. Dies sind die Klasse C^* der totalstetigen Funktionen und die Klassen $\operatorname{Lip}(\beta, p)$ bzw. $\operatorname{Lip}\beta$ mit $0 < \beta \leqq 1$, $p \geqq 1$, die definiert sind durch

$$\left\{ \int_{-\pi}^{\pi} |f(\varphi + h) - f(\varphi)|^p \, d\varphi \right\}^{1/p} = O(h^\beta) \quad \text{für} \quad h \to +0$$

bzw.

$$\sup_\varphi |f(\varphi + h) - f(\varphi)| = O(h^\beta) \quad \text{für} \quad h \to +0.$$

Genauer gelten (wenn man wie bisher Funktionenklassen mit den zugehörigen Klassen von FOURIER-Reihen identifiziert) die Implikationen [30])

$$\sum \Re\, a_n e^{in\varphi} \in \operatorname{Lip}(\beta, p) \quad \text{bzw.} \quad \operatorname{Lip}\beta \Rightarrow \sum \Re (in)^\gamma a_n e^{in\varphi} \in L^p \quad \text{bzw.} \quad B,$$
$$\sum \Re (in)^\beta a_n e^{in\varphi} \in L^p \quad \text{bzw.} \quad B \quad \Rightarrow \sum \Re\, a_n e^{in\varphi} \in \operatorname{Lip}(\beta, p) \quad \text{bzw.} \quad \operatorname{Lip}\beta$$

für $0 < \beta \leqq 1$, $p \geqq 1$, $0 < \gamma < \beta$.

Das Hauptgewicht der folgenden Sätze liegt auf den Aussagen über Nichtlokalisation, da in vielen Fällen zugleich mit der Lokalisation sogar Summierbarkeit vorhanden ist [31]).

5.6. Satz 10. *Die Klassen $\operatorname{Lip}(\beta, p)$ und $\operatorname{Lip}\beta$ mit $0 < \beta \leqq 1$, $p \geqq 1$, allgemeiner alle Klassen K mit $\operatorname{Lip}(\beta, 1) \supseteqq K \supseteqq \operatorname{Lip}\beta$, besitzen C_α-Lokalisation für $\alpha > -\beta$ und nicht für $\alpha \leqq -\beta$ $(\beta < 1)$.*

---

[28]) Vgl. TSUCHIKURA [1954].

[29]) KACMARZ-STEINHAUS [1935], S. 240 oben.

[30]) Vgl. HARDY-LITTLEWOOD [1928_1], [1928_2]; TS, § 9.8.

[31]) Ist $f \in \operatorname{Lip}(\beta, p)$, so ist die zugehörige FOURIER-Reihe C_α-summierbar für $\alpha > -\beta$, und zwar gleichmäßig für $\beta p > 1$, überall für $\beta = p = 1$ und fast überall für $\beta p \leqq 1$. Vgl. HARDY-LITTLEWOOD [1928_1], CHOW [1951]. Außerdem folgt $|C_\alpha|$-Summierbarkeit für $\alpha > \frac{1}{p} - \beta$ $(1 \leqq p \leqq 2)$ bzw. $\alpha > \frac{1}{2} - \beta$ $(p > 2)$, und zwar überall für $\beta p > 1$, $\beta = p = 1$, und fast überall für $\beta p \leqq 1$. Vgl. BOSANQUET [1936] $(\beta = p = 1)$, CHOW [1937], [1942], CHEN [1944], SUNOUCHI [1949] $(\beta p > 1)$, MATSUYAMA [1949], CHOW [1951] $(\beta p \leqq 1$, $\beta < 1)$, HYSLOP [1937] $(p = \infty)$. Nach PRIVALOFF (TS, § 7.4) bzw. HARDY-LITTLEWOOD [1928_2] (TS, § 7.6.15) folgen daraus auch Aussagen über die konjugierten Reihen.

Zum *Beweis* genügt es zu bemerken, daß (17′) für $\mathrm{Lip}(\beta, 1)$ und $\alpha > -\beta$ erfüllt ist (nach TS, § 2.21), während es für $\alpha \leq -\beta$ $(\beta < 1)$ Gegenbeispiele aus $\mathrm{Lip}\,\beta$ gibt (nach TS, § 2.9.3).

5.7. Satz 11. *Die Klasse* $\mathrm{Lip}(\beta, p)$ *mit* $0 < \beta \leq 1$, $1 \leq p \leq 2$ *besitzt* $|C_\alpha|$-*Lokalisation für* $\alpha > \frac{1}{p} - \beta$ *und nicht für* $\alpha \leq \frac{1}{p} - \beta$.

Der *Beweis* ergibt sich sozusagen durch β-fache Integration aus den Sätzen 7 und 8: Wegen 5.5 gilt nämlich in $\mathrm{Lip}(\beta, p)$ notwendig[32])

$$\sum n^{\gamma-\alpha} |a_n| < \infty \quad \text{für} \quad 0 < \gamma < \beta, \quad \alpha > \frac{1}{p},$$

während $\sum n^{\beta - \frac{1}{p}} |a_n|$ für gewisse Funktionen unendlich wird. (Die hier benötigten Gegenbeispiele ergeben sich aus den früheren unmittelbar durch Integration.)

5.8. Satz 12. *Die Klassen* $\mathrm{Lip}(\beta, p)$ *und* $\mathrm{Lip}\,\beta$ *mit* $0 < \beta \leq 1$, $p \geq 2$, *allgemeiner alle Klassen* K *mit* $\mathrm{Lip}(\beta, 2) \supseteqq K \supseteqq \mathrm{Lip}\,\beta$, *besitzen* $|C_\alpha|$-*Lokalisation für* $\alpha > \frac{1}{2} - \beta$ *und nicht für* $\alpha \leq \frac{1}{2} - \beta$.

Der *Beweis* ergibt sich aus Satz 9 nach der Beweismethode von Satz 11. Die Lokalisation folgt auch direkt aus Satz 11. Die Nichtlokalisation für $\mathrm{Lip}\,\beta$ $(\beta < 1)$ folgt auch aus dem „konkreten" Beispiel $\sum \Re \frac{e^{i n \log n}}{n^{\frac{1}{2}+\beta}} e^{i n \eta}$ (vgl. TS, § 5.3).

5.9. Satz 13. *Die Klasse* C^* *besitzt* C_α-*Lokalisation für alle* $\alpha > -1$, *dagegen* $|C_\alpha|$-*Lokalisation für* $\alpha > 0$ *und nicht für* $\alpha \leq 0$.

Der *Beweis* ergibt sich aus den Sätzen 6 und 7 durch Integration.

Literatur

BHATNAGAR, S. P.: A local property of the allied series of a FOURIER series. Proc. Lond. Math. Soc. **44**, 315—322 (1938). — BOSANQUET, L. S.: Note on the absolute summability (*C*) of a FOURIER series. J. Lond. Math. Soc. **11**, 11—15 (1936). — BOSANQUET, L. S., and H. KESTELMAN: The absolute convergence of series of integrals. Proc. Lond. Math. Soc. **45**, 88—97 (1939). — BOSANQUET, L. S., and A. C. OFFORD: A local property of FOURIER series. Proc. Lond. Math. Soc. (2) **40**, 273—280 (1935). — CHEN, KIEN-KWONG: On the absolute CESÀRO summability of negative order for a FOURIER series at a given point. Amer. J. Math. **66**, 299—312 (1944). — CHOW, H. C.: Note on the absolute CESÀRO summability of power series. Proc. Lond. Math. Soc. **43**, 484—489 (1937). — On the absolute summability of FOURIER series. J. Lond. Math. Soc. **17**, 17—23 (1942). — A note on the summability of a power series on its circle of convergence. J. Lond. Math. Soc. **26**, 290—294 (1951). — FOÀ, A.: Il fenomeno si RIEMANN per la somme $|C, \alpha|$ di una serie di FOURIER con $0 < \alpha \leq 1$. Inst. Lomb. Rend. **2**, 359—366 (1938). — Sulle sommabilita assoluta $|C, \alpha|$ delle serie di FOURIER di una funzione sommabile L^p con $p > 1$. Boll. Un. mat. Ital. **2**, 325—332 (1940). — Aggiunta alla Nota: „Sulle sommabilita assoluta $|C, \alpha|$ delle serie di FOURIER." Boll. Un. mat. Ital. **3**, 393—394 (1941). — Sulla sommabilita assoluta $|C, \alpha|$ delle serie di FOURIER di una funzione sommabile L^p

[32]) Vgl. auch TS, § 6.6.6.

con $p > 1$. Atti II congr. Un. mat. Ital. 152—153, 1942. — HARDY, G. H., and J. E. LITTLEWOOD: Some properties of fractional integrals. I. Math. Z. **27**, 565—606 (1928_1). — A convergence criterion for FOURIER series. Math. Z. **28**, 612—634 (1928_2). — HYSLOP, J. M.: On the absolute summability of FOURIER series. Proc. Lond. Math. Soc. **43**, 475—483 (1937). — KACZMARZ, S., u. H. STEINHAUS: Theorie der Orthogonalreihen. Warsaw 1935. — MATSUYAMA, N.: Notes on FOURIER Analysis XIV. Absolute CESÀRO summability of FOURIER series. Tôhoku math. J. (2) **1**, 40—45 (1949). — RANDELS, W. C.: On the absolute summability of FOURIER series. II. Bull. Amer. Math. Soc. **46**, 86—88 (1940). — SUNOUCHI, G.: Notes on FOURIER Analysis XI. On the absolute summability of FOURIER series. J. math. Soc. Jap. **1**, 122—129 (1949). — TSUCHIKURA, T.: Absolute CESÀRO summability of orthogonal series. Tôhoku math. J. (2) **5**, 52—66 (1953). — Absolute CESÀRO summability of orthogonal series. II. Correction and remark to the previous paper. Tôhoku math. J. (2) **5**, 302—312 (1954). — YANO, S.: A remark on absolute CESÀRO summability of FOURIER series. Tôhoku math. J. (2) **5**, 194—195 (1953). — ZYGMUND, A.: Sur la théorie riemannienne des séries trigonométriques. Math. Z. **24**, 47—104 (1926). — Trigonometrical series (zitiert als TS). Warsaw 1935.

Tübingen, Mathematisches Institut der Universität

Gießen, Mathematisches Institut der Justus-Liebig-Hochschule

(Eingegangen am 27. Juli 1955)

RIBENBOIM, P.
Math. Zeitschr. Bd. 64, S. 159—168 (1956)

Sur une note de Nagata relative à un problème de Krull

Par
P. RIBENBOIM *)

Dans un article paru en 1936, Krull[1]) a fait la conjecture suivante: *Tout anneau d'integrité primaire, complètement intégralement clos, est un anneau de valuation.*

En 1952, Nagata[2]) a publié une note dans laquelle il affirmait résoudre par la négative la conjecture de Krull. Pour cela, il a construit un anneau et il a «démontré» qu'il s'agissait d'un anneau d'intégrité primaire complètement intégralement clos, mais non un anneau de valuation.

Or, l'examen de la démonstration du contre-exemple de Nagata nous a permis de constater qu'elle presentait des lacunes qui n'étaient pas simples à corriger. Du même coup, le problème de savoir si la conjecture de Krull serait vraie ou fausse était à nouveau ouvert.

L'auteur ayant précisement abordé un aspect de cette question dans une autre note[3]) il était de toute opportunité de trancher une fois pour toutes le doute sur cette conjecture. En outre, Krull a posé la question plus précise suivante: *Est-il possible d'obtenir un anneau d'intégrité primaire qui est intersection d'anneaux de valuations discrètes (de rang 1) mais qui n'est pas un anneau de valuation?*

Cette note est dediée à la démonstration de l'existence d'un tel anneau; ceci améliore le résultat obtenu par Nagata, car l'existence de son contre-exemple n'entraîne pas trivialement l'existence de notre exemple. En plus, la méthode utilisée pour la démonstration que l'anneau indiqué est vraiment un anneau primaire s'applique sans modifications essentielles à la démonstration correcte de que l'anneau de Nagata est primaire. L'auteur veut d'ailleurs préciser qu'ayant communiqué à Nagata l'existence de lacunes dans sa démonstration, il s'est empressé de trouver indépendemment une démonstration correcte qui devra être publiée[4]).

Comme sous-produit de cette démonstration, l'auteur determine le groupe des unités de l'anneau indiqué à l'exemple et il montre en plus que l'idéal premier unique peut s'exprimer comme réunion d'une suite strictement

---

*) Boursier du Conselho Nacional de Pesquizas, Rio de Janeiro, Brasil.

[1]) KRULL, W.: Beiträge zur Arithmetik kommutativer Integritätsbereiche, II. Math. Z. **41**, 665—679 (1936).

[2]) NAGATA, M.: On Krull's conjecture concerning valuation rings. Nagoya Math. J. **4**, 29—33 (1952).

[3]) RIBENBOIM, P.: Sur une conjecture de Krull en théorie des valuations. A paraître dans le Nagoya Math. J.

[4]) NAGATA, M.: A correction to my paper on Krull's conjecture concerning valuation rings. A paraître dans le Nagoya Math. J.

croissante d'idéaux principaux, chacun desquels est une puissance du suivant; néanmoins, cette suite $(\mathcal{A}\, t_r)$ ne vérifie pas la propriété suivante: si $a, b \in \mathcal{A}$, $a, b \notin \mathcal{A}\, t_{r+1}$, alors $ab \notin \mathcal{A}\, t_r$ (pour tout $r \geq 1$). Cela découle d'ailleurs d'un théorème plus général dû à l'auteur[3]).

Pour toute la terminologie concernant cette note, nous renvoyons le lecteur à un des articles cités.

1. Soit K un corps algébriquement clos, w une valuation de K dont le groupe des valeurs est celui des nombres rationnels. Soient α, β, deux nombres irrationnels, tels que $0 < \alpha < \beta$.

Dans le corps $K(x)$ des fractions rationnelles à coefficients dans K, où x est une indeterminée, considérons les valuations suivantes. Pour tout élément $e \in K$, et pour tout nombre réel $\lambda \geq 0$ soit la valuation $w_{e,\lambda}$ de $K(x)$ définie par:

$$w_{e,\lambda}\left(\sum_{i=0}^{n} a_i (x+e)^i\right) = \min\{w(a_i) + i\,\lambda\}.$$

Considérons l'anneau $\mathcal{A}$, intersection des anneaux des valuations $w_{e,\lambda}$, lorsque $w(e) > \alpha$, $\alpha < \lambda < \beta$, *λ rationnel.*

Alors:

(I) *$\mathcal{A}$ est un anneau d'intégrité primaire, complètement intégralement clos, mais non un anneau de valuation.*

2. Il est clair que $\mathcal{A}$ est complètement intégralement clos. Puisque $x \in \mathcal{A}$ alors le corps des fractions de $\mathcal{A}$ est $K(x)$. $\mathcal{A}$ n'est pas un anneau de valuation, car si on prend $a \in K$ et λ_1, λ_2, des nombres rationnels, tels que $\alpha < \lambda_1 < w(a) < \lambda_2 < \beta$ alors on a $\frac{x}{a}$, $\frac{a}{x} \notin \mathcal{A}$.

Si $p \in K(x)$, $p \neq 0$, notons $\varepsilon(p) = \inf\{w_{e,\lambda}(p)\}$ et $\varphi(p) = \sup\{w_{e,\lambda}(p)\}$. Supposons démontré

(II) *Si $p \in \mathcal{A}$, non nul, non unité, alors $0 < \varepsilon(p) \leq \varphi(p) < +\infty$.*

S'il en est ainsi, alors $\mathcal{A}$ est un anneau primaire. Car si $p, q \in \mathcal{A}$, non nuls, p non unité de $\mathcal{A}$, si n est un entier assez grand pour que $n \cdot \varepsilon(p) \geq \varphi(q)$, alors $p^n \in \mathcal{A} q$.

Tout revient à montrer (II). Cela sera fait en plusieurs parties.

(III) *Si $p \in \mathcal{A}$, non nul, non unité, alors $w_{0,\lambda}(p) > 0$, quelque soit λ rationnel, $\alpha < \lambda < \beta$.*

(III') *Si $p \in \mathcal{A}$, non nul, non unité, alors*

$$\varepsilon_1(p) = \inf\{w_{0,\lambda}(p)\} > 0, \qquad \varphi_1(p) = \sup\{w_{0,\lambda}(p)\} < +\infty.$$

(IV) *Si* $p = \dfrac{\prod_{i=1}^{m}(x+a_i)}{\prod_{j=1}^{n}(x+b_j)}$, $w(a_i) = w(b_j) = \lambda$, $\alpha < \lambda < \beta$, *si* $e \in K$, $w(e) = \lambda$, *alors pour tout rationnel μ, $\lambda \leq \mu < \beta$, on a*

$$w_{e,\mu}(p) \geq \min\{w_{0,\lambda}(p),\, w_{b_j,\mu}(p)\}.$$

(IV′) *Si* $p \in \mathcal{A}$, *non nul, non unité, alors*

$$\varepsilon_2(p) = \inf\{w_{e,\lambda}(p) \mid e \neq 0\} > 0, \qquad \varphi_2(p) = \sup\{w_{e,\lambda}(p) \mid e \neq 0\} < +\infty.$$

Il est clair que (III′) et (IV′) entraînent (II).

3. K étant algébriquement clos, tout élément $p \in K(x)$, non nul, est de la forme

$$p = c \cdot \frac{\prod_{i=1}^{m}(x+a_i)}{\prod_{j=1}^{n}(x+b_j)}$$

avec $a_i, b_j, c \in K$, $c \neq 0$, $a_i \neq b_j$, $m \geq 0$, $n \geq 0$.

Pour les considérations que nous ferons, nous pouvons mettre p sous *forme canonique*, en divisant par des unités de $\mathcal{A}$. Nous arrivons ainsi à des éléments du type suivant:

$$p = c\,\frac{\prod_{i=1}^{m}(x+a_i)}{\prod_{j=1}^{n}(x+b_j)} \tag{1}$$

avec $a_i, b_j, c \in K$, $c \neq 0$, $a_i \neq b_j$, $w(c) \neq 0$, $\alpha < w(a_i) < \beta$ lorsque $a_i \neq 0$, $\alpha < w(b_j) < \beta$ lorsque $b_j \neq 0$, $w(a_i - b_j) < \beta$, car $\frac{x+a}{a}$ est unité lorsque $w(a) < \alpha$, $\frac{x+a}{x}$ est unité lorsque $\beta < w(a)$ et $\frac{x+a}{x+b}$ est unité lorsque $\alpha < w(a) = w(b) < \beta$ et $w(a-b) > \beta$.

Désormais, tous les éléments seront supposés sous forme canonique.

Donné un élément p du type (1), notons A, B, resp. les familles d'éléments a_i, b_j, qui figurent au numérateur et dénominateur de p (remarquons qu'on peut avoir $a_{i_1} = a_{i_2}$, $b_{j_1} = b_{j_2}$, pour $i_1 \neq i_2$, $j_1 \neq j_2$). Notons L l'ensemble $L = \{w(a_i) \mid a_i \neq 0\} \cup \{w(b_j) \mid b_j \neq 0\}$. Si $L \neq \emptyset$ écrivons $L = \{\lambda_1, \lambda_2, \ldots, \lambda_l\}$ où $\alpha = \lambda_0 < \lambda_1 < \lambda_2 < \cdots < \lambda_l < \lambda_{l+1} = \beta$.

Il est encore convenable d'introduire la notation suivante. Pour tout λ, $\alpha \leq \lambda \leq \beta$, soit $p = p''_\lambda p_\lambda p'_\lambda$, avec

$$p''_\lambda = c \cdot \frac{\prod(x+a_i)}{\prod(x+b_j)}$$

(produit étendu aux $a_i \in A$, $b_j \in B$, tels que $w(a_i) < \lambda$, $w(b_j) < \lambda$),

$$p_\lambda = \frac{\prod(x+a_i)}{\prod(x+b_j)}$$

(produit étendu aux $a_i \in A$, $b_j \in B$, tels que $w(a_i) = w(b_j) = \lambda$),

$$p'_\lambda = \frac{\prod(x+a_i)}{\prod(x+b_j)}$$

(produit étendu aux $a_i \in A$, $b_j \in B$, tels que $w(a_i) > \lambda$, $w(b_j) > \lambda$).

Notons $m''_\lambda, m_\lambda, m'_\lambda$ (et analoguement $n''_\lambda, n_\lambda, n'_\lambda$) le nombre de facteurs $x+a_i$ $(x+b_j)$ qui figurent dans le numérateur (dénominateur) de $p''_\lambda, p_\lambda, p'_\lambda$, respectivement.

4. Démonstration de (III). Soit $p \in \mathcal{A}$, non nul, non unité, du type (1).

Si $L=\emptyset$ alors $p=cx^M$, $c\neq 0$, M entier. Si $M=0$ alors c'est trivial. Si $M\neq 0$, alors $w_{0,\lambda}(p)=w(c)+M\lambda$. Si on a $w_{0,\lambda}(p)=0$ avec λ rationnel, $\alpha<\lambda<\beta$, la fonction ci-dessus étant linéaire, il existe un nombre rationnel λ', $\alpha<\lambda'<\beta$, tel que $w_{0,\lambda'}(p)<0$, absurde!

Soit donc $L\neq\emptyset$.

Lemme 1. *Si $p\in\mathcal{A}$, non nul, $L\neq\emptyset$, si $w_{0,\xi}(p)=0$, où ξ est rationnel, $\alpha<\xi<\beta$, alors il existe $\lambda_k\in L$ tel que $w_{0,\lambda_k}(p)=0$.*

En effet, si $\lambda_h<\xi<\lambda_{h+1}$ (où $0\leq h\leq l$) alors si on a $\lambda_h<\lambda<\lambda_{h+1}$ on déduit que $w_{0,\lambda}(p)=w_{0,\xi}(p)=0$. Par continuité de la fonction $w_{0,\lambda}(p)$, quand λ est réel, on a $w_{0,\lambda_h}(p)=w_{0,\lambda_{h+1}}(p)=0$.

Lemme 2. *Si $p\in\mathcal{A}$, non nul, si $\lambda_k\in L$ et $w_{0,\lambda_k}(p)=0$ alors on a $m_{\lambda_k}\leq n_{\lambda_k}$, $n_{\lambda_k}\neq 0$, et si $e\in K$, tel que $w(e)=\lambda_k$, on a $w_{e,\mu}(p_{\lambda_k})\geq w_{0,\lambda_k}(p_{\lambda_k})$ pour tout rationnel μ, $\lambda_k\leq\mu<\beta$.*

En effet, soient ξ,η, rationnels tels que $\lambda_{k-1}\leq\xi<\lambda_k<\eta\leq\lambda_{k+1}$, alors $w_{0,\lambda_k}(p)=0$, $w_{0,\xi}(p)\geq 0$, $w_{0,\eta}(p)\geq 0$, et $w_{0,\xi}(p''_{\lambda_k})=w_{0,\lambda_k}(p''_{\lambda_k})=w_{0,\eta}(p''_{\lambda_k})$; donc on déduit comme l'a fait Nagata que $m_{\lambda_k}\leq n_{\lambda_k}$. De $\lambda_k\in L$ on a $n_k\neq 0$. Si $e\in K$, $w(e)=\lambda_k$, si μ est rationnel, $\lambda_k\leq\mu<\beta$, alors $w_{e,\mu}(p)\geq 0$ donc $w_{e,\mu}(p)-w_{0,\lambda_k}(p)=w_{e,\mu}(p_{\lambda_k})-w_{0,\lambda_k}(p_{\lambda_k})\geq 0$.

L'affirmation (III) résulte alors du lemme suivant:

Lemme 3. *Soit $p\in K(x)$, du type $p=\dfrac{\prod_{i=1}^{m}(x+a_i)}{\prod_{j=1}^{n}(x+b_j)}$, avec $w(a_i)=w(b_j)=\lambda$, $m\leq n\neq 0$, $a_i\neq b_j$, $w(a_i-b_j)<\beta$. Alors il existe $b_{j_1}\in B$ et un rationnel μ, $\lambda<\mu<\beta$, tels que $w_{b_{j_1},\mu}(p)<w_{0,\lambda}(p)$.*

Soit $R=\{w(b_j-b_k)\mid b_j\neq b_k\}$, $r\geq 0$ le nombre d'éléments de R.

Supposons d'abord $r=0$, donc $p=\dfrac{\prod_{i=1}^{m}(x+a_i)}{(x+b_1)^n}$. Prenons μ rationnel, $\lambda\leq\max\{w(a_i-b_1)\}<\mu<\beta$ quand $m>0$, ou $\lambda<\mu$ quand $m=0$; alors $w_{b_1,\mu}(p)<w_{0,\lambda}(p)$.

Supposons le lemme vrai pour tout entier strictement inférieur à r (où $r\geq 1$). Soit ϱ_1 le plus petit élément de R. Posons $b_j\equiv b_k$ quand $w(b_j-b_k)>\varrho_1$. On obtient la partition en classes d'équivalence $B=\bigcup B^{(\nu)}$. Pour tout b_k soit $A_{b_k}=\{a_i\mid w(a_i-b_k)>\varrho_1\}$. Si $b_j\equiv b_k$ alors $A_{b_j}=A_{b_k}$, si $b_j\not\equiv b_k$ alors $A_{b_j}\cap A_{b_k}=\emptyset$. Donc, la correspondance $b_k\to A_{b_k}$ induit une correspondance biunivoque $B^{(\nu)}\to A^{(\nu)}$ et $A\supseteq\bigcup A^{(\nu)}$ (les $A^{(\nu)}$ étant éventuellement vides). Puisque $m\leq n$, il existe un indice, par exemple $\nu=1$, tel que $m^{(1)}\leq n^{(1)}$ (avec notations évidentes). Soit $p_1=\dfrac{\prod(x+a_i)}{\prod(x+b_j)}$ (pour tous les $a_i\in A^{(1)}$, $b_j\in B^{(1)}$). Si $m\leq n^{(1)}$

posons $p_1' = \prod (x + a_i)$ (pour les autre $s a_i$); si $m > n^{(1)}$ posons $p_1' = \prod (x + a_i)$ (on prend $n^{(1)} - m^{(1)}$ éléments $a_i \notin A^{(1)}$). Ecrivons $p = p_1 p_1' p_2$. Par l'induction, il existe $b_{j_1} \in B^{(1)}$ et un nombre rationnel μ, $\lambda < \mu < \beta$, tels que $w_{b_{j_1}, \mu}(p_1 p_1') < w_{0,\lambda}(p_1 p_1')$ (car $w(b_j - b_k) > \varrho_1$ quand b_j, $b_k \in B^{(1)}$). D'autre part, on a $w_{b_{j_1}, \mu}(p_2) \leq w_{0,\lambda}(p_2)$, comme on le vérifie aisément dans les deux cas possibles, car $\lambda \leq \varrho_1$ et le numérateur de p_2 ne possède pas plus de termes que son dénominateur. Donc, on a bien $w_{b_{j_1}, \mu}(p) < w_{0,\lambda}(p)$.

5. Démonstration de (III'). Considérons pour un moment aussi les valuations $w_{0,\lambda}$, lorsque λ est *réel*, $\alpha \leq \lambda \leq \beta$. Alors $w_{0,\lambda}(p)$ est une fonction continue de λ définie dans le compact $[\alpha, \beta]$. Elle est donc bornée et assume ses valeurs maximum et minimum. Donc, $\varphi_1(p) < \infty$.

Si $\varepsilon_1(p) = 0$, il existe alors un irrationnel γ, $\alpha \leq \gamma \leq \beta$, tel que $w_{0,\gamma}(p) = 0$. Or, $w_{0,\alpha}(p) = w(c) + (m - n)\alpha \neq 0$ car α est irrationnel. Si on a $\lambda_k < \gamma < \lambda_{k+1}$, avec $0 \leq k \leq l$, alors $w_{0,\gamma}(p) = w_{0,\lambda_k}(p''_{\lambda_k} p_{\lambda_k}) + (m'_{\lambda_k} - n'_{\lambda_k})\gamma = 0$; or, $w_{0,\lambda}(p)$ étant une fonction linéaire de λ dans l'intervalle $[\lambda_k, \lambda_{k+1}]$, et d'autre part positive, car $p \in \mathcal{A}$, alors elle est identiquement nulle, et il existerait un λ rationnel tel que $w_{0,\lambda}(p) = 0$, absurde, en vertu de (III). Enfin, on vérifie analoguement que $w_{0,\beta}(p) \neq 0$.

6. Démonstration de (IV). Supposons d'abord $n = 0$. Alors, on a trivialement $w_{e,\mu}(p) \geq w_{0,\lambda}(p)$.

Soit donc $n \geq 1$. Notons $S = \{w(b_j - e) \mid b_j \in B\}$ et posons $S = \{\sigma_1, \sigma_2, \ldots, \sigma_s\}$ avec $\lambda \leq \sigma_1 < \sigma_2 < \cdots < \sigma_s$. Notons $A(\sigma_h) = \{a_i \in A \mid w(a_i - e) = \sigma_h\}$, $B(\sigma_h) = \{b_j \in B \mid w(b_j - e) = \sigma_h\}$, $m(\sigma_h)$, $n(\sigma_h)$, respectivement le nombre d'éléments de $A(\sigma_h)$, $B(\sigma_h)$. On a $A \geq \bigcup_{h=1}^{s} A(\sigma_h)$, $B = \bigcup_{h=1}^{s} B(\sigma_h)$, $m(\sigma_h) \geq 0$, $n(\sigma_h) > 0$.

1[er] cas. *Soit* $m(\sigma_h) \geq n(\sigma_h)$ *quelque soit* $\sigma_h \in S$.

Alors, on vérifie trivialement que pour tout rationnel μ, $\lambda \leq \mu < \beta$, on a $w_{e,\mu}(p) \geq w_{0,\lambda}(p)$.

2[ème] cas. *Soit* h_0 *le plus grand indice tel que* $m(\sigma_{h_0}) < n(\sigma_{h_0})$.

Montrons l'existence d'un élément $b_{j_0} \in B(\sigma_{h_0})$ tel que pour tout rationnel μ, $\lambda \leq \mu < \beta$, on ait $w_{e,\mu}(p) \geq w_{b_{j_0},\mu}(p)$.

Soit $R = \{w(b_j - b_k) \mid b_j, b_k \in B, b_j \neq b_k\}$, et $r \geq 0$ le nombre d'éléments de R.

Considérons d'abord le cas où $r = 0$. Alors, p est du type $p = \dfrac{\prod_{i=1}^{m} (x + a_i)}{(x + b_1)^n}$, donc $s = 1$ et par hypothèse, on a $m(\sigma_1) < n(\sigma_1) = n$. On peut alors vérifier, moyennant un calcul non difficile que, pour tout rationnel μ, $\lambda \leq \mu < \beta$, on a $w_{e,\mu}(p) \geq w_{b_1,\mu}(p)$.

Supposons maintenant l'affirmation valable pour tout entier strictement inférieur à r (où $r \geq 1$). Notons ϱ_1 le plus petit élément de R.

Sous-cas A. $\sigma_{h_0} > \varrho_1$.

Posons $p = p_0 p_0'$, où $p_0 = \frac{\Pi(x+a_i)}{\Pi(x+b_j)}$ (produit étendu à tous les éléments $a_i \in \bigcup_{h=h_0}^{s} A(\sigma_h)$ et à tous les éléments $b_j \in \bigcup_{h=h_0}^{s} B(\sigma_h)$). Alors, pour l'élément p_0, l'ensemble $R_0 = \left\{w(b_j - b_k) \mid b_j, b_k \in \bigcup_{h=h_0}^{s} B(\sigma_h), b_j \neq b_k\right\}$ a au plus $r-1$ éléments, car $\varrho_1 \notin R_0$, et pour p_0 on a encore $m(\sigma_{h_0}) < n(\sigma_{h_0})$, h_0 étant le plus grand indice avec cette propriété. Par l'induction, il existe $b_{j_0} \in B(\sigma_{h_0})$ tel que $w_{e,\mu}(p_0) \geq w_{b_{j_0},\mu}(p_0)$ pour tout rationnel μ, $\lambda \leq \mu < \beta$. Un calcul simple donne alors $w_{e,\mu}(p_0') \geq w_{b_{j_0},\mu}(p_0')$, donc $w_{e,\mu}(p) \geq w_{b_{j_0},\mu}(p)$.

Sous-cas B. $\sigma_{h_0} \leq \varrho_1$, *donc nécéssairement* $h_0 = 1$ (car si $\sigma_1 < \sigma_{h_0} \leq \varrho_1$, $w(b_j - e) = \sigma_1$, $w(b_k - e) = \sigma_{h_0}$, alors $w(b_j - b_k) = \sigma_1 < \varrho_1$, absurde).

Si $b_j, b_k \in B(\sigma_1)$, posons $b_j \equiv b_k$ quand $w(b_j - b_k) > \varrho_1$. On obtient la partition en classes d'équivalence $B(\sigma_1) = \bigcup B^{(\nu)}$. Pour tout élément $b_k \in B(\sigma_1)$, soit $A_{b_k} = \{a_i \in A(\sigma_1) \mid w(a_i - b_k) > \varrho_1\}$. Si $b_j \equiv b_k$ alors $A_{b_j} = A_{b_k}$, si $b_j \not\equiv b_k$ alors $A_{b_j} \cap A_{b_k} = \emptyset$. Donc, la correspondance $b_k \to A_{b_k}$ induit une correspondance biunivoque $B^{(\nu)} \to A^{(\nu)}$ et $A(\sigma_1) = (\bigcup A^{(\nu)}) \cup A'$ (les $A^{(\nu)}$, A', étant éventuellement vides et deux à deux disjoints). Puisque $m(\sigma_1) < n(\sigma_1)$, alors il existe un indice, par exemple $\nu = 1$, tel que $m^{(1)} < n^{(1)}$ (avec notations évidentes). Soit $p_1 = \frac{\Pi(x+a_i)}{\Pi(x+b_j)}$ (produit étendu à tous les $a_i \in A^{(1)}$ et $b_j \in B^{(1)}$).

Si $m(\sigma_1) < n^{(1)}$ soit $p_1' = \prod (x + a_i)$ (produit étendu à tous les $a_i \in A(\sigma_1)$, $a_i \notin A^{(1)}$). Si $m(\sigma_1) \geq n^{(1)}$ soit $p_1' = \prod (x + a_i)$ (produit étendu à $n^{(1)} - 1 - m^{(1)}$ éléments $a_i \in A(\sigma_1)$, $a_i \notin A^{(1)}$). Ecrivons $p = p_1 p_1' p_2$.

Pour l'élément $p_1 p_1'$ l'ensemble $R_1 = \{w(b_j - b_k) \mid b_j, b_k \in B^{(1)}, b_j \neq b_k\}$ a au plus $r-1$ éléments, et en outre, le nombre de facteurs au numérateur de $p_1 p_1'$ est inférieur au nombre de facteurs au dénominateur. Par l'induction, il existe un élément $b_{j_0} \in B^{(1)} \subseteq B(\sigma_1)$, tel que $w_{e,\mu}(p_1 p_1') \geq w_{b_{j_0},\mu}(p_1 p_1')$ pour tout rationnel μ, $\lambda \leq \mu < \beta$. Enfin, il n'est pas difficile à vérifier qu'on a $w_{e,\mu}(p_2) \geq w_{b_{j_0},\mu}(p_2)$, pour tout rationnel μ, $\lambda \leq \mu < \beta$. On conclut donc que $w_{e,\mu}(p) \geq w_{b_{j_0},\mu}(p)$, pour tout rationnel μ, $\lambda \leq \mu < \beta$.

Ceci termine de montrer l'affirmation (IV).

7. Démonstration de (IV'). Commençons en faisant une remarque. Si $p = c \frac{\prod_{i=1}^{m} (x + a_i)}{\prod_{j=1}^{n} (x + b_j)}$ et si $e \in K$, soit p^e l'élément $p^e = c \frac{\prod_{i=1}^{m} (x + a_i - e)}{\prod_{j=1}^{n} (x + b_j - e)}$. Alors, $(p^e)^{-e} = p$ et si $e' \in K$, on a $w_{e+e',\lambda}(p) = w_{e,\lambda}(p^{e'})$. De cela, il résulte que si $e_0 \in K$, $w(e_0) > \alpha$, alors $p \in \mathcal{A}$ si et seulement si $p^{e_0} \in \mathcal{A}$; car, si $p \in \mathcal{A}$ et si $w(e) > \alpha$, alors $w_{e,\lambda}(p^{e_0}) = w_{e+e_0,\lambda}(p) \geq 0$, puisque $w(e + e_0) > \alpha$, donc $p^{e_0} \in \mathcal{A}$, et réciproquement, si $p^{e_0} \in \mathcal{A}$, $w(e) > \alpha$, alors $w_{e,\lambda}(p) = w_{e,\lambda}\left((p^{e_0})^{-e_0}\right) = w_{e-e_0,\lambda}(p^{e_0}) \geq 0$, car $w(e - e_0) > \alpha$, donc $p \in \mathcal{A}$.

Soit maintenant $p \in \mathcal{A}$, non nul, non unité.

Si $e \in K$, $e \neq 0$, tel que $w(e) = \mu \notin L$, alors pour tout rationnel λ, $\alpha < \lambda < \beta$, on a $w_{e,\lambda}(p) = w_{0,\min\{\lambda,\mu\}}(p)$.

Soit $e \in K$, $e \neq 0$, tel que $w(e) = \lambda_k \notin L$. Si λ est rationnel, $\alpha < \lambda \leq \lambda_k$, on a $w_{e,\lambda}(p) = w_{0,\lambda}(p)$. Si, par contre, on a $\lambda_k < \lambda < \beta$, alors $w_{e,\lambda}(p''_{\lambda k}) = w_{0,\lambda k}(p''_{\lambda k})$ et $w_{e,\lambda}(p'_{\lambda k}) = w_{0,\lambda k}(p'_{\lambda k})$. En vertu de (IV), on a pour tout λ rationnel, $\lambda_k < \lambda < \beta$, l'inégalité $w_{e,\lambda}(p_{\lambda k}) \geq \min \{w_{0,\lambda k}(p_{\lambda k}), w_{b_j,\lambda}(p_{\lambda k}) \mid w(b_j) = \lambda_k\}$. Donc $w_{e,\lambda}(p) \geq \min \{w_{0,\lambda_k}(p), w_{b_j,\lambda}(p) \mid w(b_j) = \lambda_k\}$.

Pour montrer que $\varepsilon_2(p) = \inf \{w_{e,\lambda}(p) \mid e \neq 0\} > 0$ il suffit, en vertu de (III'), de montrer, pour tout $\lambda_k \in L$, qu'on a $\varepsilon_{2,k}(p) = \inf \{w_{e,\lambda}(p) \mid w(e) = \lambda_k \in L$, $\lambda_k < \lambda < \beta$, λ rationnel$\} > 0$. Or, $w_{b_j,\lambda}(p) = w_{0,\lambda}(p^{b_j}) \geq 0$. Si, pour un b_j on avait $\inf\{w_{b_j,\lambda}(p) \mid \lambda_k < \lambda < \beta\} = 0$ alors $\inf\{w_{0,\lambda}(p^{b_j}) \mid \lambda_k < \lambda < \beta\} = 0$. En vertu de (III), l'élément $p^{b_j} \in \mathcal{A}$ serait une unité, donc $w_{0,\lambda}(p^{b_j}) = w_{b_j,\lambda}(p) = 0$ quelque soit λ rationnel, $\alpha < \lambda < \beta$, donc p serait unité, absurde! Ainsi, il résulte que $\inf \{w_{b_j,\lambda}(p) \mid \lambda_k < \lambda < \beta\} > 0$ pour tout b_j tel que $w(b_j) = \lambda_k$; donc, $\varepsilon_{2,k}(p) > 0$.

Soit maintenant $\varphi_2(p) = \sup\{w_{e,\lambda}(p) \mid e \neq 0\}$. En vertu de (III'), il suffit de montrer, pour tout $\lambda_k \in L$, qu'on a $\varphi_{2,k}(p) = \sup \{w_{e,\lambda}(p) \mid w(e) = \lambda_k \in L$, $\lambda_k < \lambda < \beta$, λ rationnel$\} < +\infty$. Or, $\varphi_{2,k}(p) = -\inf \{w_{e,\lambda}(p^{-1}) \mid w(e) = \lambda_k$, $\lambda_k < \lambda < \beta\} \leq -\inf\big\{\min\{w_{0,\lambda_k}(p^{-1}), w_{a_i,\lambda}(p^{-1}) \mid a_i \notin A, w(a_i) = \lambda_k\} \mid \lambda_k < \lambda < \beta\big\} = \max\big\{w_{0,\lambda_k}(p), \sup\{w_{a_i,\lambda}(p) \mid \lambda_k < \lambda < \beta\} \mid a_i \in A,\ w(a_i) = \lambda_k\big\} < +\infty$ en vertu de (IV) et de (III'), car $w_{a_i,\lambda}(p) = w_{0,\lambda}(p^{a_i})$ et $p^{a_i} \in \mathcal{A}$.

Ceci termine de montrer (IV') et établit ainsi la validité de (I).

8. Le contre-exemple avec les valuations discrètes. Soit K_0 le corps des nombres rationnels, w_0 une valuation discrète normée de K_0. Soit K le corps de tous les nombres algébriques, w une valuation de K prolongeant w_0. Donc, la valuation w possède groupe de valeurs égal à celui des nombres rationnels.

Dans le corps $K(x)$, soit l'anneau $\mathcal{A}$ de l'exemple indiqué au numéro 1; donc $\mathcal{A} = \bigcap \mathcal{A}_{w_{e,\lambda}}$, où λ est rationnel, $\alpha < \lambda < \beta$, $e \in K$, $w(e) > \alpha$.

Posons $\mathcal{A}^0 = \mathcal{A} \cap K_0(x)$. Donc, le corps des fractions de $\mathcal{A}^0$ est égal à $K_0(x)$.

Donnés $e \in K$, avec $w(e) > \alpha$, et λ rationnel, tel que $\alpha < \lambda < \beta$, soit $w^0_{e,\lambda}$ la valuation induite par $w_{e,\lambda}$ sur le corps $K_0(x)$. Alors $\mathcal{A}^0 = \bigcap \mathcal{A}_{w^0_{e,\lambda}}$.

Remarquons que $w_{e,\lambda}$ est la seule valuation de $K(x)$ prolongeant $w^0_{e,\lambda}$. En effet, si v est une valuation (nécéssairement de rang 1) de $K(x)$ prolongeant $w^0_{e,\lambda}$, et si $v \neq w_{e,\lambda}$ alors il existe un élément $x + a \in K(x)$ tel que $v(x+a) \geq 0$ et $w_{e,\lambda}(x+a) < 0$. Or, $w_{e,\lambda}(x+a) = \min\{\lambda, w(a-e)\} < 0$; de $w(e) > \alpha > 0$, $\lambda > \alpha$, il vient nécéssairement $w(a) < 0$; mais alors, de $v(x) = w^0_{e,\lambda}(x) = \min\{\lambda, w(e)\} > 0$ il résulte que $v(x+a) = \min\{v(x), v(a)\} < 0$, contradiction!

De ces considérations, puisque $K(x)$ est algébrique sur $K_0(x)$, alors $\mathcal{A}$ est l'anneau des entiers algébriques de $K(x)$ sur $\mathcal{A}^0$.

Montrons que $\mathcal{A}^0$ est un anneau intersection d'anneaux de valuations discrètes (donc, complètement intégralement clos), primaire, mais non de valuation.

En effet, chaque $w^0_{e,\lambda}$ est une valuation discrète de $K_0(x)$, car si $f(x)=\sum_{i=0}^{n} a_i x^i$ est un polynome à coefficients dans K_0, alors $f(x)=\sum_{i=0}^{n} a'_i(x+e)^i = g(x+e)$, où les coefficients de $g(x+e)$ sont des éléments de $a'_i \in K_0[e]$. Donc

$$w^0_{\lambda,e}(f(x)) = w^0_{\lambda,e}\left(\sum_{i=0}^{n} a'_i(x+e)^i\right) = w_{\lambda,e}\left(\sum_{i=0}^{n} a'_i(x+e)^i\right) = \min\{w(a'_i) + i\lambda\};$$

or, la valuation w de K induit sur l'extension algébrique finie $K_0(e)$ une valuation nécéssairement discrète, donc $w^0_{\lambda,e}$ est elle même une valuation discrète.

$\mathcal{A}^0$ n'est pas un anneau de valuation. En effet, $\mathcal{A}$ étant l'anneau des entiers de $K(x)$ et $\mathfrak{p}$ son seul idéal premier, alors $\mathcal{A}_{\mathfrak{p}}=\mathcal{A}$ serait un anneau de valuation de $K(x)$ prolongeant la valuation définie par $\mathcal{A}^0$, ce qui est absurde [voir Nagata[2]), lemme 2].

Enfin, $\mathcal{A}$ étant un anneau entier sur $\mathcal{A}^0$, et un anneau primaire, il résulte que $\mathcal{A}^0$ est lui-même un anneau primaire.

9. Le groupe des unités de $\mathcal{A}$ et de $\mathcal{A}^0$. Nous determinerons maintenant les unités de l'anneau $\mathcal{A}$. Au numéro 3, nous avons déjà determiné quatre types d'unités de l'anneau $\mathcal{A}$:

(i) $a \in K$ lorsque $w(a)=0$ (unité de l'anneau de la valuation w),

(ii) $\frac{a}{x+a}$, $\frac{x+a}{a}$, lorsque $w(a)<\alpha$,

(iii) $\frac{x}{x+a}$, $\frac{x+a}{x}$, lorsque $\beta < w(a)$,

(iv) $\frac{x+a}{x+b}$ lorsque $\alpha < w(a) = w(b) < \beta$, $w(a-b) > \beta$.

Nous allons montrer que toute unité de $\mathcal{A}$ s'obtient comme produit d'un nombre fini d'unités des types ci-dessus (que nous appelerons des *unités basiques*).

En effet, soit p une unité de $\mathcal{A}$. Par réduction à la forme canonique, on a $p=up'$, où u est un produit d'unités basiques et p' est une unité sous forme canonique. Tout revient à montrer: 1 est la seule unité sous forme canonique. Soit en effet p une unité sous forme canonique. Avec les notations du n°3, si $L=\emptyset$ alors p est du type $p=cx^M$ (M entier de signe quelconque). De $w_{0,\lambda}(p)=w(c)+M\lambda=0$ pour tout λ rationnel, $\alpha<\lambda<\beta$, on a $M=0$, donc $w(c)=0$ et p étant sous forme canonique, alors $p=c=1$. Si, par contre, $L\neq\emptyset$ et λ est rationnel, $\alpha<\lambda<\lambda_1$, alors $w_{0,\lambda}(p)=w(c)+(m-n)\lambda=0$, donc $m=n$ et $w(c)=0$, ainsi $c=1$. D'après le lemme 2, puisque $p\in\mathcal{A}$, $p^{-1}\in\mathcal{A}$, on a $m_{\lambda_k}=n_{\lambda_k}\neq 0$ pour tout $\lambda_k\in L$; en particulier, il ne peut pas avoir aucun facteur x dans le numérateur ou dénominateur de p. D'après le lemme 3, il existe $b_{j_1}\in B$, tel que $w(b_{j_1})=\lambda_1$, et μ rationnel, $\lambda_1\leq\mu<\beta$, tels que $w_{b_{j_1},\mu}(p_{\lambda_1})<w_{0,\lambda_1}(p_{\lambda_1})=0$. Or, si $\lambda_k>\lambda_1$ alors $w_{b_{j_1},\mu}(p_{\lambda_k})=0$ donc on déduit $w_{b_{j_1},\mu}(p)=\sum_{k=1}^{l} w_{b_{j_1},\mu}(p_{\lambda_k})<0$, absurde!

Enfin, les unités de $\mathcal{A}^0$ ne sont autres que les unités de $\mathcal{A}$ appartenant à $K_0(x)$, car l'idéal premier $\wp^0$ de $\mathcal{A}^0$ est égal à $\wp^0 = \wp \cap \mathcal{A}^0$. Donc, les unités de $\mathcal{A}^0$ sont des produit finis d'unités basiques construites avec des éléments de K_0.

10. Une popriété supplémentaire de l'anneau $\mathcal{A}$. Il est intéressant de remarquer que l'anneau $\mathcal{A}$ possède la propriété suivante:

(a) *Il est possible de trouver une suite strictement croissante d'idéaux principaux $\mathcal{A}t_r$, dont la réunion est $\wp$, chacun desquels étant une puissance du suivant.*

En effet, prenons une suite strictement décroissante de nombres rationnels positifs, ayant limite nulle; par exemple, la suite de terme général $1/n^{r-1}$, où n est le plus petit entier tel que $\beta \leq n\alpha$ (donc $n > 1$). Soit $t \in K$ tel que $w(t) = 1$, et pour tout $r \geq 1$, soit $t_r = t^{1/n^{r-1}}$. Alors, la suite d'idéaux principaux $\mathcal{A}t_r$ est strictement croissante, on a $\mathcal{A}t_r = \mathcal{A}t_{r+1}^n$; en outre, si $p \in \wp$, non nul, alors, d'après (II) il existe r assez grand tel que $\frac{1}{n^{r-1}} < \varepsilon(p)$, donc $p \in \mathcal{A}t_r$.

Remarquons maintenant que la suite $(\mathcal{A}t_r)$ ne satisfait pas la condition suivante:

(b) *Pour tout $r \geq 1$, si $p, p' \in \mathcal{A}$, $p, p' \notin \mathcal{A}t_{r+1}$, alors $pp' \notin \mathcal{A}t_r$.*

En effet, nous montrerons l'existence, pour tout r assez grand, d'éléments $p, p' \in \mathcal{A}$, $p, p' \notin \mathcal{A}t_{r+1}$, mais tels que $pp' \in \mathcal{A}t_r$.

Par simplicité, considérons l'anneau $\mathcal{A}$ défini lorsque on prend $\beta = n\alpha$. Soit r assez grand pour que $\frac{1}{n^{r-1}} < \alpha$ et prenons des nombres rationnels λ_0, λ_0', tels que $\alpha < \lambda_0 < \lambda_0' < \alpha + \frac{1}{n^{r+1}} < \beta$.

Soit $p = \frac{(x+a)^n}{x+b}$, avec $w(a) = w(b) = w(a-b) = \lambda_0$. Montrons que $p \in \mathcal{A}$, $p \notin \mathcal{A}t_{r+1}$.

Si λ est rationnel, $\alpha < \lambda < \beta$, alors on a $w_{0,\lambda}(p) = (n-1) \cdot \min\{\lambda, \lambda_0\} > \alpha > \frac{1}{n^r}$.

Soit $e \in K$, $e \neq 0$, $w(e) > \alpha$, λ rationnel, $\alpha < \lambda < \beta$. Si $w(e) \neq \lambda_0$ alors $w_{e,\lambda}(p) = (n-1) \cdot \min\{\lambda_0, \lambda, w(e)\} > \alpha > \frac{1}{n^r}$. Si $w(e) = \lambda_0$ et $\alpha < \lambda \leq \lambda_0$ alors $w_{e,\lambda}(p) = w_{0,\lambda}(p) > \alpha > \frac{1}{n^r}$. Enfin, si $w(e) = \lambda_0 < \lambda < \beta$ alors, en vertu de (IV) on a $w_{e,\lambda}(p) \geq \min\{w_{0,\lambda_0}(p), w_{b,\lambda}(p)\} = \min\{(n-1)\lambda_0, n\lambda_0 - \lambda\} = n\lambda_0 - \lambda > 0$ car $\lambda < \beta = n\alpha < n\lambda_0$. D'autre part, si on prend λ rationnel tel que $\lambda_0 < n\lambda_0 - \frac{1}{n^r} < \lambda < \beta$ $\left(\text{un tel } \lambda \text{ existe, car } \lambda_0 < \alpha + \frac{1}{n^{r+1}}\right)$ alors $w_{b,\lambda}(p) = n\lambda_0 - \lambda < \frac{1}{n^r}$. Ainsi, $p \in \mathcal{A}$ mais $p \notin \mathcal{A}t_{r+1}$.

Analoguement, soit $p' = \frac{(x+a')^n}{x+b'}$ où $w(a') = w(b') = w(a'-b') = \lambda_0'$. Alors $p' \in \mathcal{A}$, $p' \notin \mathcal{A}t_{r+1}$.

Montrons que $pp' \in \mathcal{A}t_r$.

Il est clair que si λ est rationnel, $\alpha < \lambda < \beta$, alors $w_{0,\lambda}(pp') > 2\alpha > \alpha > \frac{1}{n^{r-1}}$; de même, si $e \in K$, $e \neq 0$, $w(e) > \alpha$, $w(e) \neq \lambda_0$, $w(e) \neq \lambda_0'$, alors $w_{e,\lambda}(pp') > 2\alpha > \alpha > \frac{1}{n^{r-1}}$.

Soit $w(e)=\lambda_0$; si $\alpha<\lambda\leqq\lambda_0$ alors $w_{e,\lambda}(pp')>2\alpha>\frac{1}{n^{r-1}}$; si $\lambda_0<\lambda<\beta$ alors $w_{e,\lambda}(pp')\geqq(n\lambda_0-\lambda)+w_{0,\lambda_0}(p')=(2n-1)\lambda_0-\lambda>\frac{1}{n^{r-1}}$ car on a $\frac{1}{n^{r-1}}<$ $<\alpha<\lambda_0\leqq(n-1)\lambda_0$ donc $\beta=n\alpha<n\lambda_0<(2n-1)\lambda_0-\frac{1}{n^{r-1}}$.

Soit $w(e)=\lambda_0'$; on vérifie analoguement que $w_{e,\lambda}(pp')>\frac{1}{n^{r-1}}$.

Donc, on a bien $pp'\in\mathcal{A}t_r$.

Nous terminons en soulignant que si $\mathcal{A}$ est primaire, complètement intégralement clos, mais non un anneau de valuation (comme dans l'exemple donné) il est impossible de trouver une suite strictement croissante d'idéaux principaux satisfaisant les propriétés (a) et (b). Cela découle d'un théorème plus général demontré par l'auteur dans la note[3]). En outre, on vérifie aisément que dans l'anneau $\mathcal{A}^0$, qui est intersection d'anneaux de valuations discrètes, il est impossible que $\mathfrak{p}^0$ soit réunion d'une suite strictement croissante d'idéaux principaux chacun desquels étant une puissance du suivant.

Instituto de Matemática Pura e Aplicada, Rio de Janeiro (Brasilien)

(Eingegangen am 5. August 1955)

BEHRENS, E.-A.
Math. Zeitschr. Bd. 64, S. 169—182 (1956)

Zur additiven Idealtheorie in nichtassoziativen Ringen

Von
ERNST-AUGUST BEHRENS

Einleitung

In den letzten Jahren sind den Versuchen von Krull [8] und Fitting [6] zur Übertragung der additiven Idealtheorie kommutativer Ringe auf assoziative Ringe, bei denen die Multiplikation nicht mehr als kommutativ vorausgesetzt ist, einige weitere Arbeiten gefolgt: Curtis [5] hat 1951 die Überlegungen von Fuchs [7] (1950) über primale Ideale nichtkommutativer Ringe verallgemeinert, und McCoy [4] hat 1949, mit Hilfe einer auch für nichtkommutative Ringe geeigneten Definition der multiplikativ abgeschlossenen Systeme von Krull [9], für jedes Ideal $\mathfrak{a}$ eines assoziativen Ringes ein Radikal angeben können, das der Durchschnitt der minimalen Primoberideale von $\mathfrak{a}$ ist. Seine Untersuchungen wurden 1950 von Murdoch [11] durch Einführung der Begriffe Primärideal und Komponentenideal eines Ideales $\mathfrak{a}$ sowie durch Beweis der Eindeutigkeitssätze für die Darstellung von $\mathfrak{a}$ als Durchschnitt von Primäridealen fortgesetzt. Mehr kann man dabei nicht verlangen, weil es bekanntlich nichtkommutative Ringe gibt, in denen trotz der Gültigkeit der aufsteigenden Kettenbedingung für Rechtsideale nicht jedes Ideal als Durchschnitt von Primäridealen darstellbar ist (vgl. z.B. Krull [8]).

Ebenfalls in diesen Jahren sind auch für nichtassoziative Ringe (*na*-Ringe) einige Definitionen für Radikale aufgestellt worden (Baer [2] 1943, Behrens [3] 1953, Smiley [13] 1950, sowie die axiomatischen Untersuchungen von Amitsur [1] ab 1952). Das legt die Frage nahe, ob man einen Teil der additiven Idealtheorie kommutativer Ringe auf beliebige nichtassoziative Ringe übertragen kann.

In der vorliegenden Abhandlung werden nun zunächst der Begriff des Primideales und der Radikalbegriff von McCoy auf *na*-Ringe verallgemeinert, wobei wieder eine Definition der multiplikativ abgeschlossenen Systeme M die Hauptrolle spielt. Dabei ist das Radikal $\mathfrak{r}(\mathfrak{a})$ eines Ideales $\mathfrak{a}$ der Durchschnitt seiner minimalen Primoberideale (§ 1). — Im nächsten Paragraphen werden die Primärideale $\mathfrak{q}$ eingeführt durch die Forderung, daß aus $(a)\cdot(b)\subseteqq\mathfrak{q}$, $a\not\subset\mathfrak{q}$ folgen soll $b\subset\mathfrak{r}(\mathfrak{q})$. Als Hauptunterschied zu den assoziativen und kommutativen Ringen erweist sich dabei, daß auch bei sehr scharfen Kettenbedingungen das Radikal eines Primärideales nicht mehr prim zu sein braucht (vgl. Beispiel 1 in § 2, wo $\mathfrak{o}$ eine kommutative, aber nicht assoziative Algebra vom Range drei über ihrem Grundkörper ist). Nennt man die minimalen Primoberideale des Primärideales $\mathfrak{q}$ die zugehörigen Primideale von $\mathfrak{q}$, so hat jetzt also $\mathfrak{q}$ mitunter mehrere zugehörige Primideale. Obgleich der

Zusammenhang zwischen Primär- und Primidealen hier weniger eng ist als in der klassischen Theorie, läßt sich eine Reihe bekannter Sätze über größte Primärkomponenten und M-Komponenten, sowie Kriterien für den Begriff relativ-prim übertragen. Dabei versagen aber die in der Theorie der assoziativen Ringe üblichen, auf Potenzbildungen beruhenden Schlußweisen (vgl. Northcott [*12*] oder van der Waerden [*14*]). Sie werden teilweise ersetzt durch die in § 1, Satz 7, abgeleitete Regel $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$. Unter Voraussetzung der aufsteigenden Kettenbedingung für zweiseitige Ideale in dem *na*-Ring $\mathfrak{o}$ kann man zwar zeigen, daß auch hier eine Potenz des Radikales $\mathfrak{r}(\mathfrak{a})$ in $\mathfrak{a}$ liegt (§ 2, Kor. zu Satz 9), doch ist das weniger fruchtbar als im assoziativen Fall, weil bei der Potenzbildung die Klammersetzung zu berücksichtigen ist. — Im § 3 werden die Eindeutigkeitssätze für die Normaldarstellung eines Ideales $\mathfrak{a}$ als unverkürzbarer Durchschnitt größter Primärkomponenten bewiesen, falls das Ideal $\mathfrak{a}$ überhaupt als Durchschnitt endlich vieler Primärideale darstellbar ist (s. dagegen Beispiel 2 in § 2): Satz 1 zeigt, daß wieder die Anzahl der Primärkomponenten und deren Radikale eindeutig durch $\mathfrak{a}$ bestimmt sind, und Satz 4 verallgemeinert den bekannten Satz, daß die isolierten Komponentenideale in jeder Normaldarstellung von $\mathfrak{a}$ auftreten (van der Waerden [*41*], § 88).

In der ganzen Abhandlung wird ausschließlich von zweiseitigen Idealen geredet. Das scheint um so mehr berechtigt, als in der Idealtheorie der *na*-Ringe die einseitigen Ideale nicht als Darstellungsmoduln dienen können; Automorphismenringe bilden eben keine geeigneten Modellvorstellungen für nichtassoziative Ringe. — Im § 2 werden drei Beispiele vorgerechnet; dazu sei bemerkt, daß die Schwierigkeit bei der Entwicklung der Idealtheorie in *na*-Ringen, dort nicht mehr nach dem Assoziativgesetz multiplizieren zu dürfen, teilweise dadurch ausgeglichen wird, daß man bei der Konstruktion von Beispielen andererseits auch nicht auf dieses Gesetz zu achten braucht.

Auch der erste Teil der Abhandlung von Curtis [*5*] über primale Ideale läßt sich übrigens auf *na*-Ringe übertragen, wenn man darauf verzichtet, daß deren adjungierte Ideale sämtlich prim sind.

§ 1. Primideale und Radikale

In dem nicht notwendig assoziativen Ring (*na*-Ring) $\mathfrak{o}$ bezeichne (a) das von dem Ringelement a erzeugte Ideal, d.h. das kleinste zweiseitige Ideal, das a enthält. Das Produkt $\mathfrak{a}\cdot\mathfrak{b}$ zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$ in $\mathfrak{o}$ sei das von der Menge $\{a \cdot b;\ a < \mathfrak{a},\ b < \mathfrak{b}\}$ in $\mathfrak{o}$ erzeugte Ideal.

Definition 1. *Das Ideal $\mathfrak{p}$ ist prim, wenn aus $(a)\cdot(b) \subseteqq \mathfrak{p}$ folgt, daß $a < \mathfrak{p}$ oder $b < \mathfrak{p}$.*

Eine zweite Definition des Primideales liefert der

Satz 1. *$\mathfrak{p}$ ist dann und nur dann prim, wenn für Ideale $\mathfrak{a}$ und $\mathfrak{b}$ in $\mathfrak{o}$ aus $\mathfrak{a}\cdot\mathfrak{b} \subseteqq \mathfrak{p}$ folgt, daß $\mathfrak{a} \subseteqq \mathfrak{p}$ oder $\mathfrak{b} \subseteqq \mathfrak{p}$.*

Beweis. 1. Wenn $\mathfrak{a} \nsubseteqq \mathfrak{p}$, $\mathfrak{b} \nsubseteqq \mathfrak{p}$ gibt es zwei Elemente a und b in $\mathfrak{a}$ bzw. $\mathfrak{b}$, die nicht in $\mathfrak{p}$ liegen. Wenn $\mathfrak{p}$ überdies prim, liegt $(a)\cdot(b)$ nicht in $\mathfrak{p}$, und es gibt daher zwei Elemente $a' < (a)$ und $b' < (b)$, deren Produkt $a' \cdot b'$ nicht zu $\mathfrak{p}$ gehört; andernfalls würde nämlich das Ideal $\mathfrak{p}$ das von allen $a' \cdot b'$ erzeugte Ideal enthalten. — 2. Aus $a, b \not< \mathfrak{p}$ folgt $(a), (b) \not\leqq \mathfrak{p}$. Wenn also $\mathfrak{p}$ der im Satz formulierten Bedingung genügt, ist $(a) \cdot (b) \not\leqq \mathfrak{p}$.

Diesen Satz kann man auf n Faktoren verallgemeinern, wenn man unter $\mathfrak{P}^{(\nu)}(\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n)$ das Produkt der n Ideale $\mathfrak{a}_i$ bei einer festen Klammersetzung versteht (zur Bezeichnung vgl. Behrens [*3*]):

Satz 2. *Wenn $\mathfrak{p}$ prim und $\mathfrak{P}^{(\nu)}(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \leqq \mathfrak{p}$, dann liegt mindestens eines der Ideale $\mathfrak{a}_i$ in $\mathfrak{p}$.*

Beweis durch vollständige Induktion nach n: $n=1$ ist trivial. — Sei $\mathfrak{P}^{(\nu)}(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = \mathfrak{P}^{(\varkappa)}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k) \cdot \mathfrak{P}^{(\lambda)}(\mathfrak{a}_{k+1}, \ldots, \mathfrak{a}_n)$. Nach Satz 1 muß mindestens einer der beiden Faktoren $\mathfrak{P}^{(\varkappa)}$ und $\mathfrak{P}^{(\lambda)}$ in $\mathfrak{p}$ liegen, also nach Induktionsannahme auch eines der Ideale $\mathfrak{a}_i$.

Auch für *na*-Ringe gilt der

Satz 3. *Wenn das Ideal $\mathfrak{a}$ in keinem der Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ liegt, enthält $\mathfrak{a}$ ein Element a mit derselben Eigenschaft.*

Beweis wieder durch vollständige Induktion nach n, wobei $n=1$ trivial ist: Nach Induktionsannahme gibt es, für jedes $i=1, 2, \ldots, n$, ein Element a_i in $\mathfrak{a}$ mit a_i nicht in $\mathfrak{p}_k$ für die $n-1$ Primideale $\mathfrak{p}_k \neq \mathfrak{p}_i$. Wenn für mindestens ein i auch noch $a_i \not< \mathfrak{p}_i$, kann man $a = a_i$ nehmen. Im andern Falle liegen alle a_i in ihren $\mathfrak{p}_i$. Für festes Primideal $\mathfrak{p}_l$ gibt es dann in (a_1) und (a_2) zwei Elemente a_1' bzw. a_2' mit $a_1' \cdot a_2' \not< \mathfrak{p}_l$. Daraus folgt die Existenz von a_2'' in $(a_1' \cdot a_2')$ und von a_3' in (a_3) mit $a_2'' \cdot a_3' \not< \mathfrak{p}_l$, und so weiter bis $a_{l-2}'' \cdot a_{l-1}'$ zwar nicht in $\mathfrak{p}_l$ wohl aber in $\mathfrak{p}_1, \ldots, \mathfrak{p}_{l-1}$ liegt. Dann gibt es wieder in $(a_{l-2}'' \cdot a_{l-1}')$ ein Element a_{l-1}'' und in (a_{l+1}) ein a_{l+1}' mit $a_{l-1}'' \cdot a_{l+1}' \not< \mathfrak{p}_l$ usw., bis schließlich $a_{n-1}'' \cdot a_n' = b_l$ zu allen $\mathfrak{p}_i \neq \mathfrak{p}_l$ gehört, aber nicht zu $\mathfrak{p}_l$. Keines der n Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ enthält dann das Element $a = b_1 + b_2 + \cdots + b_n$ aus $\mathfrak{a}$.

Eine dritte Möglichkeit, das Primideal $\mathfrak{p}$ zu definieren ergibt sich aus der Betrachtung der Komplementärmenge $C(\mathfrak{p}) = \{m; m < \mathfrak{o}, m \not< \mathfrak{p}\}$. Diese Menge ist nämlich multiplikativ abgeschlossen oder ein M-System in folgendem Sinne:

Definition 2. *Eine Menge M aus $\mathfrak{o}$ ist ein M-System, wenn es zu je zwei Elementen m_1 und m_2 aus M in den Idealen (m_1) und (m_2) zwei Elemente m_1' bzw. m_2' gibt mit $m_1' \cdot m_2'$ in M. Auch die leere Menge soll ein M-System sein.*

Diese M-Systeme spielen bei den *na*-Ringen die gleiche Rolle wie die von McCoy in [*4*] für assoziative Ringe definierten M-Systeme, so daß sich ein Teil der Sätze und Beweise von McCoy übertragen läßt. Zunächst folgt aus der Definition eines Primideales sofort der

Satz 4. *Ein Ideal $\mathfrak{p}$ ist dann und nur dann prim, wenn $C(\mathfrak{p})$ ein M-System ist.*

Man kann in diesem Satz — wie bei McCoy — die Voraussetzung, daß $\mathfrak{p}$ ein Ideal sei, abschwächen. Unter einem *minimalen Primoberideal* $\mathfrak{p}$ *eines Ideales* $\mathfrak{a}$ verstehe man ein Primideal, das zwar $\mathfrak{a}$ umfaßt, aber kein Primoberideal von $\mathfrak{a}$ echt enthält.

Satz 5. *Die Menge* $\mathfrak{p}$ *ist dann und nur dann minimales Primoberideal von* $\mathfrak{a}$, *wenn* $C(\mathfrak{p})$ *ein maximales* $\mathfrak{a}$ *nicht treffendes* M*-System ist, d. h.* $C(\mathfrak{p}) \cap \mathfrak{a} = \emptyset$.

Beweis. 1. Die Menge $\mathfrak{p}$ genüge der Bedingung des Satzes. Da $M = C(\mathfrak{p})$ das Ideal $\mathfrak{a}$ nicht trifft, liegt $\mathfrak{a}$ in $\mathfrak{p} = C(M)$. Nach dem Lemma von Zorn existiert nun ein maximales M nicht treffendes Ideal $\mathfrak{p}^*$, das $\mathfrak{a}$ enthält. $\mathfrak{p}^*$ ist prim, wie folgende Überlegung zeigt: Seien a_1 und a_2 nicht in $\mathfrak{p}^*$, also $(\mathfrak{p}^*, a_i) \cap M \neq \emptyset$, $i = 1, 2$, und etwa b_i in (a_i), $b_i \equiv m_i \pmod{\mathfrak{p}^*}$, m_i in M. Da M ein M-System ist, existieren Elemente m_i' in (m_i) derart, daß das Produkt $m_1' \cdot m_2'$ in M und damit nicht in $\mathfrak{p}^*$ liegt. m_1' entsteht dabei aus m_1 durch eine Reihe von Multiplikationen mit Elementen aus $\mathfrak{o}$ und dazwischengeschaltete Additionen der Produkte bzw. des Elementes m_1 selbst. Wendet man dieselben Operationen auf b_1 an, so ergibt sich ein Element $b_1' \equiv m_1' \pmod{\mathfrak{p}^*}$, das in (b_1) liegt; analog $b_2' \equiv m_2'$. Aus $b_i' \subset (b_i) \subseteqq (a_i)$, $b_1' \cdot b_2' \equiv m_1' \cdot m_2' \not\equiv 0 \pmod{\mathfrak{p}^*}$ folgt $(a_1) \cdot (a_2) \nsubseteq \mathfrak{p}^*$, also $\mathfrak{p}^*$ prim. — Da $\mathfrak{p}^*$ M nicht trifft, ist $C(\mathfrak{p}^*)$ nach Satz 4 ein M umfassendes M-System, das, wegen $\mathfrak{p}^* \supseteqq \mathfrak{a}$, $\mathfrak{a}$ nicht trifft. Folglich muß $C(\mathfrak{p}^*) = M$ sein, da M als maximal vorausgesetzt war, was $\mathfrak{p}^*$ gleich $\mathfrak{p}$, also $\mathfrak{p}$ Primideal nach sich zieht. — Daß schließlich $\mathfrak{p}$ minimales Primoberideal von $\mathfrak{a}$ ist, folgt daraus, daß das Komplement $C(\mathfrak{p}')$ eines Primideales $\mathfrak{p}'$ mit $\mathfrak{a} \subseteqq \mathfrak{p}' \subset \mathfrak{p}$ ein $\mathfrak{a}$ nicht treffendes, M echt umfassendes M-System wäre. — 2. Wenn $\mathfrak{p}$ minimales Primoberideal von $\mathfrak{a}$, ist $C(\mathfrak{p})$ ein $\mathfrak{a}$ nicht treffendes M-System. Es muß maximal sein, weil es sonst ein maximales M-System $M' \supset M$, $M' \cap \mathfrak{a} = \emptyset$, gäbe, dessen Komplement nach dem in Teil 1 Bewiesenen ein Primoberideal $C(M')$ von $\mathfrak{a}$ mit $\mathfrak{a} \subseteqq C(M') \subset \mathfrak{p}$ wäre. Dabei wurde das Lemma von Zorn auf M-Systeme angewandt; das ist zulässig, weil eine aufsteigende Kette von M-Systemen induktiv ist. (Zum Begriff induktiv vgl. J. Schmidt [*15*].)

In den folgenden Untersuchungen spielt nun der Durchschnitt aller minimalen Primoberideale eines Ideales eine große Rolle.

Definition 3. *Das Radikal* $\mathfrak{r}(\mathfrak{a})$ *eines Ideales* $\mathfrak{a}$ *ist der Durchschnitt aller minimalen Primoberideale von* $\mathfrak{a}$.

Natürlich ist $\mathfrak{r}(\mathfrak{a})$ ein Ideal. — Nach der Bemerkung am Ende des Beweises des vorigen Satzes könnte man $\mathfrak{r}(\mathfrak{a})$ auch als Durchschnitt *aller* Primoberideale von $\mathfrak{a}$ erklären; jedes $\mathfrak{a}$ umfassende Primideal $\mathfrak{p}'$ enthält nämlich ein minimales Primoberideal $\mathfrak{p}$ von $\mathfrak{a}$, da die Komplemente einer absteigenden Kette $\mathfrak{a}$ enthaltender Primideale eine aufsteigende Kette $\mathfrak{a}$ nicht treffender M-Systeme bilden. Daraus läßt sich sogleich ableiten der

Satz 6. $\mathfrak{r}(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{r}(\mathfrak{a}) \cap \mathfrak{r}(\mathfrak{b})$.

Beweis. Jedes Primoberideal von $\mathfrak{a}$ oder von $\mathfrak{b}$ ist auch Primoberideal von $\mathfrak{a} \cap \mathfrak{b}$. Wenn andererseits das Primideal $\mathfrak{p}$ den Durchschnitt $\mathfrak{a} \cap \mathfrak{b}$ enthält, dann auch das Produkt $\mathfrak{a} \cdot \mathfrak{b}$ und folglich, nach Satz 1, mindestens einen der Faktoren $\mathfrak{a}$ und $\mathfrak{b}$.

Satz 7. $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$.

Beweis. $\mathfrak{r}(\mathfrak{a}) \subseteqq \mathfrak{r}(\mathfrak{r}(\mathfrak{a}))$ ist trivial. — Jedes minimale Primoberideal von $\mathfrak{a}$ umfaßt den Durchschnitt aller dieser Ideale, d.h. es ist Primoberideal auch von $\mathfrak{r}(\mathfrak{a})$ und enthält damit, nach Def. 3, $\mathfrak{r}(\mathfrak{r}(\mathfrak{a}))$. Also enthält auch der Durchschnitt $\mathfrak{r}(\mathfrak{a})$ aller dieser Ideale $\mathfrak{r}(\mathfrak{r}(\mathfrak{a}))$.

Dieser Satz ist deshalb außerordentlich wichtig, weil er mitunter die auf Potenzbildungen beruhenden Schlußweisen der additiven Idealtheorie assoziativer Ringe durch Beweismethoden zu ersetzen gestattet, die für beliebige nichtassoziative, und damit nicht einmal mehr potenzassoziative Ringe gelten.

Trivial ist $\mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$ für ein Primideal $\mathfrak{p}$ und die Monotonie, daß aus $\mathfrak{a} \subseteqq \mathfrak{b}$ folgt $\mathfrak{r}(\mathfrak{a}) \subseteqq \mathfrak{r}(\mathfrak{b})$. Für den folgenden Satz benötigt man aber Satz 7:

Satz 8. Aus $\mathfrak{a} \subseteqq \mathfrak{b} \subseteqq \mathfrak{r}(\mathfrak{a})$ folgt $\mathfrak{r}(\mathfrak{a}) = \mathfrak{r}(\mathfrak{b})$.

Beweis. Die Voraussetzung zieht wegen der Monotonie nach sich

$$\mathfrak{r}(\mathfrak{a}) \subseteqq \mathfrak{r}(\mathfrak{b}) \subseteqq \mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a}).$$

Daß $\mathfrak{r}(\mathfrak{a})$ die für ein Radikal übliche Eigenschaft von Satz 10 besitzt, erkennt man am bequemsten aus folgendem, von McCoy [4] für assoziative Ringe aufgestellten

Satz 9. *Ein Ringelement r liegt dann und nur dann in $\mathfrak{r}(\mathfrak{a})$, wenn jedes r enthaltende M-System das Ideal $\mathfrak{a}$ trifft.*

Beweis. Wenn r der Bedingung des Satzes genügt, darf ein M-System, das $\mathfrak{a}$ nicht trifft, r nicht enthalten, also liegt r in dessen Komplement. Insbesondere liegt r in den Komplementen der maximalen $\mathfrak{a}$ nicht treffenden M-Systeme, also nach Satz 5 im Durchschnitt $\mathfrak{r}(\mathfrak{a})$ aller dieser minimalen Primoberideale von $\mathfrak{a}$. — Wenn das Element b der Bedingung des Satzes jedoch nicht genügt, existiert ein b enthaltendes M-System, das $\mathfrak{a}$ nicht trifft; also auch ein maximales derartiges M-System, dessen Komplement, wieder nach Satz 5, ein b nicht enthaltendes, minimales Primoberideal von $\mathfrak{a}$ ist. Folglich liegt b nicht in $\mathfrak{r}(\mathfrak{a})$.

Definition 4. *Das Radikal des Ringes $\mathfrak{o}$ ist das Radikal $\mathfrak{r}(0)$ seines Nullideales* (0).

Satz 10. $\mathfrak{r}(\mathfrak{o}/\mathfrak{r}(0)) = (0)$.

Beweis. Würde das Radikal $\mathfrak{r}(\mathfrak{o}/\mathfrak{r}(0))$ des Restklassenringes $\mathfrak{o}/\mathfrak{r}(0)$ ein von $\bar{0}$ verschiedenes Element $\bar{a}$ enthalten, dann läge ein Urbild a von $\bar{a}$ beim natürlichen Homomorphismus H von $\mathfrak{o}$ auf $\mathfrak{o}/\mathfrak{r}(0)$ nicht in $\mathfrak{r} = \mathfrak{r}(0)$. Demnach gäbe es ein a, aber nicht 0 enthaltendes M-System in $\mathfrak{o}$, also auch ein maximales derartiges System M. Sein Komplement $C(M)$ wäre ein Primideal in $\mathfrak{o}$; es müßte also $\mathfrak{r}$ enthalten. Das ist aber nicht möglich, denn nach dem Isomorphiesatz $\mathfrak{o}/C(M) \cong \mathfrak{o}/\mathfrak{r}/C(M)/\mathfrak{r}$ ginge beim Homomorphismus H das a enthaltende M-System M über in ein $\bar{a}$ enthaltendes M-System $\overline{M}$ in $\mathfrak{o}/\mathfrak{r}$. Da nach Voraussetzung $\bar{a}$ in $\mathfrak{r}(\mathfrak{o}/\mathfrak{r})$ liegt, müßte $\overline{M}$ auch $\bar{0}$ enthalten, während oben gezeigt wurde, daß $\mathfrak{r}$ in $C(M)$, also nicht in M liegt.

Wenn $\mathfrak{b}$ ein Ideal des Ringes $\mathfrak{o}$ ist, läßt $\mathfrak{b}$ sich seinerseits als Ring auffassen und dann dessen Radikal N bilden. Ziemlich trivial ist $\mathfrak{b} \cap \mathfrak{r}(0) \subseteqq N$. Die genauen Bedingungen aber, unter denen das Gleichheitszeichen gilt, sind mir nicht bekannt.

Ein *Ring* $\mathfrak{o}$ heißt *prim*, wenn sein Nullideal es ist, z. B. der Restklassenring von $\mathfrak{o}$ nach einem Primideal. Da $\mathfrak{r}(0) = (0)$ bedeutet, daß der Durchschnitt aller Primideale von $\mathfrak{o}$ gleich (0) ist, folgt auf dem üblichen Wege (s. z. B. Behrens [*3*]), daß ein $\mathfrak{r}$-halbeinfacher Ring subdirekte Summe primer Ringe ist.

Über das Verhältnis von $\mathfrak{r}(0)$ zu andern Radikalbegriffen läßt sich sagen, daß $\mathfrak{r}(0)$ ein Nilideal ist (s. Behrens [*3*]) weil die Menge $\{\mathfrak{P}_n^{(\nu)}(a);\, n, \nu = 1, 2, \ldots\}$ der irgendwie gebildeten Potenzen von a ein a enthaltendes M-System bildet und daher 0 enthalten muß, falls a in $\mathfrak{r}(0)$ liegt. Das Nilradikal $W(\mathfrak{o})$ umfaßt also das Radikal $\mathfrak{r}(0)$. — In assoziativen Ringen mit absteigender Kettenbedingung für Rechtsideale ist nach Hopkins jedes Nilideal $\mathfrak{i}$ nilpotent, und aus $\mathfrak{i}^n \subseteqq \mathfrak{r}(0) \subseteqq \mathfrak{p}$ für alle Primideale von $\mathfrak{o}$ folgt $\mathfrak{i} \subseteqq \mathfrak{p}$, also $\mathfrak{i} \subseteqq \mathfrak{r}(0)$. In diesem Falle ist daher $\mathfrak{r}(0)$ das Radikal von Wedderburn.

Bei einem Noetherschen Ring (kommutativer und assoziativer Ring mit aufsteigender Kettenbedingung für Ideale und Einselement) fällt $\mathfrak{r}(\mathfrak{a})$ zusammen mit dem dort üblichen Radikal als Durchschnitt aller minimalen Primoberideale von $\mathfrak{a}$ (vgl. Krull [*10*] oder Northcott [*12*]).

§ 2. Primärideale

Definition 1. *Das Ideal* $\mathfrak{q}$ *ist (rechts-)primär, wenn aus* $(a) \cdot (b) \subseteqq \mathfrak{q}$, $a \not\subset \mathfrak{q}$ *folgt* $b \subset \mathfrak{r}(\mathfrak{q})$.

Auf Grund des letzten Absatzes von § 1 geht diese Definition für Noethersche Ringe in die dort übliche über. Ähnlich wie bei den Primidealen kann man auch hier (a) und (b) durch beliebige Ideale ersetzen:

Satz 1. $\mathfrak{q}$ *ist dann und nur dann primär, wenn für beliebige Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *aus* $\mathfrak{a} \cdot \mathfrak{b} \subseteqq \mathfrak{q}$, $\mathfrak{a} \not\subseteqq \mathfrak{q}$ *folgt* $\mathfrak{b} \subseteqq \mathfrak{r}(\mathfrak{q})$.

Beweis. 1. Wenn $\mathfrak{a} \not\subseteqq \mathfrak{q}$, $\mathfrak{b} \not\subseteqq \mathfrak{r}(\mathfrak{q})$, gibt es Elemente $a \subset \mathfrak{a}$ und $b \subset \mathfrak{b}$, die nicht in $\mathfrak{q}$ bzw. $\mathfrak{r}(\mathfrak{q})$ liegen. Wenn $\mathfrak{q}$ primär, kann $\mathfrak{q}$ dann nicht $(a) \cdot (b)$, also auch nicht $\mathfrak{a} \cdot \mathfrak{b}$ enthalten. — 2. Mit $a \not\subset \mathfrak{q}$, $b \not\subset \mathfrak{r}(\mathfrak{q})$ liegen auch (a) und (b) nicht in $\mathfrak{q}$ bzw. $\mathfrak{r}(\mathfrak{q})$. Wenn $\mathfrak{q}$ der Bedingung des Satzes genügt, ist $(a) \cdot (b)$ nicht in $\mathfrak{q}$ enthalten, $\mathfrak{q}$ also primär.

Den Hauptunterschied zur Theorie assoziativer Ringe bildet die Tatsache, daß auch bei Voraussetzung sehr scharfer Kettenbedingungen das Radikal eines Primärideales nicht prim zu sein braucht, wie das folgende Beispiel zeigt:

Beispiel 1. $\mathfrak{o}$ sei die kommutative Algebra vom Range drei über einem Grundkörper K der Charakteristik null mit folgender Multiplikationstafel für die Basiselemente A, B, C:

	A	B	C
A	0	A	A
B	A	B	A
C	A	A	C

Sie ist ein *na*-Ring, weil $[A \cdot B] \cdot C = A \neq 0 = A \cdot (B \cdot C)$. — Das Produkt zweier Elemente $a = \alpha A + \beta B + \gamma C$, $a' = \alpha' A + \beta' B + \gamma' C$ in $\mathfrak{o}$ ist $a \cdot a' = * A + \beta\beta' B + \gamma\gamma' C$, wobei der Koeffizient von A in der folgenden Untersuchung nicht gebraucht wird. — Die Mengen $(A) = \{\alpha A; \alpha < K\}$, $\mathfrak{p}_1 = \{\alpha A + \gamma C\}$, $\mathfrak{p}_2 = \{\alpha A + \beta B\}$ sind Ideale in $\mathfrak{o}$. (A) ist in jedem echten Ideal von $\mathfrak{o}$ enthalten, denn, wenn $a \neq 0$, ist bei geeigneter Wahl von β' und γ', $[a \cdot a'] \cdot A = (\beta\beta' + \gamma\gamma') A \neq 0$, wenn nicht $\beta = \gamma = 0$. In diesem Falle aber ist a selbst gleich αA. — $\mathfrak{p}_1$ und $\mathfrak{p}_2$ sind Primideale; wenn nämlich a und a' nicht in $\mathfrak{p}_1$ liegen, also $a \equiv \beta B$, $a' \equiv \beta' B \pmod{\mathfrak{p}_1}$, $\beta, \beta' \neq 0$ sind, gilt

$$(a) \cdot (a') > a \cdot a' \equiv \beta\beta' B \not\equiv 0 \pmod{\mathfrak{p}_1}.$$

Analog für $\mathfrak{p}_2$ mit C statt B. — Es ist $(A) = \mathfrak{p}_1 \cap \mathfrak{p}_2$, also gleich dem Radikal $\mathfrak{r}(0)$, da, wegen $(A) \cdot (A) = (0)$, (0) nicht prim ist. Auch $\mathfrak{r}(0)$ ist nicht prim, da $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \leqq (A)$. Andererseits ist (0) primär. Beweis: $a \neq 0$ zieht $(a) > A$ nach sich. Wenn außerdem $a' \not< \mathfrak{r}$, ist $\beta' \neq 0$ oder $\gamma' \neq 0$, also B oder C in (a'), da A in (a'). Folglich liegt $A = A \cdot B$ oder $A = A \cdot C$ in $(a) \cdot (a')$; dieses Produkt ist also ungleich (0).

Wenn $\mathfrak{q}$ primär ist, braucht $\mathfrak{r}(\mathfrak{q})$ also nicht prim zu sein. Aber auch umgekehrt, wenn $\mathfrak{r}(\mathfrak{a})$ prim ist, braucht $\mathfrak{a}$ nicht primär zu sein, selbst dann nicht, wenn $\mathfrak{r}(\mathfrak{a})$ das einzige Primideal von $\mathfrak{o}$ ist. Dafür das

Beispiel 2 mit der Multiplikationstafel

	A	B	C
A	0	A	0
B	A	C	A
C	0	A	C

Daß diese Algebra $\mathfrak{o}$ wieder ein *na*-Ring ist, zeigt $[C \cdot C] \cdot B = A \neq 0 = C \cdot [C \cdot B]$. — Hier ist $a \cdot a' = \big(\beta\alpha' + (\alpha + \gamma)\beta' + \beta\gamma'\big) A + (\beta\beta' + \gamma\gamma') C$. — Wieder folgt aus $a \neq 0$, daß $(a) \geqq (A) = \{\alpha A\}$, denn 1., wenn $\beta \neq 0$, setze $\alpha' = \beta^{-1}$, $\beta' = \gamma' = 0$; 2., wenn $\beta = 0$, $\alpha + \gamma \neq 0$, setze $\gamma' = 0$, $\beta' = (\alpha + \gamma)^{-1}$; 3., wenn $\beta = \alpha + \gamma = 0$, setze $\beta' = 0$, $\gamma' = \gamma^{-1}$, woraus in diesem Falle zunächst $(a) > C$ sich ergibt, aber dann ist $A = C \cdot B < (C)$. — (A) prim erkennt man daran, daß aus a nicht in $(A) = \{\alpha A\}$, d.h. $\beta \neq 0$ oder $\gamma \neq 0$, folgt $C < (a)$; wenn nämlich $\beta \neq 0$, setze in $a \cdot a'$ das $\alpha' = -(\alpha + \gamma) \cdot \beta^{-2}$, $\beta' = \beta^{-1}$, $\gamma' = 0$; und wenn $\beta = 0$, $\gamma \neq 0$, setze $\beta' = 0$, $\gamma' = \gamma^{-1}$. $a, a' \not< (A)$ zieht also nach sich sowohl C in (a) als auch C in (a'), daher $(a) \cdot (a') > C \cdot C \not< (A)$. — Das Radikal $\mathfrak{r}(0)$ ist demnach gerade gleich (A), also prim. Trotzdem ist (0) kein Primärideal, denn wegen $(C) = \{\alpha A + \gamma C\}$ ist $(A) \cdot (C) = (0)$, aber $A \neq 0$ und $C \not< \mathfrak{r}(0) = (A)$.

Obgleich der Zusammenhang zwischen Primär- und Primidealen hier weniger eng ist als bei den Noetherschen Ringen, allgemeiner als bei den assoziativen Ringen mit aufsteigender Kettenbedingung für Rechtsideale, läßt sich doch ein wesentlicher Teil der Theorie auch für die nichtassoziativen Ringe entwickeln.

Satz 2. *Mit* $\mathfrak{q}$ *und* $\mathfrak{q}'$ *primär,* $\mathfrak{r}(\mathfrak{q}) = \mathfrak{r}(\mathfrak{q}')$ *ist auch* $\mathfrak{q} \cap \mathfrak{q}'$ *primär mit dem selben Radikal.*

Beweis. Sei $(a) \cdot (b)$ in $\mathfrak{q} \cap \mathfrak{q}'$, aber $b \not\subset \mathfrak{r}(\mathfrak{q})$. Daraus folgt $a \subset \mathfrak{q}$, da $\mathfrak{q}$ primär. Wegen $\mathfrak{r}(\mathfrak{q}) = \mathfrak{r}(\mathfrak{q}')$ liegt b ebenfalls nicht in $\mathfrak{r}(\mathfrak{q}')$, also liegt a auch in $\mathfrak{q}'$. — $\mathfrak{r}(\mathfrak{q} \cap \mathfrak{q}') = \mathfrak{r}(\mathfrak{q}) = \mathfrak{r}(\mathfrak{q}')$ folgt aus § 1, Satz 6.

Der folgende Satz zeigt, daß der Durchschnitt von Primäridealen mit verschiedenen Radikalen nicht primär ist. Genauer nennt man einen Durchschnitt $\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$ von Primäridealen *unverkürzbar* (vgl. van der Waerden [*14*], § 87), wenn in ihm kein Primärideal den Durchschnitt der übrigen umfaßt. Dann gilt der

Satz 3. *Wenn* $\mathfrak{d} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *ein unverkürzbarer Durchschnitt von Primäridealen* $\mathfrak{q}_i$ *ist und nicht alle Radikale* $\mathfrak{r}(\mathfrak{q}_i)$ *einander gleich sind, ist* $\mathfrak{d}$ *kein Primärideal.*

Beweis. Für $j = 1, 2, \ldots, n$ ist $\left[\bigcap_{k \neq j} \mathfrak{q}_k\right] \cdot \mathfrak{q}_j \subseteqq \mathfrak{d}$, aber wegen $\bigcap_{k \neq j} \mathfrak{q}_k \nsubseteq \mathfrak{q}_j$ ist $\bigcap_{k \neq j} \mathfrak{q}_k \nsubseteq \mathfrak{d}$. Wenn $\mathfrak{d}$ primär ist, folgt $\mathfrak{q}_j \subseteqq \mathfrak{r}(\mathfrak{d}) = \mathfrak{r}(\bigcap \mathfrak{q}_i) = \bigcap \mathfrak{r}(\mathfrak{q}_i)$, und daraus, nach § 1, Satz 7, $\mathfrak{r}(\mathfrak{q}_j) \subseteqq \mathfrak{r}(\mathfrak{r}(\mathfrak{d})) = \mathfrak{r}(\mathfrak{d}) = \bigcap \mathfrak{r}(\mathfrak{q}_i)$. Aus $\mathfrak{r}(\mathfrak{q}_j) \subseteqq \mathfrak{r}(\mathfrak{q}_i)$ für alle i und j folgt, daß alle $\mathfrak{r}(\mathfrak{q}_i)$ übereinstimmen müssen.

Diese Primärideale kann man auch mit Hilfe des Begriffes relativ — (rechts)prim erklären:

Definition 2. *Der Quotient zweier Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *ist*

$$\mathfrak{a} : \mathfrak{b} = \{x;\, x \subset \mathfrak{o},\, (x) \cdot (b) \subset \mathfrak{a} \text{ für alle } b \text{ aus } \mathfrak{b}\}.$$

Man sieht sofort, daß $\mathfrak{a} : \mathfrak{b}$ ein $\mathfrak{a}$ umfassendes Ideal ist, und sagt, $\mathfrak{b}$ ist *relativ prim zu* $\mathfrak{a}$, wenn $\mathfrak{a} : \mathfrak{b} = \mathfrak{a}$ ist.

Satz 4. *Ein Ideal* $\mathfrak{p}$ *ist dann und nur dann prim, wenn* $\mathfrak{p} : \mathfrak{b} = \mathfrak{p}$ *für alle* $\mathfrak{b} \nsubseteq \mathfrak{p}$. *Ein Ideal* $\mathfrak{q}$ *ist dann und nur dann primär, wenn* $\mathfrak{q} : \mathfrak{b} = \mathfrak{q}$ *ist für alle* $\mathfrak{b} \nsubseteq \mathfrak{r}(\mathfrak{q})$.

Beide Behauptungen folgen sofort aus den Definitionen eines Prim- bzw. eines Primärideales.

Korollar. *Sei* $\mathfrak{q}$ *primär und* $\mathfrak{r}(\mathfrak{q}) = \bigcap \mathfrak{p}_\iota$. *Wenn* $b \not\subset \mathfrak{p}_\lambda$ *für mindestens ein* λ, *ist* $\mathfrak{q} : (b) = \mathfrak{q}$.

Beweis. Aus $b \not\subset \mathfrak{p}_\lambda$ folgt $b \not\subset \mathfrak{r}(\mathfrak{q})$.

Wenn q in $\mathfrak{q}$ liegt, ist natürlich $\mathfrak{q} : (q) = \mathfrak{o}$. In assoziativen Ringen mit aufsteigender Kettenbedingung ist für jedes b aus $\mathfrak{r}(\mathfrak{q})$ der Quotient $\mathfrak{q} : (b)$ echtes Oberideal von $\mathfrak{q}$ (vgl. Murdoch [*11*], th. 12). Das folgende Beispiel 3 zeigt, daß das für einen *na*-Ring nicht mehr richtig zu sein braucht. Wohl aber läßt sich sagen, daß, wenn $\mathfrak{q}$ primär, aber ungleich $\mathfrak{o}$ ist, stets ein Element b in $\mathfrak{r}(\mathfrak{q})$ mit der Eigenschaft $\mathfrak{q} : (b) > \mathfrak{q}$ existiert: Wenn nämlich $\mathfrak{q}$ sogar prim ist, gilt, für alle b in $\mathfrak{r}(\mathfrak{q}) = \mathfrak{q}$, $\mathfrak{q} : (b) = \mathfrak{o}$; wenn aber $\mathfrak{q}$ nicht prim ist, gibt es zwei Elemente a und b in $\mathfrak{o}$, die beide nicht zu $\mathfrak{q}$ gehören und für die $(a)\cdot(b)$ in $\mathfrak{q}$ liegt. Aus $\mathfrak{q}$ primär folgt dann $b < \mathfrak{r}(\mathfrak{q})$, und, da $a \not< \mathfrak{q}$, ist $\mathfrak{q}:(b) > \mathfrak{q}$.

Beispiel 3. Wieder sei $\mathfrak{o}$ eine kommutative Algebra über K mit den Basiselementen A, B, E und der Multiplikationstafel

	A	B	E
A	0	A	A
B	A	A	B
E	A	B	E

$\mathfrak{o}$ ist *na*-Ring, weil $A\cdot[B\cdot B]=0 \neq A=[A\cdot B]\cdot B$. E ist in $\mathfrak{o}$ das Einselement. — Für $a=\alpha A+\beta B+\varepsilon E$, $a'=\alpha' A+\beta' B+\varepsilon' E$ ist $a\cdot a'=*A+(\varepsilon\beta'+\beta\varepsilon')B+\varepsilon\varepsilon' E$. — $(A)=\{\alpha A;\alpha < K\}$ ist ein Ideal, das in jedem von (0) verschiedenen Ideal enthalten ist. Beweis: Zu untersuchen ist nur der Fall, daß $a \not< (A)$, also $\beta \neq 0$ oder $\varepsilon \neq 0$. Aus $[a\cdot a']\cdot A=[\varepsilon\beta'+[\beta+\varepsilon]\varepsilon']A$ folgt, daß sowohl für $\varepsilon=0$ das Element A in (a) liegt (setze $\varepsilon'=\beta^{-1}$), als auch für $\varepsilon \neq 0$ (setze $\beta'=\varepsilon^{-1}$, $\varepsilon'=0$). — Wenn $a \not< (A)$, gilt sogar schärfer, daß $(a) \geqq \{\alpha A+\beta B\}=\mathfrak{r}$. Da $A < (a)$, folgt aus dem Ausdruck für $a\cdot a'$, daß $[\varepsilon\beta'+\beta\varepsilon']B+\varepsilon\varepsilon' E$ in (a) liegt, und daraus, daß B in (a) enthalten ist (setze für β' und ε' dieselben Werte wie eben ein). — Das Ideal $\mathfrak{r}$ ist das Radikal $\mathfrak{r}(0)$, weil die einzigen $\mathfrak{r}$ nicht enthaltenden Ideale des Ringes, nämlich (0) und (A), nicht prim sind, wohl aber $\mathfrak{r}$ selbst; einerseits ist nämlich $(A)\cdot(A)=(0)$ sowie $(B)\cdot(B)=\mathfrak{r}\cdot\mathfrak{r}=(A)$, und andererseits folgt aus $a, a' \not< \mathfrak{r}$, d.h. aus $a\equiv\varepsilon E$, $a'\equiv\varepsilon' E \pmod{\mathfrak{r}}$, daß $a\cdot a'\equiv\varepsilon\cdot\varepsilon' E \not\equiv 0 \pmod{\mathfrak{r}}$, also $\mathfrak{r}$ prim ist. — Das Ideal (0) ist primär, weil aus $a\neq 0$ folgt $(a) > A$ und weil, falls $a' \not< \mathfrak{r}$ gilt, (a') das Einselement E enthält; denn, wie oben gezeigt, zieht $(a') \not\leqq \mathfrak{r}$, also $(a') \not\leqq (A)$, nach sich $(a') \geqq \mathfrak{r}$, und daher $(a') > \mathfrak{r}$; dann umfaßt aber $(a)\cdot(a')$ das Element $A\cdot E=A\neq 0$. — Obwohl B in $\mathfrak{r}(0)$ liegt, ist $(0):(B)=(0)$, denn wäre in $(x)\cdot(B)=(0)$ das $x\neq 0$, dann enthielte (x) das Element A, also $(x)\cdot(B)$ das Produkt $A\cdot B=A\neq 0$.

Satz 5. *Wenn $\mathfrak{o}$ kommutativ, $\mathfrak{q}$ primär und $a \not< \mathfrak{q}$, ist $\mathfrak{q}:(a) \leqq \mathfrak{r}(\mathfrak{q})$ und $\mathfrak{r}(\mathfrak{q}:(a))=\mathfrak{r}(\mathfrak{q})$.*

Beweis. x in $\mathfrak{q}:(a)$ ist äquivalent $(x)\cdot(a)=(a)\cdot(x) \leqq \mathfrak{q}$, da $\mathfrak{o}$ kommutativ ist. Wenn $a \not< \mathfrak{q}$, liegt $x < \mathfrak{r}(\mathfrak{q})$, da $\mathfrak{q}$ primär. — Nach § 1, Satz 8, folgt aus $\mathfrak{q} \leqq \mathfrak{q}:(a) \leqq \mathfrak{r}(\mathfrak{q})$, daß $\mathfrak{r}(\mathfrak{q}:(a))=\mathfrak{r}(\mathfrak{q})$ ist.

Bemerkung. Wenn man neben $\mathfrak{a}:\mathfrak{b}$ auch noch den Linksquotienten $\{y;\ (b)\cdot(y) \leqq \mathfrak{a}$ für alle b aus $\mathfrak{b}\}$ heranzöge, würde Satz 5 auch noch für nichtkommutative *na*-Ringe gelten, wobei in ihm $\mathfrak{q}:(a)$ durch den Linksquotienten zu ersetzen wäre.

Eine dritte Möglichkeit, diese Primärideale zu definieren, ergibt sich aus folgender Definition:

Definition 3. *M sei ein M-System. Die M-Komponente eines Ideales $\mathfrak{a}$ ist $\mathfrak{a}_M=\{x;\ (x)\cdot(c) \leqq \mathfrak{a}$ für mindestens ein c aus $M\}$.*

Satz 6. *$\mathfrak{a}_M$ ist ein Ideal in $\mathfrak{o}$.*

Beweis. Mit $x' \subset (x)$ ist auch $(x') \subseteqq (x)$. Daher braucht nur noch gezeigt zu werden, daß mit x und y auch $x - y$ in $\mathfrak{a}_M$ liegt. Sei $(x) \cdot (c) \subseteqq \mathfrak{a}$ und $(y) \cdot (d) \subseteqq \mathfrak{a}$, $c, d \subset M$. Für geeignete c' in (c) und d' in (d) liegt das Produkt $c' \cdot d'$ in M, da M ein M-System ist. Andererseits ist das Produkt

$$(x - y) \cdot (c' \cdot d') \subseteqq (x) \cdot (c' \cdot d') + (y) \cdot (c' \cdot d') \subseteqq (x) \cdot (c') + (y) \cdot (d') \subseteqq \mathfrak{a}.$$

Satz 7. *Das Ideal $\mathfrak{q}$ ist dann und nur dann primär, wenn für jedes M-System in $\mathfrak{o}$ entweder $\mathfrak{q}_M = \mathfrak{q}$ oder $\mathfrak{q}_M = \mathfrak{o}$ gilt.*

Beweis. 1. Das Ideal $\mathfrak{a} \neq \mathfrak{o}$ sei nicht primär, d.h. es gibt ein $b \not\subset \mathfrak{a}$ und ein $c \not\subset \mathfrak{r}(\mathfrak{a})$ mit $(b) \cdot (c) \subseteqq \mathfrak{a}$. Sei $\mathfrak{r}(\mathfrak{a}) = \bigcap \mathfrak{p}_\iota$. Da $c \not\subset \mathfrak{r}(\mathfrak{a})$, ist $c \not\subset \mathfrak{p}_\lambda$ für mindestens ein λ, also c in der Komplementärmenge $C(\mathfrak{p}_\lambda) = M$. Daher liegt b in $\mathfrak{a}_M$ für dieses M, aber nicht in $\mathfrak{a}$, also ist $\mathfrak{a}_M > \mathfrak{a}$. — $\mathfrak{a}_M$ kann aber auch nicht gleich dem ganzen Ring $\mathfrak{o}$ sein, weil sonst c in $\mathfrak{a}_M$ läge und daraus die Existenz eines d in M mit $(c) \cdot (d) \subseteqq \mathfrak{a} \subseteqq \mathfrak{r}(\mathfrak{a}) \subseteqq \mathfrak{p}_\lambda$ folgen würde, andererseits aber c und d beide in M, also nicht in dem Primideal $\mathfrak{p}_\lambda$ enthalten wären. — 2. Für mindestens ein M-System sei $\mathfrak{o} > \mathfrak{a}_M > \mathfrak{a}$ und etwa $(b) \cdot (c) \subseteqq \mathfrak{a}$, $b \not\subset \mathfrak{a}$, $c \subset M$. Dann muß $M \cap \mathfrak{a}$ leer sein, andernfalls würde nämlich aus der Existenz eines a in $M \cap \mathfrak{a}$ folgen $\mathfrak{o} \cdot (a) \subseteqq \mathfrak{a}$, also $\mathfrak{a}_M = \mathfrak{o}$. Nun sei M' ein maximales M enthaltendes und $\mathfrak{a}$ nicht treffendes M-System. Nach § 1, Satz 5, ist sein Komplement $C(M') = \mathfrak{p}_\lambda$ ein minimales Primoberideal von $\mathfrak{a}$. Da

$$c \subset M \subseteqq M' = C(\mathfrak{p}_\lambda),$$

liegt c nicht in $\mathfrak{p}_\lambda$, also auch nicht in $\mathfrak{r}(\mathfrak{a}) = \bigcap \mathfrak{p}_\iota$. Aus $c \not\subset \mathfrak{r}(\mathfrak{a})$, aber nach Voraussetzung $(b) \cdot (c) \subseteqq \mathfrak{a}$, $b \not\subset \mathfrak{a}$, erkennt man, daß $\mathfrak{a}$ nicht primär ist.

In Noetherschen Ringen folgt aus der aufsteigenden Kettenbedingung, daß für ein Primärideal $\mathfrak{q}$ eine Potenz des zugehörigen Primideales $\mathfrak{p}$ in $\mathfrak{q}$ enthalten ist. Das erwies sich auch für nichtkommutative, aber assoziative Ringe als richtig (Murdoch [*11*]) und läßt sich auf *na*-Ringe verallgemeinern, wie Satz 9 zeigen wird. Dazu braucht man

Satz 8. *Wenn $\mathfrak{o}$ die aufsteigende Kettenbedingung für zweiseitige Ideale erfüllt, ist das Radikal eines jeden Ideales $\mathfrak{a}$ von $\mathfrak{o}$ Durchschnitt von nur endlich vielen Primidealen.*

Beweis. Wenn $\mathfrak{a}$ prim, ist alles klar. — Andernfalls gibt es zwei Elemente $b, c \not\subset \mathfrak{a}$ mit $(b) \cdot (c) \subseteqq \mathfrak{a}$. Hätte nun $\mathfrak{a}$ unendlich viele minimale Primoberideale $\mathfrak{p}_\iota$, dann hätte, wegen $(\mathfrak{a}, b) \cdot (\mathfrak{a}, c) \subseteqq \mathfrak{a} \subseteqq \mathfrak{p}_\iota$ mindestens einer der beiden Faktoren ebenfalls unendlich viele unter den $\mathfrak{p}_\iota$ zu minimalen Primoberidealen, wäre also nicht prim. Derselbe Schluß ließe sich auf $(\mathfrak{a}, b)$ bzw. $(\mathfrak{a}, c)$ anwenden und ergäbe bei Fortsetzung eine aufsteigende Kette echt ineinander enthaltener Ideale, die nicht abbräche, q. e. a.

Satz 9. *In $\mathfrak{o}$ gelte die aufsteigende Kettenbedingung. Daher ist $\mathfrak{r}(\mathfrak{a}) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ Durchschnitt bereits endlich vieler Primideale. Dann liegt ein gewisses Produkt $\mathfrak{P}$ der $\mathfrak{p}_i$ in $\mathfrak{a}$, wobei in $\mathfrak{P}$ jedes $\mathfrak{p}_i$ mehrfach auftreten kann.*

Beweis durch Teilerinduktion (vgl. van der Waerden [*14*], § 84): Der Fall $\mathfrak{a}$ prim ist wieder trivial. — Wenn $\mathfrak{a}$ nicht prim, seien b und c wie beim Beweis des vorigen Satzes gewählt und $\mathfrak{p}'_1, \mathfrak{p}'_2, \ldots, \mathfrak{p}'_r$ die endlich vielen minimalen Primoberideale von $(\mathfrak{a}, b)$ bzw. $\mathfrak{p}'_{r+1}, \ldots, \mathfrak{p}'_s$ die von $(\mathfrak{a}, c)$. Nach Induktionsannahme ist ein gewisses Produkt $\mathfrak{P}'(\mathfrak{p}'_1, \ldots, \mathfrak{p}'_r) \subseteqq (\mathfrak{a}, b)$ und ein Produkt $\mathfrak{P}''(\mathfrak{p}'_{r+1}, \ldots, \mathfrak{p}'_s) \subseteqq (\mathfrak{a}, c)$. Daraus folgt, daß $\mathfrak{P}' \cdot \mathfrak{P}'' < (\mathfrak{a}, b) \cdot (\mathfrak{a}, c) \subseteqq \mathfrak{a}$. Jedes der Ideale $\mathfrak{p}'_k$ ist nun Primoberideal von $\mathfrak{a}$, enthält also nach dem zweiten Teil des Beweises von Satz 5 in § 1 eines der minimalen Primoberideale von $\mathfrak{a}$, etwa $\mathfrak{p}_i(k)$. Daraus folgt, daß auch $\mathfrak{P}'(\mathfrak{p}_{i(1)}, \ldots, \mathfrak{p}_{i(r)}) \cdot \mathfrak{P}''(\mathfrak{p}_{i(r+1)}, \ldots, \mathfrak{p}_{i(s)})$ in $\mathfrak{a}$ liegt.

Korollar. *Bei aufsteigender Kettenbedingung für zweiseitige Ideale in* $\mathfrak{o}$ *liegt eine gewisse Potenz von* $\mathfrak{r}(\mathfrak{a})$ *in* $\mathfrak{a}$.

Beweis. $\mathfrak{r}(\mathfrak{a})$ ist in jedem der $\mathfrak{p}_i$ von Satz 9 enthalten.

Dieses Korollar spielt beim Aufbau der Idealtheorie der *na*-Ringe keine so große Rolle wie bei den assoziativen Ringen, denn durch die Bildungen $\mathfrak{P}' \cdot \mathfrak{P}''$ kommt eine Klammersetzung in die Produkte herein. Es läßt sich z. B. beim Beweis der Sätze 2 und 3 nicht, wie sonst üblich, verwenden, sondern dort wurde $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$ herangezogen, s. auch § 3, Satz 1.

Wenn $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ ein Durchschnitt von Primäridealen und, nach dem letzten Korollar, $\mathfrak{P}_i(\mathfrak{r}(\mathfrak{q}_i)) \subseteqq \mathfrak{q}_i$, $i = 1, 2, \ldots, n$, ist, liegt $\mathfrak{P}_1 \cdot \mathfrak{P}_2 \ldots \mathfrak{P}_n \subseteqq \mathfrak{a}$ unabhängig von der Klammersetzung zwischen den $\mathfrak{P}_i$ (da deren Produkt immer im Durchschnitt liegt), aber abhängig natürlich von der Art der Potenzbildungen bei den einzelnen $\mathfrak{r}(\mathfrak{q}_i)$.

§ 3. Eindeutigkeitssätze für Durchschnitte von Primäridealen

In assoziativen und kommutativen Ringen mit Einselementen garantiert die aufsteigende Kettenbedingung für Ideale, daß jedes Ideal des Ringes sich als Durchschnitt primärer Ideale darstellen läßt. Das ist aber bekanntlich nicht mehr richtig, wenn man die Forderung der Kommutativität wegläßt, z. B. im Ring der Polynome in zwei nicht vertauschbaren Unbestimmten mit Koeffizienten aus einem Körper (s. Murdoch [*11*]). Andererseits liegt es aber auch nicht am Kommutativgesetz allein, denn das Beispiel 2 in § 2 ist eine kommutative Algebra endlichen Ranges, in der (0) weder Primärideal noch als Durchschnitt von Primäridealen darstellbar ist, da jedes von (0) verschiedene Ideal das Ideal $(A) \neq (0)$ enthält. — Mit der üblichen verbandstheoretischen Schlußweise (vgl. van der Waerden [*14*], § 87) kann man auch in *na*-Ringen mit aufsteigender Kettenbedingung für zweiseitige Ideale zeigen, daß sich jedes Ideal als Durchschnitt endlich vieler irreduzibler Ideale darstellen läßt, aber ein irreduzibles Ideal braucht eben nicht primär zu sein.

Dagegen lassen sich die Eindeutigkeitssätze übertragen. Wenn man also fragt, wie weit es möglich ist, einen Durchschnitt von Primäridealen als Durchschnitt von anderen Primäridealen darzustellen, findet man, daß in einer „Normaldarstellung" sowohl die Anzahl der Primärideale als auch deren zugehörige Radikale festgelegt sind. Auch das Auftreten der „isolierten Komponenten" in jeder solchen Darstellung des Durchschnittsideales läßt sich bei geeigneter Definition dieser Komponenten beweisen.

Zum Begriff der Normaldarstellung gelangt man so: In einer Darstellung eines Ideales $\mathfrak{a}$ als Durchschnitt endlich vieler Primärideale kann man alle diejenigen, die dasselbe Radikal besitzen, nach § 2, Satz 2, zu einem Primärideal zusammenfassen und dann den unverkürzbaren Durchschnitt bilden, d.h. diejenigen Primärideale, die den Durchschnitt der übrigen umfassen, der Reihe nach weglassen. In der so erhaltenen *Normaldarstellung* $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ ist nach § 2, Satz 3, der Durchschnitt beliebiger unter diesen Primäridealen nicht mehr primär und stets ist $\mathfrak{r}(\mathfrak{q}_i) \neq \mathfrak{r}(\mathfrak{q}_k)$ für $i \neq k$. Wir wollen die $\mathfrak{q}_i$ einer Normaldarstellung von $\mathfrak{a}$ auch *Primärkomponenten* von $\mathfrak{a}$ nennen.

Satz 1. *In zwei Normaldarstellungen* $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ *und* $\mathfrak{a} = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_n$ *ist* $m = n$ *und bei passender Numerierung* $\mathfrak{r}(\mathfrak{q}_i) = \mathfrak{r}(\mathfrak{q}'_i)$ *für* $i = 1, 2, \ldots, m$.

Beweis. Bei $\mathfrak{a} = \mathfrak{o}$ muß $m = n = 1$ und $\mathfrak{q}_1 = \mathfrak{q}'_1 = \mathfrak{r}(\mathfrak{q}_1) = \mathfrak{r}(\mathfrak{q}'_1) = \mathfrak{o}$ sein. — Es sei also $\mathfrak{a} \neq \mathfrak{o}$ und etwa $\mathfrak{r}_m = \mathfrak{r}(\mathfrak{q}_m)$ maximal unter den $m+n$ Idealen $\mathfrak{r}_i = \mathfrak{r}(\mathfrak{q}_i)$, $\mathfrak{r}'_j = \mathfrak{r}(\mathfrak{q}'_j)$, d.h. $\mathfrak{r}_m$ werde von keinem der $\mathfrak{r}_i, \mathfrak{r}'_j$ als echtem Oberideal umfaßt. Würde nun $\mathfrak{r}_m$ unter den $\mathfrak{r}'_1, \ldots, \mathfrak{r}'_n$ nicht auftreten, so würde auch $\mathfrak{q}_m$ in keinem der $\mathfrak{r}'_j$ enthalten sein, weil $\mathfrak{q}_m \subseteqq \mathfrak{r}'_j$ gemäß § 1, Satz 7, nach sich zöge $\mathfrak{r}_m = \mathfrak{r}(\mathfrak{q}_m) \subseteqq \mathfrak{r}(\mathfrak{r}'_j) = \mathfrak{r}(\mathfrak{r}(\mathfrak{q}'_j)) = \mathfrak{r}(\mathfrak{q}'_j) = \mathfrak{r}'_j$. Aus $\mathfrak{q}_m \nsubseteq \mathfrak{r}'_j$ für $j = 1, \ldots, n$ folgt nach § 2, Satz 4, $\mathfrak{q}'_j : \mathfrak{q}_m = \mathfrak{q}'_j$. Andererseits liegt auch $\mathfrak{q}_m$ in keinem der $\mathfrak{r}_1, \ldots, \mathfrak{r}_{m-1}$, weil sonst $\mathfrak{r}_m = \mathfrak{r}(\mathfrak{q}_m)$ in einem von ihnen läge, also auf Grund der Maximalität von $\mathfrak{r}_m$ gleich diesem Radikal wäre, was in einer Normaldarstellung unmöglich ist. Daraus folgt $\mathfrak{q}_i : \mathfrak{q}_m = \mathfrak{q}_i$ für $i = 1, 2, \ldots, m-1$. Auch in *na*-Ringen gilt die Rechenregel

$$[\mathfrak{a} \cap \mathfrak{b}] : \mathfrak{c} = [\mathfrak{a} : \mathfrak{c}] \cap [\mathfrak{b} : \mathfrak{c}].$$

Mit ihrer Hilfe sieht man sofort

$$\begin{aligned} \mathfrak{a} : \mathfrak{q}_m &= \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_n = \mathfrak{a} \\ &= \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{m-1}, \end{aligned}$$

da $\mathfrak{q}_m : \mathfrak{q}_m = \mathfrak{o}$ ist. Das widerspricht aber der Unverkürzbarkeit der Normaldarstellung von $\mathfrak{a}$ durch die $\mathfrak{q}_i$. Also tritt $\mathfrak{r}_m$ unter den $\mathfrak{r}'_j$ auf; es sei etwa $\mathfrak{r}_m = \mathfrak{r}'_n$. Sollte $m = 1$ sein, so wäre $\mathfrak{a} : \mathfrak{q}_1 = \mathfrak{o} = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_n$, was $\mathfrak{q}'_j \subset \mathfrak{o}$ widerspräche (Normaldarstellung!), falls $\mathfrak{r}_1$ ungleich allen $\mathfrak{r}'_j$ wäre. — Nach § 2, Satz 2, ist wegen $\mathfrak{r}(\mathfrak{q}_m) = \mathfrak{r}(\mathfrak{q}'_n)$ auch $\mathfrak{q}_m \cap \mathfrak{q}'_n = \mathfrak{q}$ primär und $\mathfrak{r}(\mathfrak{q}) = \mathfrak{r}(\mathfrak{q}_m)$. Nach genau denselben Schlüssen wie oben folgt wegen der Maximalität von $\mathfrak{r}_m$

$$\begin{aligned} \mathfrak{a} : \mathfrak{q} &= \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{n-1} \\ &= \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_{m-1}. \end{aligned}$$

Diese Schlußweise läßt sich für $\mathfrak{a} : \mathfrak{q}$ statt $\mathfrak{a}$ wiederholen und führt schließlich, falls etwa $m < n$ wäre, zu $\mathfrak{o} = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{n-m}$. Also müßte eines der $\mathfrak{q}'_j = \mathfrak{o}$ sein, die Darstellung von $\mathfrak{a}$ wäre also verkürzbar, q. e. a.

Aus der im Beweis benutzten Rechenregel folgt auch

Satz 2. *Wenn* $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *und* $\mathfrak{b} \nsubseteq \mathfrak{r}(\mathfrak{q}_i)$ *für* $i = 1, 2, \ldots, n$, *ist* $\mathfrak{a} : \mathfrak{b} = \mathfrak{a}$.

Satz 3. *M sei ein M-System und* $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, *alle* $\mathfrak{q}_i$ *primär. Ferner sei* $\mathfrak{r}_i = \mathfrak{r}(\mathfrak{q}_i)$ *und* $M \cap \mathfrak{r}_i = \emptyset$ *für* $i = 1, \ldots, m$ *und* $M \cap \mathfrak{r}_k \neq \emptyset$ *für* $k = m+1, \ldots, n$. *Dann ist* $\mathfrak{a}_M = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$.

Beweis. 1. Aus x in $\mathfrak{a}_M$ folgt $(x) \cdot (c) \subseteq \mathfrak{a}$ für mindestens ein c aus M. Da $M \cap \mathfrak{r}_i = \emptyset$ für $i = 1, \ldots, m$ ist $c \nsubseteq \mathfrak{r}_i$, also x in $\mathfrak{q}_i$ für diese i. — 2. Sei $y \subset \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$. Für $k = m+1, \ldots, n$ ist auch $M \cap \mathfrak{q}_k \neq \emptyset$ nach § 1, Satz 9, da $\mathfrak{r}_k$ das Radikal von $\mathfrak{q}_k$ ist. Sei etwa q_k in $M \cap \mathfrak{r}_k$ für diese k. Da M ein M-System ist, gibt es in (q_{m+1}) und (q_{m+2}) zwei Elemente q'_{m+1} bzw. q'_{m+2} mit $q''_{m+2} = q'_{m+1} \cdot q'_{m+2}$ in M, also auch $q''_{m+2} \subset \mathfrak{q}_{m+1} \cap \mathfrak{q}_{m+2} \cap M$. Wieder existieren in (q''_{m+2}) und (q_{m+3}) zwei Elemente q'_{m+2} und q'_{m+3} mit $q''_{m+3} = q'_{m+2} \cdot q'_{m+3}$ in M. Und so weiter bis schließlich $q''_n \subset \mathfrak{q}_{m+1} \cap \cdots \cap \mathfrak{q}_n \cap M$ erreicht ist. Dann liegt aber $(y) \cdot (q''_n)$ in $[\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m] \cdot [\mathfrak{q}_{m+1} \cap \cdots \cap \mathfrak{q}_n] \subseteq \mathfrak{a}$ und q''_n in M, also gehört y zu $\mathfrak{a}_M$.

Aus diesem Satz läßt sich der zweite Eindeutigkeitssatz ableiten:

Satz 4. *Es sei* $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *eine Normaldarstellung von* $\mathfrak{a}$ *und die* $\mathfrak{r}(\mathfrak{q}_i)$ *Durchschnitt jeweils endlich vieler* $\mathfrak{p}_{ik}$, $i = 1, \ldots, n$; $k = 1, \ldots, n_i$. *Dann tritt* $\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_t$ *in jeder Normaldarstellung von* $\mathfrak{a}$ *auf, falls es zu jedem der Primärideale* $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ *unter den zugehörigen minimalen Primoberidealen mindestens eines,* $\mathfrak{p}_{ik_i} = \mathfrak{p}'_i$, *gibt, das keines der zugehörigen minimalen Primoberideale* $\mathfrak{p}_{jk}$ *der restlichen Primärideale enthält.*

Beweis. $C(\mathfrak{p}'_i) = M_i$ ist ein M-System, $i = 1, \ldots, t$. Für $j = t+1, \ldots, n$ liegt nun nach Voraussetzung kein $\mathfrak{p}_{jk}$ in $\mathfrak{p}'_i$, also auch nicht $\mathfrak{r}_j = \mathfrak{p}_{j1} \cap \cdots \cap \mathfrak{p}_{jn_j}$, da $\mathfrak{p}'_i$ prim ist und nach § 1, Satz 2, $\mathfrak{r}_j$ das Produkt der $\mathfrak{p}_{jk}$ enthält. Aus $\mathfrak{r}_j$ nicht in $\mathfrak{p}'_i$ folgt, für $i = 1, \ldots, t$, $M_i \cap \mathfrak{r}_j \neq \emptyset$, also ist nach Satz 3 $\mathfrak{a}_{M_i}$ Oberideal von $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$. — Andererseits ist $M_i \cap \mathfrak{p}'_i = \emptyset$, folglich tritt, wieder nach Satz 3, in der Durchschnittsdarstellung von $\mathfrak{a}_{M_i}$ zumindest $\mathfrak{q}_i$ auf. Dies zieht, zusammen mit dem zuerst Bewiesenen, $\mathfrak{a}_{M_1} \cap \cdots \cap \mathfrak{a}_{M_t} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ nach sich, wobei zur Definition der linken Seite der Gleichung nur die $\mathfrak{p}'_i$, also nur die Radikale $\mathfrak{r}_1, \ldots, \mathfrak{r}_n$ benötigt werden, die nach Satz 1 in jeder Normaldarstellung von $\mathfrak{a}$ auftreten.

Die Voraussetzung, daß jedes $\mathfrak{r}_i$ Durchschnitt nur endlich vieler Primideale ist, ist nach § 2, Satz 8, sicher dann erfüllt, wenn in $\mathfrak{o}$ die aufsteigende Kettenbedingung für zweiseitige Ideale gilt. Aus dieser Bedingung folgt auch, daß ein Radikal $\mathfrak{r}(\mathfrak{a})$ dann und nur dann primär ist, wenn $\mathfrak{r}(\mathfrak{a})$ prim ist, denn jedes Primideal ist primär und sein eigenes Radikal, andererseits ist nach § 2, Satz 3, der Durchschnitt endlich vieler Primärideale zu verschiedenen Radikalen nicht primär. Schließlich kann man zeigen den

Satz 5. *Es sei* $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *und jedes* $\mathfrak{r}(\mathfrak{q}_i)$ *der Durchschnitt nur endlich vieler Primideale* $\mathfrak{p}_{ik}$, $i = 1, \ldots, n$; $k = 1, \ldots, n_i$. *Dann sind die minimalen Primoberideale von* $\mathfrak{a}$ *genau diejenigen unter den* $\mathfrak{p}_{ik}$, *die in der Menge der* $\mathfrak{p}_{ik}$ *minimal sind.*

Beweis. Nach § 2, Satz 9, liegt das Produkt $\mathfrak{P}_1 \dots \mathfrak{P}_n$ in $\mathfrak{a}$, wobei $\mathfrak{P}_i(\mathfrak{p}_{i1}, \dots, \mathfrak{p}_{in_i})$ ein Produkt der $\mathfrak{p}_{ik}$ aus $\mathfrak{r}(\mathfrak{q}_i)$ ist. Jedes Primoberideal $\mathfrak{p}$ von $\mathfrak{a}$ enthält also nach § 1, Satz 2, mindestens eines der Ideale $\mathfrak{p}_{ik}$, etwa $\mathfrak{p}_{rs}$. Wenn $\mathfrak{p}$ sogar minimales Primoberideal von $\mathfrak{a}$ ist, muß $\mathfrak{p}$ gleich diesem $\mathfrak{p}_{rs}$ und $\mathfrak{p}_{rs}$ minimal in der Menge der $\mathfrak{p}_{ik}$ sein. — Wenn andererseits $\mathfrak{p}_{rs}$ minimal in der Menge der $\mathfrak{p}_{ik}$ ist, muß $\mathfrak{p}_{rs}$ nicht nur Oberideal von $\mathfrak{r}(\mathfrak{q}_r)$ und damit von $\mathfrak{a}$ sein, sondern sogar minimales Primoberideal von $\mathfrak{a}$, denn andernfalls enthielte $\mathfrak{p}_{rs}$ als Primideal wieder ein Primideal $\mathfrak{p}_{nv}$ aus der Menge aller Primideale $\mathfrak{p}_{ik}$ als echtes Unterideal, weil aus $\mathfrak{p}_{rs} > \mathfrak{p} \geqq \mathfrak{a}$ folgt, daß $\mathfrak{P}_1 \cdot \mathfrak{P}_2 \dots \mathfrak{P}_n$ echtes Unterideal von $\mathfrak{p}$ ist.

Literatur

[1] AMITSUR, S. A.: A general theory of radicals. I, II, III. Amer. J. Math. I **74**, 775—786 (1952); II, III **76**, 100—136 (1954). — [2] BAER, R.: Radical ideals. Amer. J. Math. **65**, 537—568 (1943). — [3] BEHRENS, E.-A.: Nichtassoziative Ringe. Math. Ann. **127**, 441—452 (1954). — [4] MCCOY, N. H.: Prime ideals in general rings. Amer. J. Math. **71**, 823—833 (1949). — [5] CURTIS, CH. W.: On additive ideal theory in general rings. Amer. J. Math. **74**, 687—700 (1954). — [6] FITTING, H.: Primärkomponentenzerlegung in nichtkommutativen Ringen. Math. Ann. **111**, 19—41 (1935). — [7] FUCHS, L.: On primal ideals. Proc. Amer. Math. Soc. **1**, 1—8 (1950). — [8] KRULL, W.: Zweiseitige Ideale in nichtkommutativen Bereichen. Math. Z. **28**, 481—503 (1928). — [9] KRULL, W.: Idealtheorie in Ringen ohne Endlichkeitsbedingung. Math. Ann. **101**, 729—744 (1929). — [10] KRULL, W.: Idealtheorie. Berlin 1935. — [11] MURDOCH, D. C.: Contributions to noncommutative ideal theory. Canad. J. Math. **4**, 43—57 (1952). — [12] NORTHCOTT, D. G.: Ideal theory. Cambridge 1953. — [13] SMILEY, M. F.: Application of a radical of Brown und McCoy to nonassociative rings. Amer. J. Math. **72**, 93—100 (1950). — [14] WAERDEN, B. L. VAN DER: Moderne Algebra II, 2. Aufl. Berlin 1940. — [15] SCHMIDT, J.: Über die Rolle der transfiniten Schlußweisen in einer allgemeinen Idealtheorie. Math. Nachr. **7**, 165—182 (1952).

Frankfurt a. M., Mathematisches Seminar der Universität

(Eingegangen am 20. August 1954)

GAIER, D.
Math. Zeitschr. Bd. 64, S. 183—191 (1956)

Über die Äquivalenz der $|B_k|$-Verfahren

Von
DIETER GAIER

1. *Einleitung.* Vorgelegt sei eine Reihe

$$\sum a_n \tag{1}$$

mit beliebigen komplexen Gliedern[1]) und mit den Teilsummen s_n. Sie heißt B-summierbar zum Wert s, wenn die Transformation

$$B(x; s_\nu) = e^{-x} \sum \frac{s_n x^n}{n!}$$

für $x > 0$ existiert und gegen den Grenzwert s strebt für $x \to +\infty$; darüber hinaus heißt (1) sogar $|B|$-summierbar, wenn das Integral

$$\int_0^\infty \left| \frac{d}{dx} B(x; s_\nu) \right| dx < \infty$$

ist.

Es kann nun vorkommen, daß die Reihe (1) selbst nicht B-summierbar ($|B|$-summierbar) ist, wohl aber diejenige Reihe, die dadurch entsteht, daß man sämtliche Glieder von (1) um k Stellen nach rechts verschiebt und k Nullen vorschaltet; d.h. die Reihe

$$\underbrace{0 + 0 + 0 + \cdots + 0}_{k} + a_0 + a_1 + \cdots \tag{2}$$

kann B-summierbar ($|B|$-summierbar) sein. In diesem Falle sagt man dann, die Ausgangsreihe (1) sei B_k-summierbar ($|B_k|$-summierbar)[2]).

Diese B_k- und $|B_k|$-Verfahren werden mit wachsendem k stärker. In Verschärfung früherer Ergebnisse von GARTEN und KARAMATA wurde andererseits vor einiger Zeit nachgewiesen, daß sämtliche B_k-Verfahren in der Anwendung auf (1) äquivalent sind, sofern

$$a_n = O(K^n) \qquad (n \to \infty,\ K \text{ fest}) \tag{3}$$

gilt ([*4*], S. 453); diese Aussage wird falsch, wenn (3) durch die schwächere Forderung

$$a_n = O(K^n \cdot n^{\varepsilon n}) \qquad (n \to \infty,\ K \text{ fest},\ \varepsilon > 0) \tag{4}$$

---

[1]) Statt $\sum_{n=0}^{\infty} a_n$ schreiben wir stets $\sum a_n$.

[2]) Diese so definierten Summierungsverfahren sind ausführlich diskutiert z.B. in SANNIA ([*10*]) und KNOPP ([*7*] und [*8*]).

ersetzt wird [5]. Der Zweck dieser Note ist es, das folgende entsprechende Resultat für die $|B_k|$-Verfahren zu beweisen:

Satz 1. *Sämtliche* $|B_k|$-*Verfahren* ($k=0, 1, 2, \ldots$)[3]) *sind in der Anwendung auf* (1) *äquivalent, sofern* (3) *gilt; diese Aussage wird falsch, wenn* (3) *durch die schwächere Forderung* (4) *ersetzt wird.*

Als Hilfsmittel beim Beweis dienen, wie beim entsprechenden Fall der Äquivalenz der B_k-Verfahren, gewisse Sätze aus der Funktionentheorie und insbesondere aus der Theorie der ganzen Funktionen; diese sind auch unabhängig von der hier behandelten Fragestellung interessant und werden dem Beweis von Satz 1 (§ 3) in § 2 vorangestellt.

Der Verf. dankt den Herren K. KNOPP und K. ZELLER für Verbesserungsvorschläge zu der ursprünglichen Fassung der Arbeit.

2. *Hilfssätze über ganze Funktionen.* Die im Winkelraum $\alpha \leq \arg z \leq \beta$ reguläre Funktion heißt dort vom Exponentialtyp k, wenn

$$M(r) = O(e^{(k+\varepsilon)r}) \qquad (r \to \infty)$$

gilt für jedes $\varepsilon > 0$, aber für kein $\varepsilon < 0$; dabei ist $M(r)$ das Maximum von $|f(z)|$ auf dem Kreisbogen $|z| = r$, $\alpha \leq \arg z \leq \beta$. Zur genaueren Beschreibung des Wachstums von $|f(z)|$ längs Radien dient die Indikatorfunktion

$$h_f(\varphi) = \overline{\lim_{r\to\infty}} \frac{\log|f(r e^{i\varphi})|}{r} \qquad (\alpha \leq \varphi \leq \beta).$$

Hilfssatz 1 (A. J. MACINTYRE). *Für die in* $\Re(z) \geq 0$ *reguläre Funktion* $f(z)$ *vom Exponentialtyp* k *sei* $h_f(0) \leq 0$. *Dann gibt es zu jedem* $\varepsilon > 0$ *eine Zerlegung* $f(z) = f_1(z) + f_2(z)$ *in* $\Re(z) \geq 0$ *derart, daß gilt:*

a) $f_1(z)$ *ist eine ganze Funktion vom Exponentialtyp* $\leq k + \varepsilon$;

b) $f_1(x) = O\left(\frac{1}{|x|}\right)$ $(x \to -\infty)$;

c) $f_2(x) = O\left(\frac{1}{x}\right)$ $(x \to +\infty)$.

Dieser Hilfssatz findet sich implizit bei A. J. MACINTYRE ([9], S. 14—16); bei BOAS ([2], S. 80) fehlt die Aussage b), die aber a. a. O. (S. 181) benützt wird; bei HARVEY ([6], S. 196) wird behauptet, $f_1(z)$ sei vom Exponentialtyp k, was im allgemeinen nicht zutrifft[4]).

Da kein vollständiger Beweis von Hilfssatz 1 vorzuliegen scheint, wollen wir den bei BOAS ([2], S. 80—81) gegebenen ergänzen.

Beweis von Hilfssatz 1. Auf Grund der Voraussetzung $h_f(0) \leq 0$ existiert die LAPLACE-Transformierte $F(w)$ von $f(z)$ für $\Re(w) > 0$. Sie besitzt überdies, wie in [2], S. 78ff. näher ausgeführt ist, eine analytische Fortsetzung in das

[3]) Wegen des $|B_r| \to |B_s|$-Satzes ($s \geq r \geq 0$) (vgl. [8], S. 8) gilt Satz 1 für alle $|B_k|$-Verfahren ($k \geq 0$, reell).

[4]) Man nehme z.B. $f(z) = C \neq 0$. Wäre in diesem Fall die ganze Funktion $f_1(z)$ mit $f_1(x) = o(1)$ $(x \to -\infty)$ und $f_1(x) = f(x) - f_2(x) = C + o(1)$ $(x \to +\infty)$ vom Exponentialtyp $k = 0$, so wäre (z.B. [2], S. 83, Theorem 6.2.13) $f_1(z)$ eine Konstante, im Widerspruch zu ihrem Verhalten für $x \to \pm\infty$.

untengezeichnete schraffierte Gebiet und ist auf dem Weg $C = C_1 + C_2^{(1)} + C_2^{(2)}$ beschränkt. Mit ihrer Hilfe kann man dann

$$f(z) = \frac{1}{2\pi i}\int_C e^{zw} F(w)\,dw = f_1(z) + f_2^{(1)}(z) + f_2^{(2)}(z) \qquad \left(|\arg z| < \frac{\pi}{2}\right)$$

schreiben.

Wollen wir zunächst $f_1(z)$ näher betrachten, so zerlegen wir C_1 in seine drei Geradenstücke. Der Beitrag des Weges $w = \varepsilon + iv$ $(-k-\varepsilon \leq v \leq k+\varepsilon)$ gibt eine Funktion

$$\varphi_1(z) = \frac{1}{2\pi}\int_{-k-\varepsilon}^{+k+\varepsilon} e^{z\varepsilon}\cdot e^{izv}\cdot F(\varepsilon+iv)\,dv = \frac{e^{z\varepsilon}}{2\pi}\int_{-k-\varepsilon}^{+k+\varepsilon} e^{izv} F(\varepsilon+iv)\,dv.$$

Der zweite Faktor hierin ist eine ganze Funktion vom Exponentialtyp $\leq k+\varepsilon$, wie man sofort sieht, die überdies auf der reellen Achse beschränkt ist; also ist $\varphi_1(z)$ eine ganze Funktion vom Exponentialtyp $\leq k + 2\varepsilon$, für die $\varphi_1(x) = O(e^{-|x|\varepsilon})$ $(x \to -\infty)$ gilt. — Weiter gibt der Beitrag des Weges $w = i(k+\varepsilon) + u$ $(0 \leq u \leq \varepsilon)$ eine Funktion

$$\varphi_2(z) = \frac{e^{iz(k+\varepsilon)}}{2\pi i}\int_0^{\varepsilon} e^{uz} F(i(k+\varepsilon)+u)\,du,$$

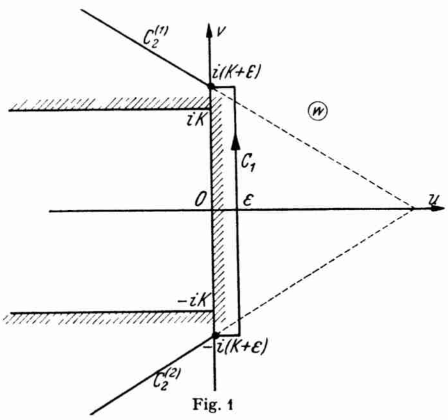

Fig. 1

was ebenfalls eine ganze Funktion vom Exponentialtyp $\leq k + 2\varepsilon$ ergibt. Die Abschätzung des Integrals führen wir nach partieller Integration aus. Man erhält für $z = -x$ $(x > 0)$

$$|\varphi_2(-x)| = O\left(\frac{1}{x}\right) \qquad (x \to +\infty).$$

Entsprechend behandelt man den Beitrag, der vom dritten Geradenstück herrührt, und erhält insgesamt in $f_1(z)$ eine ganze Funktion vom Exponentialtyp $\leq k+2\varepsilon$, mit $f_1(x) = O\left(\frac{1}{|x|}\right)$ $(x \to -\infty)$.

Daher ist $f_2^{(1)}(z) + f_2^{(2)}(z)$ in $\Re(z) \geq 0$ regulär, und eine einfache Abschätzung auf Grund der Beschränktheit von $F(w)$ auf C zeigt ferner (z.B. [2], S. 81) die Gültigkeit von $f_2^{(1)}(x) + f_2^{(2)}(x) = O\left(\frac{1}{x}\right)$ $(x \to +\infty)$. Damit ist Hilfssatz 1 bewiesen.

Hilfssatz 2. *Für die in $\Re(z) \geq 0$ reguläre Funktion $f(z)$ vom Exponentialtyp sei $\int_0^\infty |f(x)|^p\,dx < \infty$ $(p > 0)$. Dann ist auch $\int_0^\infty |f(x+iy)|^p\,dx < \infty$, gleichmäßig in jedem beschränkten Intervall $-a \leq y \leq +a$.*

Der erste Teil der Aussage ist bekannt ([2], S. 99), doch benötigen wir zum Beweis von Satz 2 weiter unten auch den zweiten Teil der Aussage von Hilfssatz 2.

Beweis von Hilfssatz 2. Wir betrachten zunächst alle y in $0 \leq y \leq a$. Wir haben $\lim_{x \to \infty} f(x) = 0$ ([2], S. 99), weshalb für die Funktion $g(z) = (z + i + 1)^{1/p} \cdot f(z)$ die Voraussetzungen von Hilfssatz 1 für ein gewisses k erfüllt sind $\left(\text{es ist ja } h_f(\varphi) = h_g(\varphi) \text{ in } -\frac{\pi}{2} \leq \varphi \leq +\frac{\pi}{2}\right)$. Zerlegt man $g(z)$ entsprechend der dortigen Aussage,

$$g(z) = (z + i + 1)^{1/p} \cdot f(z) = g_1(z) + g_2(z),$$

so sieht man sofort, daß in $\Re(z) \geq 0$

$$f(z) = f_1(z) + f_2(z)$$

gilt; dabei ist $f_1(z)$ in $\Im(z) \geq 0$ regulär, mit der Abschätzung $f_1(x) = O\left(|x|^{-1-\frac{1}{p}}\right)$ für $x \to -\infty$, während $f_2(z)$ in $\Re(z) \geq 0$ regulär ist, mit der Abschätzung $f_2(x) = O\left(x^{-1-\frac{1}{p}}\right)$ für $x \to +\infty$. Daraus folgt nun einerseits, daß $z^{1+\frac{1}{p}} \cdot f_2(z) = O(1)$ ist für $z = x \to +\infty$, also gleichmäßig im Halbstreifen $x \geq 0$, $0 \leq y \leq a$ (z.B. [2], S. 82); also ist für alle y in $\langle 0, a \rangle$

$$\int_0^\infty |f_2(x + iy)|^p \, dx \leq C \int_0^\infty \left(x^{-1-\frac{1}{p}}\right)^p dx \leq A_2, \tag{5}$$

d.h. speziell $f_2 \in L_p(0, \infty)$. Andererseits folgt daraus, zusammen mit der Voraussetzung $f \in L_p(0, \infty)$, daß auch $f_1 = f - f_2 \in L_p(0, \infty)$ ist $\big(L_p(0, \infty)$ ist ja ein linearer Raum für jedes $p > 0\big)$, also

$$\int_0^\infty |f_1(x)|^p \, dx < \infty.$$

Wegen $f_1(x) = O\left(|x|^{-1-\frac{1}{p}}\right)$ für $x \to -\infty$ ist aber auch $\int_{-\infty}^0 |f_1(x)|^p dx < \infty$, insgesamt also

$$\int_{-\infty}^{+\infty} |f_1(x)|^p \, dx < \infty.$$

Daraus folgt nun aber

$$\int_{-\infty}^{+\infty} |f_1(x + iy)|^p \, dx \leq e^{pk'y} \int_{-\infty}^{+\infty} |f_1(x)|^p \, dx \qquad (0 \leq y \leq a), \tag{6}$$

wenn k' den Typ von $f_1(z)$ in $\Im(z) \geq 0$ bezeichnet[5]). Insgesamt ist also $\int_0^\infty |f_s(x+iy)|^p dx \leq A_s$ $(s = 1, 2)$, also $\int_0^\infty |f(x+iy)|^p dx \leq A$ für y in $0 \leq y \leq a$. Entsprechend schließt man für die y in $-a \leq y \leq 0$, und Hilfssatz 2 ist bewiesen.

---

[5]) Die Ungleichung (6) findet sich ohne Beweis bei BOAS ([2], S. 98, Theorem 6.7.7), doch läßt sich der Beweis ganz in Analogie zum Beweis des dortigen Satzes 6.7.4 führen, indem man wieder die R. NEVANLINNAsche Darstellung einer in $\Im(z) > 0$ regulären Funktion bzw. deren Abschätzung durch ihre Werte auf der reellen Achse ([2], S. 93) heranzieht.

Hilfssatz 3. *Die Funktion $f(z)$ sei im abgeschlossenen Quadrat $\overline{Q}$ (Q: $|x|<1$, $|y|<1$; $z=x+iy$) mit dem Rand R regulär. Dann gibt es zu jedem $k=0, 1, 2, \ldots$ und $p>0$ Konstanten $A(k,p)$ derart, daß gilt*

$$|f^{(k)}(0)|^p \leq A(k,p) \int_R |f(z)|^p\,|dz|. \tag{7}$$

Beweis. Wir betrachten zunächst den Fall $k=0$. Ist $f(0)=0$, so ist nichts zu beweisen. Es sei daher $f(0)\neq 0$ und insbesondere $f(z)\not\equiv 0$, weshalb $f(z)$ nur endlich viele Nullstellen $z_1, z_2, \ldots, z_n$ in Q hat; sie seien ihrer Vielfachheit entsprechend aufgeführt. Nun bezeichne $w=g_r(z)$ eine konforme Abbildung von Q auf $|w|<1$ mit $g_r(z_r)=0$; $g_r(z)$ ist in Q regulär und hat genau eine Nullstelle in Q an der Stelle z_r. Daher ist die Funktion

$$F(z)=\frac{f(z)}{g_1(z)\cdot\cdots\cdot g_n(z)}$$

in Q regulär und nullstellenfrei. In $\overline{Q}$ ist diese Funktion stetig, da alle $g_r(z)$ in $\overline{Q}$ stetig und auf dem Rande $\neq 0$ sind. Daher gilt

$$\{F(0)\}^p=\frac{1}{2\pi i}\int_R \frac{\{F(z)\}^p\,dz}{z},$$

also

$$|f(0)|^p \leq |F(0)|^p \leq \frac{1}{2\pi}\int_R \frac{|F(z)|^p\,|dz|}{|z|}=\frac{1}{2\pi}\int_R \frac{|f(z)|^p\,|dz|}{|z|}\leq \frac{1}{2\pi}\int_R |f(z)|^p\,|dz|,$$

also gilt (7) im Falle $k=0$.

Für den Fall $k=1$ betrachten wir die Funktion $f_1(z)=\frac{f(z)-f(0)}{z}$. Die Voraussetzungen von Hilfssatz 3 sind erfüllt, und seine bereits bewiesene Gültigkeit im Falle $k=0$ liefert

$$\left\{\begin{aligned} |f_1(0)|^p=|f'(0)|^p &\leq A(0,p)\int_R \frac{|f(z)-f(0)|^p}{|z|^p}\,|dz| \\ &\leq A(0,p)\int_R [|f(z)|+|f(0)|]^p\,|dz|. \end{aligned}\right. \tag{8}$$

α) $0<p\leq 1$. Es gilt $[|f(z)|+|f(0)|]^p \leq |f(z)|^p+|f(0)|^p$, und somit folgt aus (8)

$$|f'(0)|^p \leq A(0,p)\Big\{\int_R |f(z)|^p\,|dz| + |f(0)|^p \int_R |dz|\Big\},$$

also zusammen mit (7) im Fall $k=0$

$$|f'(0)|^p \leq A(0,p)\,[1+8A(0,p)]\int_R |f(z)|^p\,|dz|.$$

β) $p\geq 1$. Die Minkowskische Ungleichung liefert dann

$$\Big\{\int_R [|f(z)|+|f(0)|]^p\,|dz|\Big\}^{1/p} \leq \Big\{\int_R |f(z)|^p\,|dz|\Big\}^{1/p}+\Big\{\int_R |f(0)|^p\,|dz|\Big\}^{1/p}.$$

Verwendet man zur Abschätzung des zweiten Terms wieder (7) im Fall $k=0$, addiert beide Terme und potenziert mit p, so folgt aus (8) sofort die Gültigkeit von (7) für $k=1$ auch für $p\geq 1$.

Ganz entsprechend verfährt man in den Fällen $k=2, 3, \ldots$; z.B. betrachtet man im Fall $k=2$ die Hilfsfunktion $f_2(z)=\frac{f(z)-f(0)-f'(0)z}{z^2}$ und wendet auf sie wieder die Ungleichung (7) für $k=0$ an. Damit ist Hilfssatz 3 bewiesen.

Wichtig für unsere Anwendung zur Äquivalenz der $|B_k|$-Verfahren ist nun der

Satz 2. *Für die in* $\Re(z)\geq 0$ *reguläre Funktion* $f(z)$ *vom Exponentialtyp sei* $\int\limits_0^\infty |f(x)|^p\,dx<\infty$ ($p>0$). *Dann ist auch* $\int\limits_0^\infty |f'(x)|^p\,dx<\infty$.

Zusatz 1. *Die Aussage von Satz 2 wird falsch für ganze Funktionen* $f(z)$ *der Ordnung* >1.

Beweis. Für ein $x_0>1$ seien die Wege C_1, C_2, C_3, C_4 wie folgt gewählt:

$$\left.\begin{array}{ll} C_1\colon x=x_0+1,\ -1\leq y\leq +1; & C_2\colon x_0+1\geq x\geq x_0-1,\ y=1;\\ C_3\colon x=x_0-1,\ +1\geq y\geq -1; & C_4\colon x_0-1\leq x\leq x_0+1,\ y=-1; \end{array}\right\}(z=x+iy),$$

ferner sei $C=C(x_0)=C_1+C_2+C_3+C_4$. Dann ist mit einer von x_0 unabhängigen Konstanten B

$$|f'(x_0)|^p\leq B\int\limits_{C(x_0)}|f(z)|^p\,|dz|=B\sum_{i=1}^{4}\int\limits_{C_i(x_0)}|f(z)|^p\,|dz|$$

(Hilfssatz 3). In der Abschätzung für $\int\limits_\alpha^\beta |f'(x_0)|^p\,dx_0$ $(1<\alpha<\beta<\infty)$ tritt daher einmal der Term

$$\int\limits_\alpha^\beta\int\limits_{-1}^{+1}|f(x_0+1+iy)|^p\,dy\,dx_0<\int\limits_{-1}^{+1}\int\limits_0^\infty|f(x+iy)|^p\,dx\,dy$$

auf, was unter einer von α,β unabhängigen Schranke bleibt (Hilfssatz 2). Andererseits rührt von $C_2(x_0)$ in der Abschätzung von $\int\limits_\alpha^\beta |f'(x_0)|^p\,dx_0$ der Term

$$\int\limits_\alpha^\beta\int\limits_{-1}^{+1}|f(x_0+t+i)|^p\,dt\,dx_0 \tag{9}$$

her. Setzen wir

$$\varphi_1(x)=\int\limits_0^x|f(t+i)|^p\,dt\qquad(x>0),$$

so wird dieser Ausdruck

$$\int\limits_\alpha^\beta[\varphi_1(x_0+1)-\varphi_1(x_0-1)]\,dx_0=\int\limits_{\beta-1}^{\beta+1}\varphi_1(t)\,dt-\int\limits_{\alpha-1}^{\alpha+1}\varphi_1(t)\,dt<2\varphi_1(\beta+1),$$

also bleibt auch (9) unter einer von α,β unabhängigen, endlichen Schranke. Entsprechend schließt man für die von den Wegteilen $C_3(x_0)$, $C_4(x_0)$ herrührenden Terme, und man hat insgesamt $\int\limits_0^\infty |f'(x)|^p\,dx<\infty$, womit Satz 2 bewiesen ist.

Auch der Zusatz 1 ist bewiesen, sobald wir gezeigt haben:

Zu jedem $p > 0$ und $\varepsilon > 0$ gibt es eine ganze Funktion $f(z)$ vom Normaltyp der Ordnung $1+\varepsilon$, für die $\int\limits_0^\infty |f(x)|^p \, dx < \infty$, aber $\int\limits_0^\infty |f'(x)|^p \, dx = \infty$ ist.

Wir wählen die Größen σ und δ mit $\sigma = 0, 1, 2, \ldots$ und $0 \leqq \delta < 1$ so, daß $\sigma + \delta > \frac{1}{p}$ und $\sigma + \delta \leqq \frac{1}{p} + \varepsilon$ ist, und definieren dann die beiden folgenden ganzen Funktionen $g_1(z)$, $g_2(z)$.

$g_1(z) = E_\alpha\left(z \cdot e^{i\frac{\pi\alpha}{2}}\right)\left(\alpha = \frac{1}{1+\varepsilon}\right)$, wobei $E_\alpha(t)$ die MITTAG-LEFFLERsche Funktion vom Normaltyp der Ordnung $\frac{1}{\alpha} = 1 + \varepsilon$ ist. Die Funktion $g_1(z)$ hat die Eigenschaften

$$g_1(x) = O(1) \qquad (x \to +\infty),$$
$$|g_1'(x)| = o(1) + \frac{x^\varepsilon}{\alpha^2} \qquad (x \to +\infty);$$

diese Eigenschaften lassen sich leicht aus einer Integraldarstellung für $E_\alpha(z)$ ableiten ([*1*], S. 272—275 und [*5*]).

$g_2(z)$ soll eine ganze Funktion vom Exponentialtyp sein, die für $x \to +\infty$ das Verhalten zeigt

$$g_2(x) = x^{-\delta} + O(x^{-1}) \qquad (x \to +\infty).$$

Für $\delta = 0$ nehme man einfach $g_2(z) = 1$, für $0 < \delta < 1$ folgt die Existenz von $g_2(z)$ aus einer Anwendung von Hilfssatz 1 auf die in $\Re(z) \geqq 0$ reguläre Funktion $(z+1)^{-\delta}$; man lege sie so fest, daß sie für $x > 0$ positiv werde.

Nun betrachten wir die ganze Funktion vom Normaltyp der Ordnung $1+\varepsilon$

$$f(z) = g_1(z) \cdot \left(\frac{\sin z}{z}\right)^\sigma \cdot g_2(z) = g_1(z) \cdot f_1(z).$$

Für sie gilt in $x \geqq 1$ die Abschätzung (K_i Konstanten)

$$|f(x)| \leqq K_1 \cdot x^{-\sigma} \cdot x^{-\delta}, \quad \text{also ist} \quad |f(x)|^p \leqq K_2 \cdot x^{-\sigma p - \delta p},$$

und auf Grund der Wahl $p(\sigma + \delta) > 1$ ist somit jedenfalls $\int\limits_0^\infty |f(x)|^p \, dx < \infty$.

Danach untersuchen wir die Ableitung $f'(z) = g_1(z) f_1'(z) + g_1'(z) f_1(z) = \varphi_1(z) + \varphi_2(z)$. Nach Konstruktion war $h(z) = z^{\sigma+\delta} \cdot f_1(z)$ eine in $\Re(z) > 0$ reguläre Funktion vom Exponentialtyp, die für $x \geqq 1$ beschränkt war. Also ist ([*2*], S. 82) $h(z)$ gleichmäßig beschränkt in jedem Halbstreifen $|y| \leqq a$, $x \geqq 1$, und eine einfache Anwendung der CAUCHYschen Formel zeigt die Beschränktheit von $h'(x)$ für $x \geqq 1$, d.h. $|f_1'(x)| \leqq K_3 \cdot x^{-\sigma-\delta}$ $(x \geqq 1)$ und somit $|\varphi_1(x)| \leqq K_4 \cdot x^{-\sigma-\delta}$ $(x \geqq 1)$; daher ist infolge unserer Wahl $p(\sigma+\delta) > 1$ die Funktion $\varphi_1(x) \in L_p(0, \infty)$.

Andererseits haben wir für $\varphi_2(x)$ eine Abschätzung nach unten:

$$|\varphi_2(x)| \geqq K_5 \cdot x^\varepsilon |\sin x|^\sigma \cdot x^{-\sigma-\delta} \, (x \geqq 1),$$

also ist

$$\int\limits_1^\infty |\varphi_2(x)|^p \, dx \geqq K_6 \cdot \int\limits_1^\infty |\sin x|^{p\sigma} \cdot x^{p(\varepsilon-\sigma-\delta)} \, dx = +\infty,$$

d.h. $\varphi_2(x) \notin L_p(0, \infty)$. Dann ist aber auch $f'(x) = \varphi_1(x) + \varphi_2(x) \notin L_p(0, \infty)$, also $\int\limits_0^\infty |f'(x)|^p \, dx = \infty$, und dies war zu zeigen.

3. *Äquivalenz der $|B_k|$-Verfahren.* Wir kommen nun auf unsere ursprüngliche Fragestellung zurück und wollen Satz 1 beweisen. Offensichtlich genügt es, aus der Existenz von $|B_1| - \sum a_n$ die Existenz von $|B| - \sum a_n$ zu erschließen, da ja das umgekehrte sicher richtig ist. Es sei also

$$b_0 + b_1 + b_2 + \cdots = 0 + a_0 + a_1 + \cdots; \qquad t_n = \sum_{\nu=0}^{n} b_\nu = s_{n-1},$$

und $|B| - \sum b_n$ existent, d.h.

$$\int\limits_0^\infty \left| \frac{d}{dx} B(x; t_\nu) \right| dx < \infty. \tag{10}$$

Auf Grund unserer Voraussetzung (3) gilt $|t_n| \leq M_1 n \cdot K^n \leq M_2 \cdot (K+1)^n$ für $n \geq 0$ und Konstanten M_2, K, also haben wir für die ganze Funktion $B(z; t_\nu)$ die Abschätzung

$$|B(z; t_\nu)| \leq e^{|z|} M_2 \cdot \sum \frac{(K+1)^n |z|^n}{n!} = M_2 \cdot e^{|z|(K+2)},$$

d.h. $B(z; t_\nu)$ und also auch $\frac{d}{dz} B(z; t_\nu)$ ist eine ganze Funktion vom Exponentialtyp. Setzen wir daher in Satz 2 $p = 1$ und berücksichtigen die Annahme (10), so folgt aus Satz 2

$$\int\limits_0^\infty \left| \frac{d^2}{dx^2} B(x; t_\nu) \right| dx < \infty. \tag{11}$$

Nun hängen aber $B(x; t_\nu)$ und $B(x; s_\nu)$ zusammen durch die Transformation

$$B(x; t_\nu) = e^{-x} \int\limits_0^x e^t B(t; s_\nu) \, dt, \tag{12}$$

und es ist

$$\frac{d}{dx} B(x; t_\nu) = B(x; s_\nu) - B(x; t_\nu),$$

also

$$\frac{d}{dx} B(x; s_\nu) = \frac{d^2}{dx^2} B(x; t_\nu) + \frac{d}{dx} B(x; t_\nu). \tag{13}$$

Diese Relation, zusammen mit (10) und (11), liefert sofort

$$\int\limits_0^\infty \left| \frac{d}{dx} B(x; s_\nu) \right| dx < \infty,$$

d.h. $|B| - \sum a_n$ existiert, falls (3) und (10) gelten.

Um zu sehen, daß aus der Existenz von $|B| - \sum b_n$ noch nicht die von $|B| - \sum a_n$ zu folgen braucht, falls nur (4) gilt, definieren wir die Folge $\{a_n\}$ durch die Relation

$$\sum \frac{t_n z^n}{n!} = e^z \int_0^z f(t)\, dt,$$

wobei $f(z)$ die im Beweis zu Zusatz 1 für die Zahlen $p = 1$ und $\frac{\varepsilon}{1-\varepsilon}$ konstruierte ganze Funktion vom Normaltyp der Ordnung $\frac{1}{1-\varepsilon}$ ist. Dann erfüllt $\{a_n\}$ die Voraussetzung (4), was etwa aus der Tatsache gefolgert werden kann, daß $\sum \frac{t_n z^n}{n!}$ eine ganze Funktion vom Normaltyp der Ordnung $\frac{1}{1-\varepsilon}$ ist, zusammen mit der Koeffizientenabschätzung für solche Funktionen ([*1*], S. 238). Weiter ist

$$\int_0^\infty \left| \frac{d}{dx} B(x; t_\nu) \right| dx < \infty,$$

d.h. $|B_1| - \sum a_n$ existiert; jedoch ist

$$\int_0^\infty \left| \frac{d^2}{dx^2} B(x; t_\nu) \right| dx = +\infty, \qquad \text{also} \qquad \int_0^\infty \left| \frac{d}{dx} B(x; s_\nu) \right| dx = +\infty,$$

wegen (13), d.h. $|B| - \sum a_n$ existiert nicht. Damit ist Satz 1 vollständig bewiesen.

Literatur

[*1*] Bieberbach, L.: Lehrbuch der Funktionentheorie, 2. Aufl., Bd. II. Leipzig 1931. — [*2*] Boas jr., R. P.: Entire Functions. New York 1954. — [*3*] Duffin, R. J., and A. C. Schaeffer: Power series with bounded coefficients. Amer. J. Math. **67**, 141 bis 154 (1945). — [*4*] Gaier, D.: Zur Frage der Indexverschiebung beim Borel-Verfahren. Math. Z. **58**, 453—455 (1953). — [*5*] Gaier, D.: On the change of index for summable series. Erscheint demnächst in Pacific J. Math. — [*6*] Harvey, A. R.: The mean of a function of exponential type. Amer. J. Math. **70**, 181—202 (1948). — [*7*] Knopp, K.: Bemerkung zum Borelschen Limitierungsverfahren. Rend. Circ. Mat. Palermo **54**, 331—334 (1930). — [*8*] Knopp, K.: Einige Bemerkungen zur A-, E_k- und B_k-Summierung. Rend. Circ. Mat. Palermo (2) **1**, 1—10 (1952). — [*9*] Macintyre, A. J.: Laplace's transformation and integral functions. Proc. London Math. Soc. (2) **45**, 1—20 (1938/39). — [*10*] Sannia, G.: Nuovo metodo di sommazione delle serie: Estensione del metodo di Borel. Rend. Circ. Mat. Palermo **42**, 303—322 (1917).

Stuttgart, Technische Hochschule, Mathematisches Institut A

(Eingegangen am 19. Juni 1955)

GROOT, J. DE
Math. Zeitschr. Bd. 64, S. 192—194 (1956)

A System of Continuous, Mutually Non-differentiable Functions

By

J. DE GROOT

The following problem was raised by MYCIELSKI: *does there exist a system —of potency of the continuum—of continuous, real valued functions such that any two different functions of the system—say $F(x)$ and $G(x)$—have no (finite or infinite) derivative with respect to each other?* I.e., for each x

$$\lim_{h\to 0} \frac{F(x+h)-F(x)}{G(x+h)-G(x)}$$

does not exist. One might expect that *the answer is positive*[1]). Indeed, we shall prove that among the system of functions

$$F(x) = \sum_{n=1}^{\infty} r_n f_n(x), \tag{1}$$

where the r_n are positive real numbers and $f_n(x)$ denotes the distance between x and the nearest number of the form $m/10^n$, where m is an integer, such systems occur.

More precisely, the following system $\{F_\alpha(x)\}$ $(0<\alpha<\frac{1}{2})$ satisfies the properties required:

$$F_\alpha(x) = \sum_{n=1}^{\infty} \delta_{\alpha,n} t_n f_{k_n}(x), \tag{2}$$

where

$$\delta_{\alpha,2n} = \varepsilon_{\alpha n}, \qquad \delta_{\alpha,2n-1} = 1-\varepsilon_{\alpha n} \qquad (n=1,2,3,\ldots), \tag{3}$$

$$1, \varepsilon_{\alpha 1}\varepsilon_{\alpha 2}\ldots\varepsilon_{\alpha n}\ldots = \sum_{\varkappa=0}^{\infty} 2^{2^{[\varkappa\alpha]}-2^{\varkappa^2}} \tag{4}$$

(the left hand side denotes the dyadic expansion of the corresponding real number in the right hand side for every α under consideration), and where t_n is a sequence of positive numbers with

$$t_n \geq 3\sum_{i=1}^{n-1} t_i \tag{5}$$

and k_n is a sequence of positive integers tending to infinity such that

$$t_n < 2^{k_n}. \tag{6}$$

[1]) J. MYCIELSKI gave a proof using the continuum hypothesis (in litt.).

The functions (1) are clearly related to well-known non-differentiable functions, defined in VAN DER WAERDEN [*1*] and KNOPP [*2*].

First we prove a lemma which itself is perhaps of some interest, since we give an effective proof of it and the system of sequences is given explicitly[2]).

LEMMA. *There exists a system of continuously many sequences*

$$a_1, a_2, a_3, \ldots, a_n, \ldots, \quad \textit{each} \quad a_i = 0 \quad \textit{or} \quad 1,$$

such that any two distinct sequences of the system have different elements on infinitely many corresponding places ($a_{\varkappa_i} \neq a'_{\varkappa_i}$ for an infinite number of indices $\varkappa_i$).

Proof. The *"von Neumann-numbers"* [*4*] in (4) form a system of continuously many algebraically independent numbers. The dyadic expansions of two such distinct numbers y_1 and y_2 differ in infinitely many places; otherwise $y_1 - y_2$ should be rational, in contradiction with the algebraical independency. So, the system of sequences denoted in (4) satisfies the property mentioned.

From this follows in particular that any two different sequences $\{\delta_{\alpha,n}\}$, $\{\ {}_{\alpha',n}\}$, defined by (3), have the stronger property

$$\begin{cases} \delta_{\alpha,n_i} = 0, & \delta_{\alpha',n_i} = 1 \qquad (i = 1, 2, \ldots), \\ \delta_{\alpha,m_i} = 1, & \delta_{\alpha',m_i} = 0 \qquad (i = 1, 2, \ldots), \end{cases} \tag{7}$$

for suitable sequences of positive integers n_i and m_i.

Using this result and exploiting the elegant proof in [*1*], due to A. HEYTING), we reach our goal as follows.

Each $F_\alpha(x)$ is continuous since the series (2) is uniformly convergent in view of (6).

Let x be a real number, expressed as a decimal. If the q-th figure is 4 or 9, let $x_q = x - 10^{-q}$; otherwise let $x_q = x + 10^{-q}$. Then it follows from the definition of $f_n(x)$, that

$$\begin{aligned} f_n(x_q) - f_n(x) &= \pm 10^{-q} \qquad (n < q) \\ &= 0 \qquad\qquad (n \geq q). \end{aligned}$$

Hence, assuming $\alpha \neq \alpha'$,

$$Q = \frac{F_\alpha(x_q) - F_\alpha(x)}{F_{\alpha'}(x_q) - F_{\alpha'}(x)} = \frac{\sum_{n=1}^{q-1} \pm \delta_{\alpha,n} t_n}{\sum_{n=1}^{q-1} \pm \delta_{\alpha',n} t_n}.$$

---

[2]) The lemma itself is contained in the following general set-theoretical theorem of C. KURATOWSKI [*3*], p. 330: given an infinite set S of potency m, there exists a family—of potency 2^m—of subsets $X, Y, \ldots$ of S, such that the potency of $X \setminus Y$ equals m for every pair of different sets X, Y.

If $q-1$ takes one of the values n_i we find for the quotient Q in view of (7) and (5)

$$|Q| \leq \left| \frac{\sum_{i=1}^{n_i-1} t_i}{2 \sum_{i=1}^{n_i-1} t_i} \right| = \frac{1}{2}.$$

If, on the other hand $q-1$ takes a value m_i, we find

$$|Q| \geq \left| \frac{2 \sum_{i=1}^{m_i-1} t_i}{\sum_{i=1}^{m_i-1} t_i} \right| = 2.$$

Hence, if $i \to \infty$, thus $x_{n_i}, x_{m_i} \to x$ the difference-quotient Q has no limit, finite or infinite and the proof is completed.

Remark. From our result follows easily, that each of the functions (2) is non-differentiable itself.

References

[1] WAERDEN, B. L. VAN DER: Ein einfaches Beispiel einer nicht-differenzierbaren stetigen Funktion. Math. Z. **32**, 474—475 (1930). — [2] KNOPP, K.: Ein einfaches Verfahren zur Bildung stetiger nirgends differenzierbaren Funktionen. Math. Z. **2**, 1—26 (1918). — [3] KURATOWSKI, C.: Topologie, vol. I. Warszawa 1952. — [4] NEUMANN, J. V.: Ein System algebraisch unabhängiger Zahlen. Math. Ann. **99**, 134—141 (1928).

Math. Inst. der Universität, Amsterdam C (Holland)

(Eingegangen am 23. September 1955)

WITT, E.
Math. Zeitschr. Bd. 64, S. 195—216 (1956)

Die Unterringe der freien Lieschen Ringe

Von
ERNST WITT

In Analogie zu dem von O. SCHREIER stammenden Satz, daß *jede Untergruppe einer freien Gruppe wieder frei ist,* soll hier der bereits von mir angekündigte Satz[1]) bewiesen werden, daß *jeder Unterring eines freien* LIE*schen Ringes wieder frei ist,* wobei ein Körper als Koeffizientenbereich vorausgesetzt wird. Diesen Satz habe ich 1938 im Anschluß an meine Untersuchungen über die assoziative Hülle LIEscher Ringe vermutet, aber erst 1940 beweisen können. Der Grundgedanke dieses Beweises ergibt sich durch Analogieübertragung bei geeigneter Auffassung des SCHREIERschen Beweises: Das von SCHREIER eingeführte Repräsentantensystem liefert bei Multiplikation mit Gruppenelementen eine monomiale Darstellung der Gruppe mit der besonderen Eigenschaft, daß die von 1 verschiedenen Koeffizienten der Darstellungsmatrizen der Erzeugenden der ganzen Gruppe ein freies Erzeugendensystem der Untergruppe bilden.

Für die von MAGNUS[2]) stammenden wichtigen gruppentheoretischen Anwendungen müssen ganze Zahlen als Koeffizienten genommen werden. In diesem Fall gilt nun der obige Satz nicht mehr uneingeschränkt, wie schon ganz einfache Beispiele zeigen, jedoch läßt er sich für viele gruppentheoretisch wichtige Unterringe beweisen.

Es sei gestattet, hier die Theorie von MAGNUS in kurzen Zügen darzulegen. $\mathfrak{G}$ sei eine beliebige (auch nichtkommutative) additiv geschriebene Gruppe. Mit den Bezeichnungen

(1) $$ab = a + b - a - b$$

(2) $$a^b = b + a - b$$

lassen sich die von PH. HALL stammenden Regeln

(3) $$ab + ba = 0, \qquad aa = 0$$

(4) $$a(b + b') = ab + ab' + (b'a)\, b$$

(5) $$(ab)\, c^b + (bc)\, a^c + (ca)\, b^a = 0$$

approximativ als Regeln eines LIEschen Ringes deuten[3]).

[1]) WITT, E.: Über freie Ringe und ihre Unterringe. Math. Z. **58**, 113—114 (1953). — Nach Fertigstellung der vorliegenden Arbeit erfuhr ich durch Herrn LAZARD, daß ŠIRŠOV diesen Satz inzwischen unabhängig bewiesen hat. ŠIRŠOV, A. I.: Unteralgebren freier LIEscher Algebren. [Russisch.] Mat. Sbornik (2) **33**, 441—452 (1953). Diese Arbeit war mir bisher nicht zugänglich.

[2]) MAGNUS, W.: Über Beziehungen zwischen höheren Kommutatoren. J. reine u. angew. Math. **177**, 105—115 (1937). Ein ausgedehntes Literaturverzeichnis findet sich bei M. LAZARD: Sur les groupes nilpotents et les anneaux de LIE. Ann. sci. Ecole norm. sup. (III. S r.) **71**, 101—190 (1954).

[3]) Durch Ausdrücken von $a(b+c) + b(c+a) + c(a+b) = 0$ nach (4) bekommt man eine neungliedrige Identität, welche genau dieselben Dienste wie (5) leistet. Es gilt übrigens allgemein bei zyklischer Vertauschung $a_1(a_2 + \cdots + a_n) + \cdots = 0$.

$\mathfrak{A}+\mathfrak{B}$ und $\mathfrak{A}\mathfrak{B}$ bezeichne nun die von allen Elementen a, b bzw. allen Kommutatoren $a b$ erzeugte Untergruppe ($a \in \mathfrak{A}, b \in \mathfrak{B}$). Mit $\mathfrak{A}$ und $\mathfrak{B}$ sind auch $\mathfrak{A}+\mathfrak{B}$ und $\mathfrak{A}\mathfrak{B}$ Normalteiler von $\mathfrak{G}$. Nach (5) gilt für Normalteiler

$$(8) \qquad (\mathfrak{A}\mathfrak{B})\mathfrak{C} \leqq (\mathfrak{B}\mathfrak{C})\mathfrak{A} + (\mathfrak{C}\mathfrak{A})\mathfrak{B} \qquad \text{(Ph. Hall)}.$$

Für die charakteristischen Normalteiler $\mathfrak{G}^n$ der absteigenden Zentralreihe, die induktiv durch $\mathfrak{G}^n = \mathfrak{G}^{n-1}\mathfrak{G}$, $\mathfrak{G}^1 = \mathfrak{G}$ erklärt sind, gilt dann

$$(9) \qquad \mathfrak{G}^i \mathfrak{G}^k \leqq \mathfrak{G}^{i+k} \qquad \text{(Ph. Hall)},$$

wie sich nach (8) bei beliebigem k durch Induktion nach i ergibt:

$$\mathfrak{G}^i\mathfrak{G}^k = (\mathfrak{G}^{i-1}\mathfrak{G})\mathfrak{G}^k \leqq (\mathfrak{G}\mathfrak{G}^k)\mathfrak{G}^{i-1} + (\mathfrak{G}^k\mathfrak{G}^{i-1})\mathfrak{G}$$
$$\leqq \mathfrak{G}^{k+1}\mathfrak{G}^{i-1} + \mathfrak{G}^{k+i-1}\mathfrak{G} \leqq \mathfrak{G}^{i+k}.$$

Für $a \in \mathfrak{G}^\alpha$, $b, b' \in \mathfrak{G}^\beta$, $c \in \mathfrak{G}^\gamma$ gelten dann nach (9)

$$(1') \qquad a + b \leqq b + a + \mathfrak{G}^{\alpha+\beta}$$

$$(3) \qquad ab + ba = 0, \qquad aa = 0,$$

$$(4') \qquad a(b+b') \leqq ab + ab' + \mathfrak{G}^{\alpha+\beta+1},$$

$$(4'') \qquad a(b + \mathfrak{G}^{\beta+1}) \leqq ab + \mathfrak{G}^{\alpha+\beta+1},$$

$$(5') \qquad a(bc) + b(ca) + c(ab) \leqq \mathfrak{G}^{\alpha+\beta+\gamma+1},$$

wobei die Glieder $\mathfrak{G}^n$ die Abweichungen von den genauen Regeln eines LIEschen Ringes angeben.

Für eine Menge X von Unbestimmten sei nun

$\mathfrak{L}$ der von X erzeugte freie LIEsche Ring,

$\mathfrak{G}$ die von X erzeugte freie Gruppe,

$\mathfrak{A}$ der von X erzeugte freie assoziative Ring mit Einselement.

$\mathfrak{L}_{(n)}$, $\mathfrak{A}_{(n)}$ mögen die entsprechenden homogenen Moduln n-ten Grades bezeichnen. Nach den erwähnten approximativen Regeln haben Elemente von $\mathfrak{L}_{(n)}$ in gleicher Schreibweise auch in $\mathfrak{G}^n/\mathfrak{G}^{n+1}$ einen Sinn, und dabei entsteht eine homomorphe Abbildung φ_n von $\mathfrak{L}_{(n)}$ auf $\mathfrak{G}^n/\mathfrak{G}^{n+1}$. *Es gilt nun die wichtige Tatsache, daß φ_n ein Isomorphismus ist, wodurch jeder Satz über freie* LIE*sche Ringe unmittelbar eine Bedeutung für freie Gruppen hat.* Zum Nachweis dessen wird eine Abbildung ψ_n von $\mathfrak{G}^n/\mathfrak{G}^{n+1}$ in $\mathfrak{A}_{(n)}$ angegeben, für welche die zusammengesetzte Abbildung $\psi_n\varphi_n$ gerade Bestandteil der kanonischen Abbildung von $\mathfrak{L}_{(n)}$ in $\mathfrak{A}_{(n)}$ bedeutet, die Produkte von $\mathfrak{L}$ in Kommutatoren von $\mathfrak{A}$ überführt und die nach BIRKHOFF-MAGNUS-WITT[4]) eine

[4]) BIRKHOFF, G.: Representability of Lie algebras and Lie groups by matrices. Ann. of Math. (2) **38**, 526—532 (1937). — MAGNUS, W.[2]), u. E. WITT: Treue Darstellung LIEscher Ringe. J. reine u. angew. Math. **177**, 152—160 (1937).

isomorphe Abbildung ist. Hierzu werden unendliche Reihen

$$a = 1 + a_1 + a_2 + \cdots \qquad (a_n \in \mathfrak{A}_{(n)})$$

betrachtet, die bei formaler Multiplikation eine von MAGNUS eingeführte Gruppe $\mathfrak{M}$ bilden. Für die Reihen

$$a = 1 + a_i + \cdots, \qquad a' = 1 + a_i' + \cdots, \qquad b = 1 + b_k + \cdots$$

ergibt sich

$$a\,a' = 1 + (a_i + a_i') + \cdots \quad \text{und} \quad a\,b\,a^{-1}\,b^{-1} = 1 + (a_i\,b_k - b_k\,a_i) + \cdots,$$

wobei jeweils Glieder höheren Grades fortgelassen sind. Vermöge

$$\psi(x) = 1 + x \qquad (x \in X)$$

wird nun eine homomorphe Abbildung ψ von $\mathfrak{G}$ in $\mathfrak{M}$ erzeugt, für welche sich mit $g \in \mathfrak{G}^n$

$$\psi(g) = 1 + \psi_n(g) + \cdots \qquad (\psi_n(g) \in \mathfrak{A}_{(n)})$$

die gewünschte Abbildung ψ_n von $\mathfrak{G}^n/\mathfrak{G}^{n+1}$ in $\mathfrak{A}_{(n)}$ ergibt.

Diese Theorie von MAGNUS bleibt auch dann noch gültig, wenn der darin eingehende Begriff des graduierten Ringes in folgender Weise verallgemeinert wird:

Zugrunde gelegt sei (wie in § 2, 2) eine feste Abbildung $x \to |x| > 1$ $(x \in X)$ in den **wohlgeordneten**[5]) kommutativen Kegel $\mathfrak{S}$ einer geordneten Gruppe. $\mathfrak{L}_{(s)}$ bzw. $\mathfrak{A}_{(s)}$ seien die homogenen Bestandteile vom „Grade" s, dabei sei $\mathfrak{L}$ und $\mathfrak{A}$ direkte Summe der $\mathfrak{L}_{(s)}$ bzw. $\mathfrak{A}_{(s)}$.

Die im Sinne von § 1 formalen Reihen $\sum a_s\, s$ mit $a_1 = 1$, $a_s \in \mathfrak{A}_{(s)}$ bilden dann wieder eine multiplikative Gruppe $\mathfrak{M}$. Indem man wieder die Elemente von $\mathfrak{L}$ unter Beibehaltung der Schreibweise als Elemente von $\mathfrak{G}$ auffaßt, seien $\mathfrak{G}_s$ und $\mathfrak{H}_s$ die von $\bigcup_{t \geq s} \mathfrak{L}_{(t)}$ bzw. $\bigcup_{t > s} \mathfrak{L}_{(t)}$ in $\mathfrak{G}$ erzeugten Untergruppen. Die Zuordnung

$$\mathfrak{L}_{(n)} \to \mathfrak{G}^n/\mathfrak{G}^{n+1} \to \mathfrak{A}_{(n)} \quad \text{mit} \quad \psi(x) = 1 + x$$

der ursprünglichen Theorie braucht man jetzt nur noch zu ersetzen durch

$$\mathfrak{L}_{(s)} \to \mathfrak{G}_s/\mathfrak{H}_s \to \mathfrak{A}_{(s)} \quad \text{mit} \quad \psi(x) = 1 + x \cdot |x|.$$

Dieser allgemeinere Begriff des graduierten Ringes bietet auch sonst wesentliche Vorteile. Zum Beispiel überträgt sich die in § 3 hiermit formulierte Voraussetzung IV über freie LIEsche Ringe $\mathfrak{L}$ auf alle homogenen Unterringe $\mathfrak{U}$ mit torsionslosem Faktormodul $\mathfrak{L}/\mathfrak{U}$ (Satz 5), während bei dem üblichen Grundbegriff diese Voraussetzung einfach bedeutet, daß $\mathfrak{L}$ nur endlich viele Erzeugende hat, eine Eigenschaft, die sich gewiß nicht immer auf $\mathfrak{U}$ überträgt.

Das in § 1 eingeführte Hilfsmittel der formalen Konvergenz erlaubt die Aufstellung einer einfachen Beziehung zwischen den Rangzahlen von $\mathfrak{L}_{(s)}$ und $\mathfrak{A}_{(s)}$ (Satz 6), die ihrerseits wieder Grundlage für weitere Schlüsse darstellt und zu einem Kriterium für freie Unterringe führt.

[5]) Unter **Wohlordnung** wird hier stets eine Ordnung mit Minimalbedingung verstanden.

Die Theorien von MAGNUS und BIRKHOFF-WITT gelten sinngemäß auch bei sog. p-LIEschem Ring $\mathfrak{L}$ (auch eingeschränkter LIEscher Ring genannt) für Primzahlcharakteristik p, bei dem außer den LIEschen Verknüpfungen noch eine Operation $x \to x^p$ erklärt ist mit den Bedingungen

$$\left.\begin{aligned} x^p \circ y &= x \circ (x \circ (\ldots (x \circ y))) \\ (x+y)^p &= x^p + y^p + \Lambda(x, y) \end{aligned}\right\} \quad (p \text{ Faktoren } x)$$

mit einem in naheliegender Weise bestimmten LIEschen Polynom $\Lambda(x, y)$. Wie im gewöhnlichen Fall hat auch $\mathfrak{L}$ wieder eine assoziative Hülle $\tilde{\mathfrak{L}}$, in der dann $x^p = x x \ldots x$ (p Faktoren) gilt. Mit Hilfe der oben erwähnten Isomorphismen ψ_n lassen sich nach MAGNUS mühelos zwei weitere Regeln von HALL herleiten:

$$\left.\begin{aligned} &(6p) \qquad (p\,a)\,b \in a(a(\ldots b)) + p\,\mathfrak{G}^2 \\ &(7p) \qquad p(a+a') \in p\,a + p\,a' + \mathfrak{G}^p + p\,\mathfrak{G}^2 \end{aligned}\right\} \quad (p \text{ Faktoren } a),$$

worin $\mathfrak{G}^2$, $\mathfrak{G}^p$ der oben erklärten absteigenden Zentralreihe von $\mathfrak{G}$ angehören und allgemein $p\,\mathfrak{C}$ die von allen pc erzeugte Untergruppe bedeute ($c \in \mathfrak{C}$). Zusammen mit (3), (4), (5) dienen diese Regeln zur Herleitung des Analogons der Theorie von MAGNUS für den p-Fall. Dabei ist natürlich die bisherige absteigende Zentralreihe durch die „absteigende p-Zentralreihe" zu ersetzen, nämlich durch die schwächste Folge $\mathfrak{G}_i$ mit

$$\mathfrak{G}_i\,\mathfrak{G}_k \subseteqq \mathfrak{G}_{i+k}, \qquad p\,\mathfrak{G}_i \subseteqq \mathfrak{G}_{pi}, \qquad \mathfrak{G}_1 = \mathfrak{G}.$$

Auch die im folgenden dargestellte Theorie der Erzeugung von Unterringen eines LIEschen Ringes läßt sich sinngemäß auf p-LIEsche Ringe übertragen. Änderungen, die sich bei Betrachtung *dieses p-Falles* ergeben, werden an den betreffenden Stellen ohne nähere Begründung angemerkt; die Formelnummern sind dann mit Index p versehen.

In § 4 werden gewisse minimale Basen eines freien LIEschen Ringes konstruiert. Eine Basis dieser Art habe ich 1942 angegeben[6]), eine andere fand M. HALL 1950[7]).

Am Schluß der Arbeit zeigen einige Beispiele, daß bei geeignetem Koeffizientenbereich nicht jeder Unterring eines freien LIEschen Ringes frei erzeugbar ist.

§ 1. Formale Konvergenz

In einer geordneten Gruppe (in der also aus $x \leq y$, $x' \leq y'$ auch $x x' \leq y y'$ folgt) sei $\mathfrak{S}$ der **Kegel** aller Elemente $s \geqq 1$. Mit einem assoziativen

[6]) Vortrag an der Universität Berlin. Hauptgegenstand war der hier dargestellte Beweis des Hauptsatzes. In einem 1944 an der Universität Göttingen gehaltenen Vortrag bewies ich den für gruppentheoretische Anwendungen wichtigen Satz 5. Die in der vorliegenden Arbeit dargestellte Theorie bis einschließlich Satz 9 war der Inhalt einer Vortragsreihe, die ich im Herbst 1953 auf Einladung der Universität Barcelona hielt.

[7]) MARSHALL HALL jr.: A basis for free Lie rings and higher commutators in free groups. Proc. Amer. Math. Soc. 1, 575—581 (1950).

Koeffizientenring P mit Einselement sei dann $\mathfrak{R}$ der Ring derjenigen formalen Summen

$$a = \sum \alpha_s s \qquad (s \in \mathfrak{S},\ \alpha_s \in \mathsf{P}),$$

bei dem zu jedem t für fast alle $s \leqq t$ $\alpha_s = 0$ ist (d.h. bis auf endlich viele Ausnahmen). Die Multiplikation in $\mathfrak{R}$ sei erklärt durch

$$a\,b = \sum \alpha_s s \cdot \sum \beta_{s'} s' = \sum_{ss'=t} (\sum \alpha_s \beta_{s'})\, t.$$

$\mathfrak{R}_t$ bezeichne das Ideal aller $a \in \mathfrak{R}$ mit $\alpha_s = 0$ für alle $s \leqq t$.

In $\mathfrak{R}$ werde nun eine Topologie eingeführt, indem der von den Idealen $\mathfrak{R}_t$ erzeugte Filter als Umgebungsfilter der 0 gewählt wird. Diese Topologie werde die *Topologie der formalen Konvergenz* genannt. Der so erklärte topologische Ring $\mathfrak{R}$ ist *Hausdorffsch* wegen $\bigcap_t \mathfrak{R}_t = 0$. Ferner ist er *vollständig*, denn in einem CAUCHY-Filter gehören die Approximationsmengen der Feinheit $\mathfrak{R}_t$ sämtlich derselben Restklasse $\sum_{s \leqq t} \alpha_s s \bmod \mathfrak{R}_t$ an. Sie geben also Anlaß zur Konstruktion eines Limeselementes $\sum \alpha_s s$ aus $\mathfrak{R}$, weil die Koeffizienten α_s eines Elementes a aus $\mathfrak{R}$ für $s \leqq t$ bereits durch $a \bmod \mathfrak{R}_t$ bestimmt sind. — $\mathfrak{R}_t$ läßt sich übrigens charakterisieren als abgeschlossenes Ideal in $\mathfrak{R}$, das möglichst viele Elemente aus $\mathfrak{S}$, aber nicht t enthält.

In diesem Ring $\mathfrak{R}$ gelten folgende einfache Regeln über Summierbarkeit und Multiplizierbarkeit:

1. $A = \sum \pm a_i$ ist genau dann summierbar (i aus einer Menge I),

$B = \prod (1 + a_i)$ ist genau dann multiplizierbar (i aus einer Kette I, d.h. I total geordnet),

$C = \sum^{(<)} a_{i_1} \ldots a_{i_n}$ ist genau dann summierbar (n variabel $\geqq 0$; $i_1 < \cdots < i_n$ aus einer Kette I),

wenn für jedes t nur endlich viele $a_i \not\equiv 0 \bmod \mathfrak{R}_t$ sind, und in diesem Falle ist $B = C$.

2. Sind $\sum a_i$ und $\sum b_k$ (i aus Menge I, k aus Menge K) summierbar, so gilt

$$(\sum a_i)\,(\sum b_k) = \sum a_i b_k$$

mit summierbarer rechter Seite. Entsprechendes gilt auch für endlich viele Faktoren.

3. $\mathfrak{R}$ besteht genau aus den Werten der summierbaren Summen $\sum \alpha_s s$, unter denen also die endlichen Summen einen dichten Teilring von $\mathfrak{R}$ bilden.

Im folgenden sei $\mathfrak{S}$ **wohlgeordnet**[5]), d.h. jede nicht leere Teilmenge von $\mathfrak{S}$ enthalte mindestens ein minimales Element (*Minimalbedingung*). $\mathfrak{R}_1$ bezeichnet das Ideal der Summen $\sum \alpha_s s$ mit $s > 1$. Ferner sei $\mathfrak{a}_n$ die Menge aller Produkte aus n Faktoren, die einer Menge $\mathfrak{a}$ entnommen sind.

Hilfssatz. *Für jede endliche Teilmenge* $\mathfrak{a} \in \mathfrak{R}_1$ *gilt* $\lim_{n \to \infty} \mathfrak{a}_n = 0$.

Hiernach sind Potenzreihen $\sum a_i z^i$ mit $z \in \mathfrak{R}_1$ stets summierbar.

Beweis. Für vorgelegtes t kommen in den formalen Reihenentwicklungen $\sum \alpha_s s$ der endlich vielen $a \in \mathfrak{a}$ insgesamt nur endlich viele s mit $1 < s \leq t$ wirklich vor. Für jedes dieser s sei $t\, s^{-m_s}$ das kleinste in $\mathfrak{S}$ liegende Element der Kette $t > t\, s^{-1} > t\, s^{-2} > \cdots$. Dann ist $\mathfrak{a}_n \subseteqq \mathfrak{R}_t$ für alle $n > \sum m_s$; denn angenommen, beim Ausrechnen von $a_1 \ldots a_n \in \mathfrak{a}_n$ käme wirklich ein Monom $s_1 \ldots s_n \leq t$ vor, so erhielte man, da einer seiner Faktoren s mehr als m_s mal auftritt, $s^{m_s+1} \leq s_1 \ldots s_n \leq t$, im Widerspruch zur Definition von m_s.

Satz 1. *Aus der Summierbarkeit von* $A = \sum a_i$ $(i \in I)$ *mit* $a_i \in \mathfrak{R}_1$ *folgt im Sinne der Summierbarkeit bzw. Multiplizierbarkeit*

$$(1-A)^{-1} = \sum_{n=0}^{\infty} A^n = \sum a_{i_1} \ldots a_{i_n} \qquad (n \text{ variabel } \geqq 0;\ i_\nu \text{ aus Menge } I)$$

$$\left(\prod (1-a_i)\right)^{-1} = \prod (1-a_i)^{-1} = \sum^{(\leq)} a_{i_1} \ldots a_{i_n}$$
$$(n \text{ variabel};\ i_1 \leq \cdots \leq i_n \text{ aus Kette } I)$$

und umgekehrt.

Beweis. $\mathfrak{a}$ sei die endliche Menge der $a_i \not\equiv 0 \bmod \mathfrak{R}_t$. Nach dem Hilfssatz ist für genügend großes n $\mathfrak{a}_n \subseteqq \mathfrak{R}_t$. Das besagt die Summierbarkeit der Summe rechts oben, woraus man die der anderen Summen durch Zusammenfassen oder Weglassen erhält. Die Gleichungen des Satzes brauchen nur mod $\mathfrak{R}_t$ bewiesen zu werden und sind dann selbstverständlich. —

Unter formalen Summen und Produkten seien immer die hier behandelten summierbaren Summen und multiplizierbaren Produkte verstanden.

Wenn der Koeffizientenring P alle rationalen Zahlen enthält, so hat man die üblichen Beziehungen zwischen den Potenzreihen e^z, $\log(1+z)$, $(1+z)^a$ für $z \in \mathfrak{R}_1$, $a \in \mathfrak{R}$ unter der Voraussetzung $az = za$.

Beim Studium der *freien* LIE*schen Ringe* kommt man bei *vertauschbarem* $\mathfrak{S}$ und rationalem Körper P auf formale Identitäten der Gestalt

$$(1) \qquad 1 - \sum_s \varepsilon_s s = \prod_s (1-s)^{\beta_s} \qquad (s > 1 \text{ aus } \mathfrak{S};\ \varepsilon_s, \beta_s \in \mathsf{P}),$$

durch welche die ε_s *von den* β_s *und umgekehrt „rekursiv" abhängen.* Dabei sind mit den β_s auch die ε_s ganze Zahlen und umgekehrt. In den Anwendungen sind die ε_s und β_s natürliche Zahlen (Ränge).

Der negative Logarithmus von (1) ist

$$(2) \qquad \sum_h h^{-1} \Big(\sum_s \varepsilon_s s\Big)^h = \sum_{s,d} \beta_s d^{-1} s^d \qquad (h, d = 1, 2, \ldots).$$

Vergleich der Koeffizienten γ_t von t liefert

$$(3) \qquad \gamma_t = \sum_{\substack{h, t_\nu \\ \Pi t_\nu = t}} h^{-1} \varepsilon_{t_1} \ldots \varepsilon_{t_h} = \sum_{\substack{d, s \\ s^d = t}} d^{-1} \beta_s.$$

In $\mathfrak{S}$ heiße eine zyklische Halbgruppe $\{t_0^n\}$ $(n \geqq 0)$ **rein abgeschlossen,** wenn aus $s^d \in \{t_0^n\}$, $d \geqq 1$, immer $s \in \{t_0^n\}$ folgt. Nach (3) gilt in diesem Fall

$$(4) \qquad n\,\gamma(t_0^n) = \sum_{d|n} \frac{n}{d} \beta(t_0^{n/d}) \qquad (\gamma(s) = \gamma_s \text{ usw.}).$$

Durch MOEBIUSsche Umkehrung ergibt das

(5) $$\beta(t_0^n) = \sum_{d|n} \frac{\mu(d)}{d} \gamma(t_0^{n/d}),$$

und das ist nach (3) explizit durch die ε_s ausdrückbar.

Hat $\mathfrak{S}$ *unabhängige vertauschbare Erzeugende* s_i, so liegt jedes Element t in einer rein abgeschlossenen zyklischen Halbgruppe. Man findet so für $t = t_0^n$

(6) $$\beta_t = \sum \frac{\mu(d)}{h\,d} \varepsilon_{t_1} \ldots \varepsilon_{t_h},$$

summiert über alle Lösungen von $\prod t_\nu^d = t$. Sind nur für die Erzeugenden s_i die $\varepsilon_{s_i} \neq 0$, so ist

(7) $$\beta(s_1^{n_1} \ldots s_r^{n_r}) = \frac{1}{n} \sum_{d|n_i} \frac{\mu(d) \frac{n}{d}!}{\frac{n_1}{d}! \ldots \frac{n_r}{d}!} \varepsilon_{s_1}^{n_1/d} \ldots \varepsilon_{s_r}^{n_r/d} \qquad (n = \sum n_i)$$

und insbesondere

(8) $$\beta(s_1^n) = \frac{1}{n} \sum_{d|n} \mu(d)\, \varepsilon_{s_1}^{n/d}.$$

Für p-LIE-*Ringe* lauten die entsprechenden Formeln:

(1 p) $$1 - \sum_s \varepsilon_s s = \prod_s \left(\frac{1-s}{1-s^p}\right)^{\beta_s} \qquad (s > 1 \text{ aus } \mathfrak{S};\ \varepsilon_s, \beta_s \in \mathrm{P}),$$

(2 p) $$\sum_h h^{-1} \Big(\sum_s \varepsilon_s s\Big)^h = \sum_{s,d} \beta_s d^{-1} (s^d - s^{pd}) \qquad (h, d = 1, 2, \ldots),$$

(3 p) $$\gamma_t = \sum_{\substack{h, t_\nu \\ \Pi t_\nu = t}} h^{-1} \varepsilon_{t_1} \ldots \varepsilon_{t_h} = \sum_{\substack{d, s \\ s^d = t}} d^{-1} \beta_s - \sum_{\substack{d, s \\ s^{pd} = t}} d^{-1} \beta_s,$$

(4 p) $$n\gamma(t_0^n) = \sum_{d|n} \frac{n}{d} \beta(t_0^{n/d}) - \sum_{pd|n} \frac{n}{d} \beta(t_0^{n/pd}).$$

Die übrigen Formeln (5 p), ..., (8 p) *erhält man durch die Ersetzung*

$$\mu(d) \to \mu_p(d) = \mu(d_0)\, \varphi(p^h) \qquad (d = d_0 p^h,\ p \nmid d_0).$$

φ ist hierbei die EULERsche Funktion. — Der Schluß (4 p) $\Rightarrow$ (5 p) läßt sich durch eine etwas umständliche Induktion führen.

§ 2. Relationen für Erzeugende eines Lieschen Ringes und eines Unterringes

1. $\mathfrak{L}$ sei ein LIEscher Ring, in dem die Multiplikation mit $a \circ b$ bezeichnet werde, und $\mathfrak{U}$ ein Unterring von $\mathfrak{L}$, beide mit einem kommutativen Koeffizientenring Γ mit Einselement. Dabei sei $\mathfrak{L}$ durch eine Menge X von Erzeugenden x mit gewissen Relationen gegeben. *Unter gewissen einschränkenden Voraussetzungen I und II, die jedenfalls erfüllbar sind, wenn Γ ein Körper ist, soll für eine geeignete Erzeugung Y von $\mathfrak{U}$ ein System definierender Relationen angegeben werden.*

2. Bei fester Abbildung $x \to |x| > 1$ in den *wohlgeordneten*[5]) *kommutativen Kegel* $\mathfrak{S}$ einer geordneten Gruppe bezeichne $\mathfrak{L}_s$ bzw. $\mathfrak{L}_{(s)}$ den von allen Lieschen Produkten

$$x_1 \circ \cdots \circ x_n \quad \text{(beliebige Klammerung, Faktorenzahl } \geq 1,\ x_\nu \in X)$$

mit $|x_1| \ldots |x_n| \leq s$ bzw. mit $|x_1| \ldots |x_n| = s$ aufgespannten Γ-Modul. Es ist

$$\mathfrak{L}_s \circ \mathfrak{L}_t \subseteqq \mathfrak{L}_{st}, \quad \mathfrak{L}_{(s)} \circ \mathfrak{L}_{(t)} \subseteqq \mathfrak{L}_{(st)}.$$

Für den homogenen Fall, daß $\mathfrak{L}$ direkte Summe aller $\mathfrak{L}_{(s)}$ ist, definieren wir für später: Die Elemente und Untermoduln von $\mathfrak{L}_{(s)}$ heißen homogen vom Betrag s. Ein Unterring von $\mathfrak{L}$ heißt *homogen*, wenn er *direkte* Summe homogener Moduln beliebiger Beträge ist (ein homogener Unterring braucht also kein homogener Modul zu sein). So ist z.B. $\mathfrak{L}$ selbst ein homogener Ring, wenn seine Erzeugung X frei ist. Analog wird eine Basis *homogen* genannt, wenn sie aus lauter homogenen Elementen beliebiger Beträge besteht. Für das weitere wird zunächst keine Homogenität vorausgesetzt.

Voraussetzung I. *$\mathfrak{L}$ habe eine Basis B, die Basen für $\mathfrak{U}$ und jedes $\mathfrak{L}_s$ enthält.* (Als Basis wird stets eine freie Γ-Modulbasis verstanden.)

Durchschnittsbildung liefert dann eine Basis für $\mathfrak{U} \cap \mathfrak{L}_s$. Wir denken uns B irgendwie **total geordnet.** Für die spätere Definition von $d_{ik}(a)$ sei dabei jedes Element aus $B \cap \mathfrak{U}$ größer als die Elemente im Komplement von $B \cap \mathfrak{U}$.

3. $\tilde{\mathfrak{L}}$ sei die nach der Theorie von Birkhoff-Witt existierende *universelle assoziative Hülle* von $\mathfrak{L}$ mit adjungiertem Einselement, in der also die Kommutatorrelationen

$$a\,a' = a'\,a + a \circ a' \qquad (a, a', a \circ a' \in \mathfrak{L})$$

erfüllt sind. Das „Korrekturglied" $a \circ a'$ denke man sich für das folgende linear durch die Basis B von $\mathfrak{L}$ ausgedrückt. Nach der erwähnten Theorie bilden die geordneten Monome $b_1 \ldots b_n$ mit $b_1 \leq \cdots \leq b_n$ $(b_i \in B,\ n \geq 0)$ eine Basis von $\tilde{\mathfrak{L}}$. Im p-Fall sind nur die Monome $b_1 \ldots b_n$ mit $b_1 \leq \cdots \leq b_n$ zu betrachten, bei denen nirgends p gleiche Faktoren auftreten. In beiden Fällen werden **diese Bedingungen für die Basismonome** $b_1 \ldots b_n$ im folgenden einheitlich mit

$$\mathfrak{o}(b_1, \ldots, b_n)$$

bezeichnet. Die übrigen $\prod b_i$ lassen sich dadurch linear auf diese Basis reduzieren, indem die obigen Kommutatorrelationen sukzessive auf verkehrt nebeneinanderstehende b_i angewandt werden, wobei im p-Fall noch die Ersetzung von b_i^p durch die entsprechende Linearkombination aus B als weitere Reduktion hinzukommt. Dies Verfahren werde kurz als **Ordnungsprozeß** bezeichnet. Aussagen, die im folgenden mit dem Ordnungsprozeß verbunden sind, lassen sich stets einfach durch Induktion nach der Anzahl der Schritte beweisen, jedoch lassen wir Einzelausführungen zugunsten größerer Übersichtlichkeit beiseite und begnügen uns hier mit diesem allgemeinen Hinweis.

In $\widetilde{\mathfrak{L}}$ bezeichne X_s bzw. $X_{(s)}$ den von allen assoziativen Produkten

$$x_1 \dots x_n \qquad (n \geqq 0,\ x_\nu \in X)$$

mit $|x_1| \dots |x_n| \leqq s$ bzw. $|x_1| \dots |x_n| = s$ aufgespannten Γ-Modul. Es ist dann wieder

$$X_s X_t \subseteqq X_{st}, \qquad X_{(s)} X_{(t)} \subseteqq X_{(st)}.$$

Falls $\widetilde{\mathfrak{L}}$ homogen ist, heißen die Elemente von $X_{(s)}$ wieder homogen vom Betrage s, analog wie vorhin. $\widetilde{\mathfrak{L}}$ ist dann ein homogener Ring. Allgemein heiße s eine *Schranke* für die Elemente von X_s. Nur die Elemente aus Γ haben die Schranke 1. Weiter sei B_s bzw. $B_s^{\mathfrak{o}}$ der von allen Produkten $b_1 \dots b_n$ aufgespannte Γ-Modul, für welche $b_\nu \in B \cap X_{s_\nu}$ und $s_1 \dots s_n \leqq s$ ist, bzw. außerdem noch $\mathfrak{o}(b_1, \dots, b_n)$ gilt.

Indem man nun unter Berücksichtigung der Voraussetzung I die $x \in X$ durch die $b \in B$ linear ausdrückt und umgekehrt die b geeignet als assoziative Polynome in den x schreibt, sieht man, daß $X_s = B_s$ ist. Darüber hinaus ist $B_s = B_s^{\mathfrak{o}}$, da sich der *Ordnungsprozeß* von B_s innerhalb X_s durchführen läßt. Da ferner die Basis B von $\mathfrak{L}$ in der Basis $\widetilde{B}$ von $\widetilde{\mathfrak{L}}$ enthalten ist, folgt

$$\mathfrak{L} \cap X_s = \mathfrak{L} \cap B_s^{\mathfrak{o}} = \mathfrak{L}_s.$$

Ausreichend und sogar einfacher wäre es gewesen, von vornherein die Voraussetzung I durch Ersetzung von $\mathfrak{L}_s$ durch $\mathfrak{L} \cap X_s$ abzuschwächen. Aber dann hätte die Voraussetzung nicht direkt $\mathfrak{L}$, sondern $\widetilde{\mathfrak{L}}$ betroffen.

4. Im folgenden sei $\mathfrak{U}_s = \mathfrak{U} \cap X_s$ und

$$\mathfrak{V}_s = \mathfrak{U} \cap \sum_{\substack{t_\nu < s \\ \Pi\, t_\nu \leq s}} \mathfrak{U}_{t_1} \dots \mathfrak{U}_{t_n} \qquad (t_\nu < s \text{ ist wesentlich!}). \tag{1}$$

Beachtet man nun wieder, daß die Basis B von $\mathfrak{L}$ in der Basis $\widetilde{B}$ von $\widetilde{\mathfrak{L}}$ enthalten ist, so kann man

$$\mathfrak{V}_s = \sum_{t<s} \mathfrak{U}_t + \sum_{t<s} \mathfrak{U}_t \circ \mathfrak{U}_{t^{-1}s}, \tag{2}$$

$$\mathfrak{V}_s = \sum_{t<s} \mathfrak{U}_t + \sum_{t<s} \mathfrak{U}_t \circ \mathfrak{U}_{t^{-1}s} + \sum_{t^p \leq s} \mathfrak{U}_t^p \tag{2p}$$

zeigen: In der Tat kann durch Anwendung des erwähnten *Ordnungsprozesses* auf (1) die Faktorenzahl auf $n \leqq 2$ reduziert werden. $n = 1$ liefert dann die erste Summe von (2), während für $n = 2$ eine nochmalige Reduktion auf die zweite Summe in (2) führt.

Voraussetzung II. *Für jedes $s \in \mathfrak{S}$ hat $\mathfrak{U}_s/\mathfrak{V}_s$ eine Basis, deren allgemeines Element mit y_s bezeichnet sei.*

Aus (2) folgt durch Induktion (weil $\mathfrak{S}$ ja wohlgeordnet war), daß der Γ-Modul $\mathfrak{U}_s$ von den LIEschen Produkten $y_{s_1} \circ \dots \circ y_{s_n}$ beliebiger Klammerung mit $\prod s_\nu \leqq s$ erzeugt wird. Insbesondere wird der LIEsche Unterring $\mathfrak{U}$ von der Menge Y aller $y_s, y_t, \dots$ erzeugt. — $\widetilde{\mathfrak{U}}$ bezeichne nun die assoziative Hülle von $\mathfrak{U}$ mit Einselement. Aus dem eben Bewiesenen oder aus (1) folgt, daß $\tilde{\mathfrak{U}} \cap X_s = \tilde{\mathfrak{U}} \cap B_s^0$ von den assoziativen Produkten $y_{s_1} \dots y_{s_n}$ mit $\prod s_\nu \leq s$ erzeugt wird. Dies werde symbolisch durch $\tilde{\mathfrak{U}} \cap X_s = Y_s$ ausgedrückt.

5. Die gesuchten Relationen zwischen den $y \in Y$ werden nun gewonnen mit Hilfe einer bestimmten Darstellung $D(a)$ von $\tilde{\mathfrak{L}}$. Hierzu sei $\{c_k\}$ die Familie aller geordneten Potenzprodukte der in B steckenden Basis von $\mathfrak{L}/\mathfrak{U}$. Das leere Produkt sei dabei $c_0 = 1$. Indem man $a\,c_k$ durch die Basis $\tilde{B}$ ausdrückt, erhält man vermöge

(3) $$a\,c_k = \sum c_i\, d_{ik}(a)$$

eine Darstellung von $\tilde{\mathfrak{L}}$ durch zeilenfinite Matrizen $(d_{ik}(a))$ mit Koeffizienten aus $\tilde{\mathfrak{U}}$. Insbesondere ist

(4) $$d_{i0}(\tilde{u}) = \delta_{i0} \cdot \tilde{u} \qquad (\tilde{u} \in \tilde{\mathfrak{U}};\ \delta_{00} = 1,\ \text{sonst } \delta_{i0} = 0).$$

Für $a \in \mathfrak{L}$ treten bei Anwendung des *Ordnungsprozesses* auf $a\,c_k$ *bei jedem Schritt*, wie sich durch Induktion ergibt, nur solche Glieder $\lambda b_1 \dots b_n$ ($n \geq 1$, $b_\nu \in B$) auf, die nach Streichung höchstens *eines* der b_ν die Gestalt λc_j haben. Dementsprechend sieht also die rechte Seite von (3) aus. Daher ist

(5) $$d_{ik}(\mathfrak{L}) \subseteqq \Gamma + \mathfrak{U} \quad \textit{und} \quad d_{0k}(\mathfrak{L}) \subseteqq \mathfrak{U}.$$

Mit $s(a)$ und $t(a)$ seien allgemein Schranken von $a \in \tilde{\mathfrak{L}}$ bezeichnet, mit der Abkürzung

(6) $$s_k = s(c_k) \quad \text{und} \quad t_i = t(c_i).$$

Mit willkürlichen Schranken $s(a)$, s_k liegt $a\,c_k$ in X_r, $r = s(a) \cdot s_k$. Wegen $X_r = B_r^0$ ist $a\,c_k$ Linearkombination aus Monomen $b_1 \dots b_n$, für welche das Produkt passender Schranken $\leq r$ ist. So erhält man für jedes Glied von (3) mit $d_{ik}(a) \neq 0$:

(7) $$s(a) \cdot s_k \geq t_i \cdot t(d_{ik}(a)).$$

Hierbei sind, wie gesagt, die Schranken $s(a)$, s_k willkürlich und die Schranken t_i und $t(d_{ik}(a))$ dazu passend zu wählen. Dabei kann $t_0 = t(1) = 1$ genommen werden. Da $\mathfrak{S}$ in einer geordneten Gruppe liegt, folgt aus (7) für $a = x$

(8) $$1 \leq t(d_{ik}(x)) \leq t_i^{-1}|x|\, s_k \qquad d_{ik}(x) \in Y_{t_i^{-1}|x|\, s_k} \qquad (t_i^{-1}|x|\, s_k \geq 1).$$

6. Jedes $d_{ik}(x) \in Y_{t_i^{-1}|x|\, s_k}$ läßt sich entsprechend als assoziatives Polynom in den y ausdrücken. Unter den verschiedenen Möglichkeiten, dies zu tun, sei eine ausgewählt, allerdings in Abhängigkeit von der Schranke $t_i|x|\, s_k$. Nun lassen sich für jedes Glied der rechten Seite von

(9) $$d_{i0}\left(\sum \lambda\, x_1 \dots x_n\right) = \sum \lambda\, d_{ik}(x_1) \dots d_{jl}(x_{n-1})\, d_{l0}(x_n)$$

die willkürlichen Schranken $\mathfrak{s}$ vom rechten Faktor anfangend nacheinander so normieren, daß $s(x_\nu) = |x_\nu|$ und s_k jeweils gleich dem im vorhergehenden

Schritt in Übereinstimmung mit (7) bestimmten t_h ist:

(10) $$s_0 = 1, \quad s_l = t_l, \quad s_j = t_j, \ldots .$$

Damit ist jedem Polynom $f = \sum \lambda x_1 \ldots x_n$ in wohlbestimmter Weise ein Polynom $d_{i0}(f)$ in den Unbestimmten y zugeordnet.

Unter den Voraussetzungen I und II gilt nun der

Hauptsatz. *Das von der Gesamtheit aller Relationen $r(x) = 0$ induzierte System von Relationen $d_{i0}(r) = 0$ in den y erzeugt alle assoziativen Relationen in den y. Sind insbesondere die x freie Erzeugende von $\mathfrak{L}$, so sind die y freie Erzeugende von $\mathfrak{U}$. Im Falle eines Körpers als Koeffizientenbereich Γ ist jeder Unterring eines freien* LIE*schen Ringes wieder frei.*

Beweis. $\mathfrak{R}$ sei das durch die Relationen $d_{i0}(r) = 0$ definierte Ideal in dem von den Unbestimmten y_s erzeugten Ring. Die Restklasse von y_s mod $\mathfrak{R}$ sei mit y_s' bezeichnet. Entsprechend läßt sich mit Hilfe von (9) für $f \in \widetilde{\mathfrak{L}}$ eine Restklasse $d_{i0}'(f)$ mod $\mathfrak{R}$ nach Konstruktion von $\mathfrak{R}$ *eindeutig* bilden. Da nun für die y' nur Relationen gelten, die für die y sicher erfüllt sind, hat man eine kanonische homomorphe Abbildung mit $y' \to y$. Der Hauptsatz ist bewiesen, wenn wir zeigen können, daß die Anwendung von d_{00}' die Umkehrung dieser Abbildung bewirkt.

Es sei T der Gültigkeitsbereich von

(11) $$d_{i0}'(y_t) = \delta_{i0} \cdot y_t' \qquad (t \in T).$$

Indem man $d_{i0}'(f)$ als erste Spalte einer Darstellungsmatrix auffaßt, die in ihren übrigen Teilen allerdings mehrdeutig ist, folgt, daß d_{00}' jedes Polynom in $y_t (t \in T)$ homomorph auf das entsprechende Polynom in y_t' abbildet. Zur Vollendung des Beweises genügt es daher

(12) $$d_{i0}'(y_s) = \delta_{i0}\, y_s'$$

für beliebiges s durch Induktion zu bestätigen. Angenommen also, T enthalte alle Indizes $t < s$. Nun sei

(13) $$y_s = \sum \lambda x_1 \ldots x_n \quad \text{mit} \quad |x_1| \ldots |x_n| \leq s.$$

In der nach (4) und (9) bestehenden Relation in den y

(14) $$d_{i0}(y_s) = \sum \lambda\, d_{ik}(x_1) \ldots d_{jl}(x_{n-1})\, d_{l0}(x_n) = \delta_{i0}\, y_s$$

ist das Produkt der zugehörigen normierten Schranken

(15) $$[t_i^{-1}|x_1|\, t_k] \ldots [t_j^{-1}|x_{n-1}|\, t_l]\, [t_l^{-1}|x_n|] \leq t_i^{-1} s \leq s.$$

Hier ist jede Schranke $[\ ] \leq s$. Der Fall $[\ ] = s$ kann bei jedem Monom höchstens einmal auftreten, die anderen Schranken $[\ ]$ sind dann gleich 1 und die zugehörigen $d_{\alpha\beta}(x) \in \Gamma$, ferner ist dann rechts $t_i = 1$, also $i = 0$. Da dann die linke Schranke $[|x_1|\, t_k] > 1$ ist, ist *sie* es mit dem Wert s.

Hiernach kommen in der Relation (14) nur die y_t mit $t \leq s$ vor, dabei die Basiselemente von $\mathfrak{U}_s/\mathfrak{V}_s$ höchstens linear. Aber gerade auf Grund der Basiseigenschaft heben sich die letzteren in der Relation identisch fort. Also ist (14) in Wirklichkeit nur eine Relation zwischen y_t mit $t < s$ und geht daher durch Anwendung von d'_{00} in (12) über. Damit ist der Hauptsatz bewiesen. Nach der Diskussion von $[\,] = s$ folgt außerdem nach (14) mit $i = 0$ unter Beachtung von (5) der

Satz 2. $\mathfrak{U}_s/\mathfrak{V}_s$ *wird linear aufgespannt von den* $d_{0k}(x)$ *mit* $|x|\ t_k = s$.

Hier tritt das Problem auf, eine Basis B von $\mathfrak{L}$ zu finden, die so beschaffen ist, daß die von Null verschiedenen $d_{0k}(x)$ linear unabhängig sind, *so daß man deren Gesamtheit als die Erzeugung* Y *von* $\mathfrak{U}$ *nehmen kann*, von der im Hauptsatz die Rede ist. Eine solche Basis B heiße im folgenden eine **ökonomische** *Basis bezüglich* $\mathfrak{U}$. Die Frage nach der Existenz einer ökonomischen Basis wird in Satz 10 behandelt.

7. Für den Fall, daß Γ ein Körper ist, nehme man einen *total wohlgeordneten* Kegel, z. B. den (unendlichen) zyklischen Kegel $\{\xi^n\}$ und etwa $|x| = \xi$ (d. h. additiv: den Kegel der natürlichen Zahlen und Grad $x = 1$). Eine Basis B der in Voraussetzung I beschriebenen Art läßt sich dann so bilden, daß man eine nach Beträgen geordnete Basis von $\mathfrak{U}$ zu einer nach Beträgen geordneten Basis von $\mathfrak{L}$ ergänzt. Die Möglichkeit dieser Basiskonstruktion läßt sich leicht aus der angenommenen totalen Wohlordnung von $\mathfrak{S}$ beweisen. Auch in anderen Fällen ist es oft vorteilhaft, den Kegel $\mathfrak{S}$ und die Abbildung $x \to |x|$ passend zu wählen.

Eine Vereinfachung im Beweis tritt ein, wenn jedes c_k nur *eine* minimale Schranke hat (z. B. wenn $\mathfrak{S}$ total wohlgeordnet ist). Dann kann von vornherein $s_k = t_k =$ dieser minimalen Schranke gesetzt werden. Dadurch wird es möglich, allgemein $d_{jk}(\sum \lambda x_1 \ldots x_n)$ eindeutig als Polynom in den y zu erklären. Ebenso wie der Hauptsatz wird dann folgender Satz bewiesen:

Satz 3. *Das von einem definierenden System von Relationen* $r_\alpha(x) = 0$ *induzierte System der Komponenten der Matrixrelationen* $r_\alpha(d_{ik}(x)) = 0$ *erzeugt alle assoziativen Relationen in den* y.

8. Berechnung von $d_{0k}(a)$ $(a \in \mathfrak{L})$ bei spezieller Basis B zur Anwendung von Satz 2.

Voraussetzung III. *Die in Voraussetzung I angenommene Basis* B *sei so beschaffen, daß für jedes* $b_1 \notin \mathfrak{U}$ *die Menge der* $b \geq b_1$ *linear einen Unterring von* $\mathfrak{L}$ *aufspannt* $(b_1, b \in B)$.

Dies trifft z. B. zu, wenn alle Elemente der Basis homogen und die $b_\beta \in \mathfrak{L}/\mathfrak{U}$ nach aufsteigenden Beträgen geordnet sind (wobei also die Abbildung $b_\rho \to |b_\beta|$ isoton ist). In diesem Falle sind die $|b_\beta|$ natürlich total wohlgeordnet.

Es sei hier hervorgehoben, daß an den Voraussetzungen I und III das Wichtigste die Aussagen über die Relativbasis von $\mathfrak{L}/\mathfrak{U}$ sind. Auf die Basis von $\mathfrak{U}$ könnte man in vielen Fällen verzichten.

Im Fall $c_k = b_1 \ldots b_r$ werde die deutlichere **Bezeichnung** eingeführt:

(16) $$d_{0k}(a) = a \bullet b_1 \ldots b_r \qquad (a \in \mathfrak{L}).$$

Ferner bedeute

(17) $$\sum_\nu \lambda_\nu b_\nu * b_\mu = \sum_{b_\nu > b_\mu} \lambda_\nu b_\nu \circ b_\mu .$$

Satz 4. *Unter der Voraussetzung III hat man für die rekursive Darstellung der* $d_{0k}(a)$:

(18) $$\sum \lambda_\nu b_\nu \bullet 1 = \sum_{b_\nu \in \mathfrak{U}} \lambda_\nu b_\nu ,$$

(19) $$d_{0k}(b) = b \bullet b_1 \ldots b_r = (b * b_1) \bullet b_2 \ldots b_r \qquad (b \in B,\ r > 0),$$

(19p) *dazu noch im p-Fall* $b \bullet b_1 \ldots b_r = b^p \bullet b_p \ldots b_r$ *falls* $b = b_1 = \cdots = b_{p-1}$.

Insbesondere gilt die explizite Formel

(20) $$d_{0k}(a) = a \bullet b_1 \ldots b_r = \big(((a * b_1) * \cdots) * b_r\big) \bullet 1 ,$$

(20p) *(im p-Fall modifiziert sich allerdings die rechte Seite, wenn unter den* b_ν $p-1$ *gleiche vorkommen).*

Beweis. (19) ist trivial für $b \leq b_1$. Für $b > b_1$ ist

$$b\, b_1 b_2 \ldots b_r = (b * b_1)\, b_2 \ldots b_r + b_1 b\, b_2 \ldots b_r$$

und hier ist zu zeigen, daß $b_1 b b_2 \ldots b_r$ keinen Beitrag zu $d_{0k}(a)$ liefert. Das folgt daraus, daß bei jedem Schritt des Ordnungsprozesses, wie man durch Induktion sieht, immer b_1 erster Faktor und alle übrigen Faktoren $\geq b_1$ sind (im p-Fall ist die Zahl der zu b_1 gleichen Faktoren $\leq p-1$). Trivial ist auch (18); (20) folgt aus (18) und (19).

§ 3. Unterringe eines freien Lieschen Ringes mit einem Hauptidealring Γ als Koeffizientenbereich

Es werde folgende Voraussetzung gemacht:

Voraussetzung IV. *$\mathfrak{L}$ sei der mit der Erzeugung X freie* LIE*sche Ring mit einem kommutativen Hauptidealring Γ als Koeffizientenbereich. Die zugrunde gelegte Abbildung* $x \to |x| > 1$ *in den wohlgeordneten*[5]) *kommutativen Kegel $\mathfrak{S}$ einer geordneten Gruppe sei so beschaffen, daß für jedes* $s \in \mathfrak{S}$ *nur endlich viele x einen Betrag* $|x| \leq s$ *haben, mit anderen Worten,* $\sum |x|$ *sei formal summierbar.*

Die Summierbarkeit läßt sich immer erreichen, z.B. indem man die x eineindeutig auf assoziative und kommutative Unbestimmte ξ bezieht und den Kegel der aus den ξ gebildeten Monome, geordnet im Sinne der Teilbarkeit, zugrunde legt. Dieser Kegel heiße der zugehörige **monomiale** Kegel.

Aus der Summierbarkeit von $\sum |x|$ folgt

(1) $$(1 - \sum |x|)^{-1} = \sum \alpha_s s$$

mit formal summierbarer rechter Seite, in der die natürliche Zahl α_s, ihrem Bildungsgesetz entsprechend, den Rang von $X_{(s)}$ angibt, die formale Summierbarkeit also einfach die *Endlichkeit des Ranges* von $X_s = \sum_{t \leq s} X_{(t)}$ bedeutet.

Hilfssatz. *Die Voraussetzung II ist eine Folge der Voraussetzungen I und IV.*

Beweis. $\mathfrak{Y}_t$ sei der von den Elementen y_t in Voraussetzung II erzeugte Untermodul von $\mathfrak{U}_t$. Für $t<s$ sei bereits $\mathfrak{U}_t = \mathfrak{B}_t \dotplus \mathfrak{Y}_t$ gezeigt. Da Γ ein Hauptidealring ist, genügt es wegen der Endlichkeit des Ranges von X_s, in dem $\mathfrak{U}_s$ liegt, die Torsionslosigkeit von $\mathfrak{U}_s/\mathfrak{B}_s$ zu beweisen. Dazu sei für ein beliebiges Primelement $\pi \in \Gamma$ und für $u \in \mathfrak{U}_s$

$$\pi u = f(y_t) \in \mathfrak{B}_s \qquad (t < s). \tag{2}$$

Es werde nun die Abbildung $\mathfrak{L} \to \mathfrak{L}/\pi\mathfrak{L}$ vorgenommen. Der neue Koeffizientenbereich Γ/π ist ein Körper. Bei dieser Abbildung bleibt jede direkte Zerlegung $\mathfrak{L} = \sum \mathfrak{M}_\nu$ direkt, also bleibt B aus Voraussetzung I eine Basis mit gleicher Eigenschaft. Folglich bleibt $\mathfrak{U}_\sigma = \mathfrak{U} \cap \mathfrak{L}_\sigma$ bestehen, und nach (2) § 2 behält $\mathfrak{B}_\sigma$ seine alte Bedeutung. Da die $\mathfrak{U}_\sigma$ direkte Summanden von $\mathfrak{L}$ sind, bleibt $\mathfrak{U}_t = \mathfrak{B}_t \dotplus \mathfrak{Y}_t$ für $t<s$ auch nach der Abbildung bestehen. Da Γ/π ein Körper ist, gilt die Voraussetzung II sicher nach der Abbildung, insbesondere bestehen dann nach dem Hauptsatz für die y_t mit $t<s$ keinerlei Relationen. Das bedeutet aber, daß in (2) $\pi u = f(y_t) = \pi g(y_t)$ ist, und, weil $\mathfrak{L}$ torsionslos ist, $u = g(y_t) \in \mathfrak{B}_s$, wie zu zeigen war.

Unter der Voraussetzung IV gilt der für die Anwendungen in der Gruppentheorie wichtige Satz:

Satz 5. *Jeder homogene Unterring $\mathfrak{U}$ eines freien* Lie*schen Ringes $\mathfrak{L}$ mit torsionslosem Faktormodul $\mathfrak{L}/\mathfrak{U}$ läßt sich durch homogene Elemente y frei erzeugen. Die Voraussetzung IV überträgt sich von $\mathfrak{L}$ auf $\mathfrak{U}$ hinsichtlich $y \to |y|$.*

Beweis. Zur Anwendung des Hauptsatzes ist nach dem eben bewiesenen Hilfssatz nur noch die Voraussetzung I nachzuprüfen.

$\mathfrak{L}_{(s)}$ und $\mathfrak{U}_{(s)} = \mathfrak{U} \cap X_{(s)}$ haben als Untermoduln des freien Γ-Moduls $X_{(s)}$ Basen bezüglich Γ. Als torsionsloser Faktormodul des endlichen Γ-Moduls $\mathfrak{L}_{(s)}$ hat auch $\mathfrak{L}_{(s)}/\mathfrak{U}_{(s)}$ eine Γ-Basis. Die Vereinigung B der Γ-Basen aller $\mathfrak{U}_{(s)}$ und $\mathfrak{L}_{(s)}/\mathfrak{U}_{(s)}$ ist dann eine homogene Basis, die die Voraussetzung I erfüllt. Zugleich sieht man, daß $\mathfrak{U}$ eine freie homogene Erzeugung Y hat. $\sum |y|$ hat schließlich nach (1) die summierbare Majorante $\sum \alpha_s s$.

Unter der Voraussetzung IV gilt der für numerische Rangberechnungen grundlegende

Satz 6. *Zwischen den freien Erzeugenden X und einer homogenen Basis B von $\mathfrak{L}$ besteht die formale Relation*

$$(1 - \sum |x|)^m = \prod (1 - |b|)^m \qquad (x \in X,\ b \in B,\ m = \pm 1), \tag{3}$$

$$(1 - \sum |x|)^m = \prod \left(\frac{1 - |b|}{1 - |b|^p}\right)^m \qquad (x \in X,\ b \in B,\ m = \pm 1). \tag{3p}$$

Mit anderen Worten: Für einen freien LIE*schen Ring gilt unter der Voraussetzung IV*

$$(4)\qquad 1-\sum \varepsilon_s s = \prod (1-s)^{\beta_s},$$

$$(4p)\qquad 1-\sum \varepsilon_s s = \prod \left(\frac{1-s}{1-s^p}\right)^{\beta_s},$$

wo ε_s die Anzahl der freien Erzeugenden x vom Betrage s und β_s die Anzahl der homogenen Basiselemente b vom Betrage s bezeichnet.

Wie schon in § 1 gesagt, sind durch (4) *die ε_s von den β_s und umgekehrt „rekursiv" abhängig.*

Beweis von Satz 6. Von $\tilde{\mathfrak{L}}$ kennen wir folgende zwei homogene Basen: 1. Alle Potenzprodukte der x, und 2. die geordneten Potenzprodukte der b. Daher ist

$$(5)\qquad \sum |x_1|\ldots|x_n| = \sum^{(0)} |b_1|\ldots|b_n| \qquad [n \text{ variabel } \geqq 0;\ \mathfrak{o}(b_1,\ldots,b_n)].$$

Die Summierbarkeit der linken Seite folgt dabei nach Satz 1 aus derjenigen von $\sum |x|$. Nach demselben Satz ist (5) gleichwertig mit (3).

Hat $\mathfrak{L}$ ε Erzeugende und wird $|x| = \xi \in \{\xi^n\}$ zugrunde gelegt, so findet man nach § 1 (8) für den Rang des in x homogenen Moduls $\mathfrak{L}_{(n)}$ (der Index wird hier additiv geschrieben) die Formel

$$(6)\qquad \psi_n(\varepsilon) = \frac{1}{n}\sum_{d|n} \mu(d)\,\varepsilon^{n/d},$$

die ich 1937 bewiesen habe[8]). Im p-Fall gilt nach § 1 (8p) die entsprechende Rangformel

$$(6p)\qquad \psi_n(\varepsilon) = \frac{1}{n}\sum_{d|n} \mu(d_0)\,\varphi(p^h)\,\varepsilon^{n/d} \qquad (d = d_0 p^h,\ p \nmid d_0)$$

mit der EULERschen Funktion $\varphi(p^h)$.

Aus Satz 6 erhält man, ebenfalls unter Voraussetzung IV:

Satz 7. *Ein Unterring $\mathfrak{U}$ eines freien* LIE*schen Ringes $\mathfrak{L}$, der von Moduln $\mathfrak{L}_{(t)}$, $t \in T \subseteqq \mathfrak{S}$, erzeugt wird, ist stets frei.*

Beweis. Nach Satz 5 ist nur zu zeigen, daß $\mathfrak{L}/\mathfrak{U}$ torsionsfrei ist. Wegen der Homogenität von $\mathfrak{L}$ genügt es, dies für alle $\mathfrak{L}_{(s)}/\mathfrak{U}_{(s)}$ ($s \in \mathfrak{S}$) zu beweisen. — K sei der Quotientenkörper von Γ und π bezeichne die Primelemente von Γ. Ferner seien $K\mathfrak{L}$ und $\mathfrak{L}/\pi\mathfrak{L}$ die freien LIEschen Ringe, die man aus $\mathfrak{L}$ erhält, indem man statt Γ die Körper K bzw. Γ/π als Koeffizientenbereich wählt. Für die Ränge von $K\mathfrak{L}_{(s)}$ bzw. $\mathfrak{L}_{(s)}/\pi\mathfrak{L}_{(s)}$ gelten dann Relationen der Form (4), jedesmal mit denselben $\varepsilon_s(\mathfrak{L})$, also stimmen diese Ränge überein. Ferner sind nach dem Hauptsatz auch $K\mathfrak{U}$ bzw. $\mathfrak{U}/\mathfrak{U} \cap \pi\mathfrak{L}$ frei, so daß für diese ebenfalls Bedingungen der Gestalt (4) gelten. Aus der Voraussetzung des Satzes und § 2, (2) folgt, daß in jedem dieser Fälle entweder $\varepsilon_s = 0$ oder β_s

[8]) WITT, E.: Treue Darstellung LIEserch Ringe. J. reine u. angew. Math. **177**, 152—160 (1937).

bekannt ist, nämlich gleich $\beta_s(\mathfrak{L})$. Da sich hieraus die übrigen ε_s und β_s jedesmal durch dieselbe Formel (4) bestimmen, haben alle ε_s und β_s für $K\mathfrak{U}$ und $\mathfrak{U}/\mathfrak{U}\cap\pi\mathfrak{L}$ dieselben Werte.

Wegen Voraussetzung IV sind nun die $\mathfrak{L}_{(s)}$ endliche Γ-Moduln. Man kann hier also den Hauptsatz für abelsche Gruppen mit endlich vielen Erzeugenden anwenden. Danach hätte $\mathfrak{L}_{(s)}/\mathfrak{U}_{(s)}$ genau dann Torsion, wenn bei passendem $\pi\in\Gamma$ der Rang von $\frac{\mathfrak{L}_{(s)}/\pi\mathfrak{L}_{(s)}}{\mathfrak{U}_{(s)}/\pi\mathfrak{U}_{(s)}}$ größer wäre als der von $K\mathfrak{L}_{(s)}/K\mathfrak{U}_{(s)}$. Dies kann aber nicht eintreten, denn diese Ränge sind nach dem eben Gesagten jedesmal gleich der Differenz zwischen den Rängen von $K\mathfrak{L}_{(s)}$ und $K\mathfrak{U}_{(s)}$, also ist $\mathfrak{L}_{(s)}/\mathfrak{U}_{(s)}$ torsionsfrei, und das sollte gezeigt werden.

Als Anwendung hiervon läßt sich z. B. der Rang β_{i+k} von $\mathfrak{L}_{(i)}\circ\mathfrak{L}_{(k)}$ explizit berechnen $(i\leqq k)$:

$$\beta_{i+k}=\gamma_{i+k}(\psi_i(\varepsilon))+\psi_i(\varepsilon)\cdot(\psi_k(\varepsilon)-\gamma_k(\psi_i(\varepsilon))),\tag{7}$$

wobei stets $\gamma_\nu=\psi_{\nu/i}$ bedeute und letzteres für echt gebrochene Indizes als Null erklärt wird. (7) läßt sich folgendermaßen zeigen:

Der von $\mathfrak{L}_{(i)}$ und $\mathfrak{L}_{(k)}$ erzeugte Unterring $\mathfrak{U}$ ist nach Satz 7 frei und hat im Falle $i<k$, den wir zunächst betrachten, $\varepsilon_{(i)}+\varepsilon_{(k)}$ freie Erzeugende, wenn $\varepsilon_{(i)}$, $\varepsilon_{(k)}$ den Rang von $\mathfrak{B}_{(i)}$ bzw. $\mathfrak{B}_{(k)}$ bedeuten. In $\beta_{i+k}=\gamma_{i+k}(\varepsilon_{(i)})+\varepsilon_{(i)}\varepsilon_{(k)}$ ist $\varepsilon_{(i)}=\psi_i(\varepsilon)$ wegen $\mathfrak{B}_{(i)}=\mathfrak{L}_{(i)}$, und $\varepsilon_{(k)}$ ergibt sich aus der Rangformel $\psi_k(\varepsilon)-\varepsilon_{(k)}=\gamma_k(\varepsilon_{(i)})$ für $\mathfrak{L}_{(k)}/\mathfrak{B}_{(k)}$. Durch Einsetzung folgt jetzt (7). Für $i=k$ ist analog $\beta_{2i}=\gamma_{2i}(\varepsilon_{(i)})=\gamma_{2i}(\psi_i(\varepsilon))$, und wegen $\gamma_i(\psi_i(\varepsilon))=\psi_i(\varepsilon)$ gilt wieder (7).

Für den Fall $i<k$ läßt sich dies übrigens auch ohne Eingehen auf den LIEschen Ring $\mathfrak{L}$ selbst, allein aus der Beziehung (4), erhalten. Man hat für $\mathfrak{U}$

$$1-\varepsilon_{(i)}\xi^i-\varepsilon_{(k)}\xi^k=(1-\xi^i)^{\beta_i(\mathfrak{L})}(1-\xi^k)^{\beta_k(\mathfrak{L})}\prod_{n\neq i,k}(1-\xi^n)^{\beta_n(\mathfrak{U})}$$

und, daneben, für $\mathfrak{L}_{(i)}$

$$1-\varepsilon_{(i)}\xi^i=\prod(1-\xi^\nu)^{\gamma_\nu(\varepsilon_{(i)})}.$$

Durch Division erhält man dann

$$1-\frac{\varepsilon_{(k)}\xi^k}{1-\varepsilon_{(i)}\xi^i}=(1-\xi^k)^{\beta_k(\mathfrak{L})-\gamma_k(\varepsilon_{(i)})}\prod_{n\neq i,k}(1-\xi^n)^{\beta_n(\mathfrak{U})-\gamma_n(\varepsilon_{(i)})}.$$

[Der erste Faktor rechts fällt wegen $\beta_i(\mathfrak{L})=\varepsilon_{(i)}=\gamma_i(\varepsilon_{(i)})$ fort.] Durch Vergleich der Koeffizienten von ξ^k und ξ^{i+k} erhält man dann

$$\varepsilon_{(k)}=\beta_k(\mathfrak{L})-\gamma_k(\varepsilon_{(i)})\qquad\text{und}\qquad\varepsilon_{(i)}\,\varepsilon_{(k)}=\beta_{i+k}(\mathfrak{U})-\gamma_{i+k}(\varepsilon_{(i)}),$$

was für $\beta_{i+k}=\beta_{i+k}(\mathfrak{U})$ dasselbe wie oben liefert. Eine völlig analoge Rechnung läßt sich im p-Fall mit Hilfe der Formel ($4p$) durchführen. —

Üblicherweise versteht man unter der absteigenden Zentralreihe von $\mathfrak{L}$ die Folge

$$\mathfrak{L}^k=\sum_{m\geq k}\mathfrak{L}_{(m)}.\tag{8}$$

Als Anwendung von Satz 6 werde folgende Aufgabe gelöst:

Aufgabe. *Unter Voraussetzung IV sollen die Rangzahlen $\beta_s(\mathfrak{L}^k)$ aus den Rangzahlen $\beta_s(\mathfrak{L})$ numerisch bestimmt werden, ohne dabei im* LIE*schen Ring zu rechnen.*

Aus (4) mit $\beta_s = \beta_s(\mathfrak{L})$ bekommt man zunächst die Anzahl ε_s der freien Erzeugenden x von $\mathfrak{L}$ vom Betrage s. Da $\mathfrak{L}^k/\mathfrak{L}^{k+1}$ isomorph ist zum Modul aller in den x homogenen LIEschen Polynome vom Grade k, lautet (4) für die neue Abbildung $x \to |x| \cdot \xi$ in das direkte Produkt $\mathfrak{S} \times \{\xi^n\}$ von $\mathfrak{S}$ mit dem (unendlichen) zyklischen Kegel $\{\xi^n\}$

$$1 - \sum \varepsilon_s\, s\, \xi = \prod_{s,k} (1 - s\,\xi^k)^{\beta_s(\mathfrak{L}^k) - \beta_s(\mathfrak{L}^{k+1})}, \tag{9}$$

$$1 - \sum \varepsilon_s\, s\, \xi = \prod_{s,k} \left(\frac{1 - s\,\xi^k}{1 - s^p\,\xi^{pk}}\right)^{\beta_s(\mathfrak{L}^k) - \beta_s(\mathfrak{L}^{k+1})}. \tag{9p}$$

Hiermit lassen sich aus den ε_s die Differenzen $\beta_s(\mathfrak{L}^k) - \beta_s(\mathfrak{L}^{k+1})$ berechnen, und aus ihnen, ausgehend von $\beta_s(\mathfrak{L})$, rekursiv die gewünschten $\beta_s(\mathfrak{L}^k)$.

Von gewissen Teilbasen von $\mathfrak{L}$ kann man unter Umständen a priori feststellen, daß zwischen ihren Elementen keine LIEschen Relationen möglich sind. Unter Voraussetzung IV gilt

Satz 8. *Ist innerhalb einer Teilmenge S des Kegels $\mathfrak{S}$ kein Element als Produkt darstellbar, so ist die Menge $Y = \bigcup B_{(s)}$ von Basen $B_{(s)}$ der homogenen Moduln $X_{(s)}$ $(s \in S)$ frei, d.h. der von Y erzeugte Unterring $\mathfrak{U}$ hat Y als freie Erzeugung.*

Beweis. $\mathfrak{U}$ ist ein homogener Ring, bestehend aus den homogenen Moduln $\mathfrak{U}_{(t)}$ mit $t = \prod s_\mu$, $s_\mu \in S$. Nun kann im Beweis des Hauptsatzes für einen homogenen Unterring $\mathfrak{U}$ mit gleicher Wirkung $\mathfrak{U}_s$ durch $\mathfrak{U}_{(s)}$, und $\mathfrak{V}_s$ durch

$$\mathfrak{V}_{(s)} = \mathfrak{V}_s \cap \mathfrak{U}_{(s)} = \mathfrak{U} \cap \sum_{\substack{t_\nu < s \\ \Pi t_\nu = s}} \mathfrak{U}_{(t_1)} \cdots \mathfrak{U}_{(t_n)}$$

ersetzt werden. S hat nun die Eigenschaft, daß $\mathfrak{V}_{(s)} = 0$ ist, daher kann in der Voraussetzung II als Basis von $\mathfrak{U}_s/\mathfrak{V}_s$ gerade $B_{(s)}$ genommen werden, und die Vereinigung dieser Basen ist dann nach dem Hauptsatz frei.

Erweiterung von Satz 8. Ersetzt man in einer homogenen freien Menge Y jedes Element y vom Betrag s durch ein

$$y^* = y + \sum y_i \quad \text{mit} \quad |y_i| < s$$

[bzw. durchgehend $|y_i| > s$], so entsteht wieder eine freie Menge.

Beweis. Angenommen $r(u)$ sei ein LIEsches Polynom mit $r(y^*) = 0$. Ist $r_0(u)$ der homogene Bestandteil höchsten [bzw. niedrigsten] Grades von $r(u)$, so müßte auch $r_0(y) = 0$ sein, obwohl Y frei angenommen war.

In ähnlicher Weise kommt man zu folgendem

Satz 9. *Zwischen zwei linear unabhängigen Elementen a und b eines freien* LIE*schen Ringes $\mathfrak{L}$ gibt es überhaupt keine Relationen.*

Dagegen kann es bei drei Elementen natürlich Relationen geben, z.B. zwischen $a, b, a \circ b$.

Im p-Fall ist Satz 9 in der vorliegenden Fassung falsch, da ja zwischen a und a^p eine Relation besteht. Statt dessen läßt sich hier sagen, daß *es für 1 Element* $a \neq 0$ *keine Relationen gibt*, wie man in $\tilde{\mathfrak{L}}$ sieht.

Beweis. a und b werden bereits aus einer endlichen Teilmenge $X_0 \subseteqq X$ erzeugt. Für den Beweis genügt es, $X = X_0$ anzunehmen. Es werde $|x| = \xi$ im zyklischen Kegel $\mathfrak{S} = \{\xi^n\}$ festgesetzt. Durch eine geeignete umkehrbare lineare Transformation kann man nun erreichen, daß die homogenen Leitglieder a_n und b_m der höchsten Grade n und m linear unabhängig sind. Es genügt nach dem obigen Beweis, zu zeigen, daß $Y = \{a_n, b_m\}$ frei ist. Dies wird fast ebenso wie Satz 8 bewiesen, nur wird man hier $\mathfrak{B}_{(\xi^n)} = \mathfrak{B}_{(\xi^m)} = 0$ direkt begründen.

Die geeignete Umkehrung von Satz 6 ergibt ein Kriterium dafür, daß ein LIEscher Ring frei ist: $\mathfrak{L}$ sei ein von einer Familie $\{x_\iota\}$, $\iota \in I$, erzeugter homogener LIEscher Ring mit einem kommutativen Hauptidealring Γ als Koeffizientenbereich. Die zugrunde gelegte Abbildung $x_\iota \to |x_\iota|$ in den wohlgeordneten Kegel $\mathfrak{S}$ einer geordneten Gruppe sei so beschaffen, daß $\sum |x_\iota| = \sum \varepsilon_s s$ formal summierbar ist. β_s sei der Rang von $\mathfrak{L}_{(s)}$ modulo seiner Torsion.

Kriterium. $\{x_\iota\}$ *ist genau dann eine freie Erzeugung von* $\mathfrak{L}$, *falls*

$$\prod (1 - s)^{\beta_s} = 1 - \sum \varepsilon_s s, \tag{10}$$

$$\prod \left(\frac{1 - s}{1 - s^p}\right)^{\beta_s} = 1 - \sum \varepsilon_s s. \tag{10p}$$

Beweis. $\bar{\mathfrak{L}}$ sei der aus lauter verschiedenen Unbestimmten $\bar{x}_\iota$ erzeugte freie LIEsche Ring ($\iota \in I$). Es werde $|\bar{x}_\iota| = |x_\iota|$ gesetzt. Hierdurch wird $\bar{\mathfrak{L}}$ ein homogener Modul. Nach Satz 6 folgt aus (10), daß β_s zugleich der Rang des freien Γ-Moduls $\bar{\mathfrak{L}}_{(s)}$ ist. Daher muß $\bar{\mathfrak{L}}_{(s)}$ isomorph zu seinem Faktormodul $\mathfrak{L}_{(s)}$ sein. Aus der Homogenität von $\mathfrak{L}$ folgt jetzt, daß $\bar{x}_\iota \to x_\iota$ einen Isomorphismus erzeugt.

Explizite Angabe einer freien Erzeugung eines Unterringes $\mathfrak{U}$ unter gewissen Bedingungen. Für die b_i einer Basis B von $\mathfrak{L}$ bedeute

$$\mathfrak{u}(b_1, \ldots, b_n) \qquad (n \geqq 0), \tag{11}$$

daß die früher erklärte Relation $\mathfrak{o}(b_1, \ldots, b_n)$ und außerdem $b_i \notin \mathfrak{U}$ besteht.

Satz 10. $\mathfrak{U}$ *sei bezüglich der Erzeugung* X *ein homogener Unterring des* LIE*schen Ringes* $\mathfrak{L}$ *mit der Basis* B. *Außer den Voraussetzungen I bis IV werde* $X \subseteqq B$ *angenommen. Dann wird* $\mathfrak{U}$ *von den Elementen*

$$y = d_{0k}(x) = x \bullet b_1 \ldots b_n \quad \begin{cases} \textit{mit} & \mathfrak{u}(b_1, \ldots, b_n) \\ \textit{aber nicht} & \mathfrak{u}(x, b_1, \ldots, b_n) \end{cases} \tag{12}$$

frei erzeugt.

Satz 10 besagt genau, daß B eine ökonomische Basis von $\mathfrak{L}$ bezüglich $\mathfrak{U}$ ist. In Verbindung mit Satz 4 ergeben sich in speziellen Fällen fertige Formeln für eine Erzeugung von $\mathfrak{U}$.

Beweis von Satz 10: Nach Satz 2 wird $\mathfrak{U}$ von diesen $d_{0k}(x)$ erzeugt, da im Fall $\mathfrak{u}(x, b_1, \ldots, b_n)$ $d_{0k}(x) = 0$ ist. In der folgenden Abzählung ist zu beachten, daß aus $\mathfrak{u}(x, b_1, \ldots, b_n)$ auch $\mathfrak{u}(b_1, \ldots, b_n)$ folgt. Durchläuft e die Menge $E = B - B \cap \mathfrak{U}$, so hat man

$$(13)\quad \begin{cases} \sum |y| - 1 = \sum |x| \prod (1 - |e|)^{-1} - \prod (1 - |e|)^{-1} \\ \qquad = (\sum |x| - 1) \prod (1 - |e|)^{-1} = - \prod (1 - |b|) \prod (1 - |e|)^{-1}, \end{cases}$$

$$(13p)\quad \begin{cases} \sum |y| - 1 = \sum |x| \prod \frac{1 - |e|^p}{1 - |e|} - \prod \frac{1 - |e|^p}{1 - |e|} \\ \qquad = (\sum |x| - 1) \prod \frac{1 - |e|^p}{1 - |e|} = - \prod (1 - |b|) \prod \frac{1 - |e|^p}{1 - |e|} \end{cases}$$

und damit ist das Kriterium (10) für die Familie $\{y\}$ erfüllt, q. e. d.

Besteht speziell die Erzeugung X aus k und E aus $\varkappa$ Elementen und ist immer $|x| = \xi \in \mathfrak{S}$ (ξ fest), so erhält man aus (13) eine explizite Formel für die Anzahl der Erzeugenden y von $\mathfrak{U}$, die den Grad $n \neq 0$ in den Erzeugenden x von $\mathfrak{L}$ haben, durch den Koeffizienten von ξ^n in

$$(14)\qquad \sum |y| - 1 = \frac{k\xi - 1}{(1 - \xi)^{\varkappa}} = \sum_{n=0}^{\infty} \left(n \frac{k - 1}{\varkappa - 1} - 1 \right) \binom{n + \varkappa - 2}{n} \xi^n,$$

$$(14p)\qquad \sum |y| - 1 = (k\xi - 1) \left(\frac{1 - \xi^p}{1 - \xi} \right)^{\varkappa} \qquad \text{(ein Polynom)}.$$

Besonderes Interesse verdient der Fall $\mathfrak{U} = \mathfrak{L}' = \mathfrak{L}^2$. Hierfür ist $E = X$ (im endlichen Fall $\varkappa = k$), und die Erzeugung Y von $\mathfrak{L}'$, die zugleich Basis von $\mathfrak{L}'/\mathfrak{L}''$ ist, besteht nach den Sätzen 10 und 4 genau aus allen Produkten

$$(15)\qquad ((x_\alpha \circ x_\beta) \circ \cdots) \circ x_\gamma \quad \text{mit} \quad x_\alpha > x_\beta, \mathfrak{o}(x_\beta, \ldots, x_\gamma),$$

die mindestens zwei Faktoren enthalten. Im p-Fall kommen noch die Produkte

$$((x^p \circ x_\beta) \circ \cdots) \circ x_\gamma \quad \text{mit} \quad x > x_\beta, \mathfrak{o}(x_\beta, \ldots, x_\gamma)$$

hinzu.

Wiederholt man diesen Schritt $\mathfrak{L} \to \mathfrak{L}'$ auf $\mathfrak{L}' \to \mathfrak{L}''$, $\mathfrak{L}'' \to \mathfrak{L}'''$, usw., so kommt man zu einer Basis B_K von $\mathfrak{L}$, die nur aus Monomen besteht.

§ 4. d-Basen

$\mathfrak{L}$ sei ein freier LIEscher Ring mit der Erzeugung X und $x \to |x|$ die Abbildung in den zugehörigen monomialen Kegel. Für einen homogenen Unterring $\mathfrak{M}$ bezeichne $|\mathfrak{M}|$ die Gesamtheit der in $\mathfrak{M}$ auftretenden Beträge.

Vorgelegt sei eine absteigende Kette $\mathfrak{U}_n$ ($\mathfrak{U}_0 = \mathfrak{L}$) von Unterringen von $\mathfrak{L}$ mit den Eigenschaften:

α) $\mathfrak{L}/\mathfrak{U}_n$ ist torsionslos.

β) Für jede in X homogene freie Erzeugung X_n von $\mathfrak{U}_n$ ist $\mathfrak{U}_{n+1}$ homogen bezüglich des durch X_n bestimmten monomialen Kegels $\mathfrak{S}_n$.

γ) $\lim |\mathfrak{U}_n| = 0$ (bezüglich $\mathfrak{S}$).

$\mathfrak{L}_{(m)}$ bezeichne den Modul aller homogenen Elemente vom Grad m in X. Die wichtigsten Beispiele für solche Folgen $\mathfrak{U}_n$ sind

(Z) die absteigende Zentralreihe $\mathfrak{L}^n = \sum\limits_{m \geq n} \mathfrak{L}_{(m)}$ $(n = 1, 2, \ldots)$,

(K) die Kommutatorreihe $\mathfrak{L}, \mathfrak{L}^2, (\mathfrak{L}^2)^2, \ldots$.

Es werde hier nur die Gültigkeit der Bedingung β) im Falle (Z) nachgewiesen, da die übrigen Bedingungen für (Z) und (K) ganz offensichtlich erfüllt sind. Man konstruiere eine in X_n homogene Basis A von $\mathfrak{L}^n$, die dann nach Voraussetzung auch in X homogen ist. A enthält daher eine Basis B für den in X homogenen Modul $\mathfrak{L}^{n+1}$, und da A in X_n homogen ist, gilt dasselbe auch für $\mathfrak{L}^{n+1}$.

Satz 11. *Unter den oben genannten Voraussetzungen besitzt $\mathfrak{L}$ eine der Kette $\mathfrak{U}_n$ angepaßte d-Basis B, d.h.*

1. *B enthält eine Basis von $\mathfrak{U}_n$, deren irgendwie totalgeordnetes Komplement mit E_n bezeichnet sei,*

2. *in der durch E_n vermittelten Darstellung $d_{ik}^{\mathfrak{L}\to\mathfrak{U}_n}$ von $\mathfrak{L}$ durch Matrizen mit Koeffizienten aus $\mathfrak{U}_n$ ist*

$$X_n = \bigcup_k d_{0k}^{\mathfrak{L}\to\mathfrak{U}_n}(X)^* \subseteqq B$$

*eine freie homogene Erzeugung von $\mathfrak{U}_n$, wobei * Weglassung aller Nullen bedeute.*

Die sich aus der Kommutatorreihe ergebende d-Basis B_K habe ich 1942 in einem Vortrag an der Universität Berlin auf dem Wege über die Darstellung d_{ik} behandelt. Auf direktem Wege (ohne die Darstellung d_{ik}) ist PH. HALL 1950 auf die d-Basis B_Z gekommen, die sich hier aus der absteigenden Zentralreihe ergibt.

Beweis. In folgender Weise werden rekursiv totalgeordnete, in X homogene Relativbasen E_n von $\mathfrak{L}/\mathfrak{U}_n$ konstruiert ($E_0 = \emptyset$) derart, daß X_n eine freie homogene Erzeugung von $\mathfrak{U}_n$ ist. Hat man E_n schon konstruiert, so ist nach β) $\mathfrak{U}_{n+1}$ bezüglich des durch X_n bestimmten monomialen Kegels homogen. Ist A_τ eine Basis des homogenen Moduls $\mathfrak{U}_{n+1(\tau)}$ $(\tau \in \mathfrak{S}_n)$ und C_τ eine Basis des torsionslosen Moduls $\mathfrak{U}_{n(\tau)}/\mathfrak{U}_{n+1(\tau)}$, wobei in A_τ und C_τ *nach Möglichkeit* Elemente von X_n aufzunehmen sind, so ist $B_n = \bigcup\limits_\tau (A_\tau \cup C_\tau)$ eine bezüglich $\mathfrak{S}_n$ homogene Basis von $\mathfrak{U}_n$, die X_n und eine Basis von $\mathfrak{U}_{n+1}$ enthält. Nun ist $E_{n+1} = E_n \cup \bigcup C_\tau$ sicher eine bezüglich $\mathfrak{S}$ homogene Basis von $\mathfrak{L}/\mathfrak{U}_{n+1}$, für welche nach Satz 10 X_{n+1} eine freie homogene Erzeugung von $\mathfrak{U}_{n+1}$ ist. Damit sind die E_n mit den gewünschten Eigenschaften konstruiert.

Jetzt werde gezeigt, daß $B = \bigcup E_n$ eine homogene Basis von $\mathfrak{L}$ ist. Für gegebenes $\sigma \in \mathfrak{S}$ gibt es nach γ) ein n derart, daß $|\mathfrak{U}_n|$ keine Beträge $\leq \sigma$ enthält. Daher enthält E_n eine Basis von $\mathfrak{L}_{(s)}$. Da ferner die E_n eine aufsteigende Kette bilden, folgt die lineare Unabhängigkeit von B. Ferner liegt $B - E_n$ nach Konstruktion in $\mathfrak{U}_n$ und muß daher eine Basis von $\mathfrak{U}_n$ sein.

Nun werde $X_n \subseteqq \bigcup E_n$ nachgewiesen. Aus dem Transitivitätssatz für die Darstellungen d_{ik} folgt

$$X_{n+1} = d_{0\,k}^{\mathfrak{U}_n \to \mathfrak{U}_{n+1}}(X_n).$$

Dabei ist

$$d_{0\,k}^{\mathfrak{U}_n \to \mathfrak{U}_{n+1}}(X_n \cap \mathfrak{U}_{n+1}) = X_n \cap \mathfrak{U}_{n+1},$$

folglich

$$X_n \cap \mathfrak{U}_{n+1} \subseteqq X_{n+1}, \quad \text{und auch} \quad X_n \cap \mathfrak{U}_m \subseteqq X_m \qquad (m \geqq n).$$

Wegen γ) gilt nun $\bigcap \mathfrak{U}_n = 0$, daher liegt ein $x \in X_n$ in einem letzten $\mathfrak{U}_m$ $(m \geqq n)$ und muß demnach zu E_{m+1} gehören. Damit ist Satz 11 bewiesen. —

Von jetzt ab sei $\mathfrak{L}$ als *gewöhnlicher* LIEscher Ring vorausgesetzt, d.h. es liege nicht der p-Fall vor. Außerdem werde angenommen, daß stets $\mathfrak{U}_n^2 \subseteqq \mathfrak{U}_{n+1}$ erfüllt ist, wie z.B. bei den Folgen (Z) und (K). Dann lassen sich aus dem eben Bewiesenen noch einige Folgerungen ziehen. — In der totalen Ordnung der betrachteten d-Basis B sei stets $E_n < E_{n+1}$. Nun gilt:

Satz 12. *Jedes Element einer der Kette $\mathfrak{U}_n$ angepaßten totalgeordneten d-Basis von $\mathfrak{L}$ ist eindeutig ein „kanonisches Produkt"*

$$p_r = \big(((x \circ b_1) \circ \cdots) \circ b_{r-1}\big) \circ b_r \qquad (r = 0, 1, \ldots;\ p_0 = x \in X)$$

mit $b_1 \leqq \cdots \leqq b_r$ *und* $p_0 > b_1, \ldots, p_{r-1} > b_r$ (in B), *und umgekehrt gehört* p_r *unter diesen Bedingungen zu* B.

Eine totalgeordnete Basis B von $\mathfrak{L}$ mit dieser Eigenschaft werde **kanonisch** genannt.

Der *Beweis* von Satz 12 läßt sich auf mannigfache Weise durch Induktion führen oder indem man sich auf den engen Zusammenhang der Bildung p_r mit dem Prozeß $X \to X_n$ bezieht. Wir wählen folgende Beweisanordnung.

1. Es werde $r > 0$ und $b_r \in E_n$ angenommen und die Umkehrung durch Induktion nach n bewiesen. Von den $b_1, \ldots, b_r$ mögen genau ϱ Elemente in E_0 liegen. Für $\varrho = 0$ ist $b_1 \in \mathfrak{U}_1$, also $x \in \mathfrak{U}_1$ wegen der Bedingung $x > b_1$. Allgemein ist nach Satz 4, (20)

$$y = \big((x \circ b_1) \circ \cdots\big) \circ b_\varrho \in X_1$$

und nach Induktionsvoraussetzung bezüglich $\mathfrak{U}_1/\mathfrak{U}_{n+1}$ ist

$$z = \big((y \circ b_{\varrho+1}) \circ \cdots\big) \circ b_r \in B.$$

2. Es werde $z \in X_{n+1}$ $(n \geqq 0)$ angenommen und die eindeutige Zerlegbarkeit in ein kanonisches Produkt durch Induktion nach n bewiesen. Nach Induktionsvoraussetzung gibt es bezüglich $\mathfrak{U}_1/\mathfrak{U}_{n+1}$ eine eindeutige kanonische Zerlegung

$$z = \big((y \circ b_{\varrho+1}) \circ \cdots\big) \circ b_r \quad \text{mit} \quad y \in X_1,$$

und darin gestattet y bezüglich $\mathfrak{U}_0/\mathfrak{U}_1$, wie früher gezeigt wurde, eine eindeutige kanonische Zerlegung

$$y = \big((x \circ b_1) \circ \cdots\big) \circ b_\varrho.$$

Die hier auftretende Aufspaltung in zwei Schritte läßt sich nicht vermeiden, wie unter 1. gezeigt wurde. Daraus folgt die Eindeutigkeit von $z = p_r$.

In derselben Weise erhält man sofort durch Induktion den

Zusatz. $b_r \in E^n$ *ist gleichbedeutend* mit $p_r \in X^{n+1}$, $p_r \notin X^n$.

Eine einfache Umformung der Definition der kanonischen Basis B führt zu folgender Kennzeichnung von *arithmetischem Charakter*, die hier ohne Beweis angefügt werde.

Satz 13. *Eine totalgeordnete Basis B von $\mathfrak{L}$ ist genau dann kanonisch, wenn folgende drei Bedingungen zugleich erfüllt sind:*

1. *B enthält die freie Erzeugung X von $\mathfrak{L}$ und besteht nur aus Monomen in X.*

2. *Jedes Element aus $B - X$ ist innerhalb B eindeutig zerlegbar in $a \circ b$ mit $a > b$.*

3. *$a \circ b$ mit $a, b \in B, a > b$, gehört genau dann zu B, falls $a \in X$ oder*

$$a = a_1 \circ a_2, \quad a_1 > a_2 \leq b, \quad a_i \in B.$$

§ 5. Beispiele

$\mathfrak{L}$ sei der von x, y erzeugte freie LIEsche Ring über dem Koeffizientenbereich Γ der ganzen Zahlen. p sei eine Primzahl.

1. $\mathfrak{U} = \Gamma(px, py)$ ist frei, obwohl $\mathfrak{L}/\mathfrak{U}$ Torsion hat. Die Freiheit folgt aus der durch $x \to px$, $y \to py$ erzeugten Isomorphie.

2. $\mathfrak{U} = \Gamma(px, py, px \circ y)$ ist nicht frei, da $px \circ y$ im Faktorkommutatorring $\mathfrak{U}/\mathfrak{U}'$ die Ordnung p hat.

3. $\mathfrak{U} = \Gamma(x, py, y + x \circ y)$ ist nicht frei, obwohl $\mathfrak{U}/\mathfrak{U}'$ keine Torsion hat. Dies soll bewiesen werden. Wegen

$$p \cdot (y + x \circ y) = py + x \circ py \equiv py \bmod \mathfrak{U}'$$

wird $\mathfrak{U}/\mathfrak{U}'$ linear von x, $y + x \circ y$ erzeugt und ist daher torsionslos.

Angenommen, $\mathfrak{U}$ wäre ein freier Unterring. Dann müßte $\mathfrak{U}$ von zwei Elementen A, B erzeugt werden, weil rational gerechnet $\mathfrak{U}$ mit $\mathfrak{L}$ zusammenfällt. Durch etwaige unimodulare Ersetzung von A, B läßt sich erreichen, daß deren Leitglieder (homogene Glieder höchsten Grades) linear unabhängig sind. Nun sieht man, daß A und B vom Grad 1 sind, denn sonst wäre nicht x und py in $\Gamma(A, B)$ enthalten. Da $y + x \circ y$ nicht der additiven Gruppe (x, py) angehört, gilt die Modulrelation

$$(x, y) \geqq (A, B) > (x, py).$$

Nun ist $(x, y)/(x, py)$ einfach, folglich $(A, B) = (x, y)$, $\mathfrak{U} = \mathfrak{L}$, was aber sicher mod $p\mathfrak{L}$ falsch ist.

Hamburg, Mathematisches Seminar der Universität

(Eingegangen am 26. März 1955)

EBEL, I.
Math. Zeitschr. Bd. 64, S. 217—228 (1956)

Analytische Bestimmung der Darstellungsanzahlen natürlicher Zahlen durch spezielle ternäre quadratische Formen mit Kongruenzbedingungen

Von
ILSE EBEL

Einleitung

In der vorliegenden Arbeit werden nach den Methoden von H. PETERSSON [1] Darstellungsanzahlen natürlicher Zahlen durch spezielle ternäre quadratische Formen mit Kongruenzbedingungen für die ganzzahligen Variablen ermittelt. Die behandelten Fälle sind in dem folgenden Schema enthalten:

Form	Kongruenzbedingungen
$Q_1 = n_1^2 + n_2^2 + n_3^2$	(a) $n_1 \equiv 0 \bmod 4,\ n_2 \equiv 0 \bmod 4,\ n_3 \equiv 1 \bmod 4,$
	(b) $n_1 \equiv 1 \bmod 4,\ n_2 \equiv 2 \bmod 4,\ n_3 \equiv 2 \bmod 4,$
$Q_2 = 3n_1^2 + n_2^2 + n_3^2$	(c) $n_1 \equiv 0 \bmod 2,\ n_2 \equiv 0 \bmod 6,\ n_3 \equiv 1 \bmod 6,$
	(d) $n_1 \equiv 1 \bmod 2,\ n_2 \equiv 1 \bmod 6,\ n_3 \equiv 3 \bmod 6,$
	(e) $n_1 \equiv 0 \bmod 2,\ n_2 \equiv 2 \bmod 6,\ n_3 \equiv 3 \bmod 6,$
	(f) $n_1 \equiv 0 \bmod 2,\ n_2 \equiv 0 \bmod 6,\ n_3 \equiv 2 \bmod 6,$
	(g) $n_1 \equiv 1 \bmod 2,\ n_2 \equiv 0 \bmod 6,\ n_3 \equiv 1 \bmod 6,$
	(h) $n_1 \equiv 1 \bmod 2,\ n_2 \equiv 2 \bmod 6,\ n_3 \equiv 3 \bmod 6.$

Die Untersuchung verläuft ähnlich wie in den von H. MAASS [2] behandelten Fällen.

Der Ansatz benutzt die einfachen Theta-Reihen

$$\vartheta_\lambda(\tau, h, N) = \sum_{m \equiv h \bmod N} m^\lambda e^{\frac{\pi i m^2 \tau}{N}}, \quad \lambda = 0 \text{ oder } 1, \tag{1}$$

die in [3] untersucht worden sind. Gewisse Produkte je dreier solchen Reihen mit $\lambda = 0$ liefern die erzeugenden Potenzreihen für die gesuchten Anzahlfunktionen. Die Bestimmung der Darstellungsanzahlen beruht auf dem klassischen Verfahren, nach dem sich jede ganze Modulform (hier die erwähnten Produkte von Theta-Reihen) mit Hilfe von Reihen vom Eisensteinschen Typ additiv auf eine ganze Spitzenform reduzieren läßt. Die benötigten Eisenstein-Reihen ergeben sich aus dem allgemeinen Ansatz (vgl. [1])

$$\varphi(\tau, s) = \sum_{M \in \mathfrak{S}(A, \Gamma)} \frac{1}{\sigma(A, L)\, v(L)\, (m_1\tau + m_2)^r\, |m_1\tau + m_2|^s} \tag{2}$$

durch Anwendung des Heckeschen Summationsverfahrens.

Die in den behandelten Fällen vorliegende funktionentheoretische Situation ist vollständig übersehbar und sehr einfach: Für alle acht auftretenden

Produkte aus Theta-Reihen (1) ist die genaue Transformationsgruppe bekannt. Daraus ergibt sich die Kenntnis der jeweils zugehörigen Eisenstein-Reihe (2) und die Möglichkeit, ihre Fourier-Koeffizienten durch Klassenzahlen imaginär-quadratischer Körper auszudrücken. Es zeigt sich andererseits, daß die ganzen Spitzenformen, zu denen man durch die oben genannte klassische Reduktion gelangt, einer jeweils eingliedrigen, durch eine Theta-Reihe (1) mit $\lambda = 1$ aufgespannten Schar angehören. Damit liegt hier der äußerst ungewöhnliche Fall vor, daß die Fourier-Koeffizienten der Spitzenformen ein sehr viel einfacheres Bildungsgesetz befolgen als die der Eisenstein-Reihen.

Zur Durchführung der Untersuchung werden zunächst in § 1 die auftretenden Formenklassen, Multiplikatorsysteme, Spitzen (eines Fundamentalbereiches) und Drehreste, die aus Theta-Reihen (1) gebildeten Formen und die zu den Spitzen mit verschwindendem Drehrest gehörigen Ansätze (2) zusammengestellt. § 2 enthält die Behandlung der Reihen (2) nach dem Heckeschen Summationsverfahren, welches die Nullwerte $\varphi(\tau, 0; v, \zeta)$ (v Multiplikatorsystem, ζ rationale Spitze) dieser Reihen als ganze Modulformen in τ erscheinen läßt und zugleich deren Fourier-Koeffizienten durch Klassenzahlen imaginär-quadratischer Körper auszudrücken lehrt. Danach lassen sich (§ 3) leicht die zwischen den Formen bestehenden linearen Relationen angeben, die schließlich die gesuchten Ausdrücke für die Darstellungsanzahlen liefern.

Diese Ausdrücke enthalten in dem Spezialfall, daß die darzustellende natürliche Zahl n ein Quadrat ist, nur noch elementare Funktionen, weil dann Diskriminante, Klassenzahl und Einheitswurzelanzahl des eingehenden quadratischen Zahlkörpers sofort angebbar sind.

Im allgemeinen, d.h. stets dann, wenn n kein Quadrat ist, fallen die von den Theta-Reihen (1) mit $\lambda = 1$ herrührenden Zusatzglieder in den Ausdrücken für die Darstellungsanzahlen fort. Die Darstellungsanzahlen werden dann rein durch die Koeffizienten der Eisenstein-Reihen gegeben. Damit ist für die Nicht-Quadratzahlen n die Situation hier die gleiche, wie sonst für alle natürlichen n in den Fällen, in denen die auftretenden Formenscharen keine nicht identisch verschwindenden Spitzenformen enthalten.

Die vorliegende Untersuchung wurde von Herrn K. WOHLFAHRT in Münster durchgesehen und zum Druck vorbereitet. Von ihm stammen die zusätzlichen Bemerkungen am Schluß der Arbeit (nach der Zusammenstellung der Formeln für die Darstellungsanzahlen A, B).

§ 1

I. Die Linearschar der ganzen Modulformen $\{\Gamma_0[8], -\frac{3}{2}, v_0\}$ mit

$$v_0(L) = e^{\frac{\pi i}{4}} \left(\frac{\gamma}{\delta}\right)_* e^{\frac{\pi i}{4}\delta(\beta-1)} \quad \text{für} \quad L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0[8]$$

hat den Rang 2. Die Drehreste $\varkappa$ in den Spitzen ζ eines Fundamentalbereiches von $\Gamma_0[8]$ sind

ζ	∞	0	$\frac{1}{2}$	$\frac{1}{4}$
$\varkappa$	$\frac{1}{8}$	0	$\frac{1}{4}$	$\frac{1}{8}$

$\{\Gamma_0[8], -\frac{3}{2}, v_0\}$ enthält die ganzen Modulformen

$$\vartheta_1(\tau, 1, 4),$$
$$\Theta_0\left(\tau\left|\begin{matrix}0 & 0 & 1\\ 4 & 4 & 4\end{matrix}\right.\right) = \vartheta_0^2(\tau, 0, 4)\,\vartheta_0(\tau, 1, 4),$$
$$\Theta_0\left(\tau\left|\begin{matrix}1 & 2 & 2\\ 4 & 4 & 4\end{matrix}\right.\right) = \vartheta_0(\tau, 1, 4)\,\vartheta_0^2(\tau, 2, 4),$$

deren erste mit $\eta^3(\tau) = \sqrt[8]{\Delta(\tau)}$ übereinstimmt, wie man etwa aus der Jacobischen Identität findet.

Zur Spitze $\zeta = 0$ ergibt sich aus (2) der Ansatz

$$\varphi(\tau, s; v_0, 0) = 2 \sum_{\substack{m_1>0,\, m_1\equiv 1 \bmod 2\\ (m_1, m_2)=1}} \left(\frac{m_2}{m_1}\right) \frac{e^{-\frac{\pi i}{4}(m_1 m_2 + m_1 + 1)}}{(m_1\tau + m_2)^{\frac{3}{2}} |m_1\tau + m_2|^s}.$$

II. Die Linearschar der ganzen Modulformen $\{\Gamma_0[12], -\frac{3}{2}, v_1\}$ mit

$$v_1(L) = e^{\frac{\pi i}{4}} \left(\frac{2\gamma}{\delta}\right)_* e^{\frac{\pi i}{12}\delta(2\beta - 3)} \quad \text{für} \quad L = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \Gamma_0[12]$$

hat den Rang 3. Die Drehreste $\varkappa$ in den Spitzen ζ eines Fundamentalbereiches von $\Gamma_0[12]$ sind

ζ	∞	0	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$
$\varkappa$	$\frac{1}{12}$	0	0	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{3}$

$\{\Gamma_0[12], -\frac{3}{2}, v_1\}$ enthält die ganzen Formen

$$\vartheta_1(\tau, 1, 6),$$
$$\Theta_0\left(\tau\left|\begin{matrix}0 & 0 & 1\\ 2 & 6 & 6\end{matrix}\right.\right) = \vartheta_0(\tau, 0, 2)\,\vartheta_0(\tau, 0, 6)\,\vartheta_0(\tau, 1, 6),$$
$$\Theta_0\left(\tau\left|\begin{matrix}1 & 1 & 3\\ 2 & 6 & 6\end{matrix}\right.\right) = \vartheta_0(\tau, 1, 2)\,\vartheta_0(\tau, 1, 6)\,\vartheta_0(\tau, 3, 6),$$
$$\Theta_0\left(\tau\left|\begin{matrix}0 & 2 & 3\\ 2 & 6 & 6\end{matrix}\right.\right) = \vartheta_0(\tau, 0, 2)\,\vartheta_0(\tau, 2, 6)\,\vartheta_0(\tau, 3, 6),$$

deren erste eine Spitzenform ist.

Zur Spitze $\zeta = 0$ ergibt sich aus (2) der Ansatz:

$$\varphi(\tau, s; v_1, 0) = 2 \sum_{\substack{m_1>0,\, m_1\equiv \pm 1 \bmod 6\\ (m_1, m_2)=1}} \left(\frac{2m_2}{m_1}\right) \frac{e^{-\frac{\pi i}{12}(2m_1 m_2 + 3m_1 + 3)}}{(m_1\tau + m_2)^{\frac{3}{2}} |m_1\tau + m_2|^s}$$

und zur Spitze $\zeta = \frac{1}{2}$:

$$\varphi\left(\tau, s; v_1, \frac{1}{2}\right) = 2 \sum_{\substack{m_1>0,\, m_1\equiv \pm 2 \bmod 12\\ (m_1, m_2)=1}} \left(\frac{m_2}{\frac{1}{2}m_1}\right) \frac{e^{-\frac{\pi i}{24}(m_1 m_2 + 3m_1 + 8)}}{(m_1\tau + m_2)^{\frac{3}{2}} |m_1\tau + m_2|^s}.$$

III. Die entsprechenden Angaben für $\{\Gamma_0[12], -\frac{3}{2}, v_2\}$ mit

$$v_2(L) = e^{\frac{\pi i}{4}} \left(\frac{2\gamma}{\delta}\right)_* e^{\frac{\pi i}{12}\delta(8\beta-3)} \quad \text{für} \quad L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0[12]$$

lauten: Rang der Linearschar $= 3$,

ζ	∞	0	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$
$\varkappa$	$\frac{1}{8}$	0	$\frac{1}{4}$	$\frac{1}{8}$	0	$\frac{1}{12}$

,

$$\vartheta_1(\tau, 2, 6), \qquad \text{(Spitzenform)},$$

$$\Theta_0\left(\tau \begin{vmatrix} 0 & 0 & 2 \\ 2 & 6 & 6 \end{vmatrix}\right) = \vartheta_0(\tau, 0, 2)\,\vartheta_0(\tau, 0, 6)\,\vartheta_0(\tau, 2, 6),$$

$$\Theta_0\left(\tau \begin{vmatrix} 1 & 0 & 1 \\ 2 & 6 & 6 \end{vmatrix}\right) = \vartheta_0(\tau, 1, 2)\,\vartheta_0(\tau, 0, 6)\,\vartheta_0(\tau, 1, 6),$$

$$\Theta_0\left(\tau \begin{vmatrix} 1 & 2 & 3 \\ 2 & 6 & 6 \end{vmatrix}\right) = \vartheta_0(\tau, 1, 2)\,\vartheta_0(\tau, 2, 6)\,\vartheta_0(\tau, 3, 6),$$

$$\varphi(\tau, s; v_2, 0) = 2 \sum_{\substack{m_1 > 0,\, m_1 \equiv \pm 1 \bmod 6 \\ (m_1, m_2) = 1}} \left(\frac{2m_2}{m_1}\right) \frac{e^{-\frac{\pi i}{12}(8m_1m_2 + 3m_1 + 3)}}{(m_1\tau + m_2)^{\frac{3}{2}} |m_1\tau + m_2|^s},$$

$$\varphi\left(\tau, s; v_2, \frac{1}{4}\right) = 2 \sum_{\substack{m_1 > 0,\, m_1 \equiv \pm 4 \bmod 12 \\ (m_1, m_2) = 1}} \left(\frac{2m_1}{m_2}\right) \frac{e^{-\frac{\pi i}{12}(2m_1m_2 + 9m_2 - 1)}}{(m_1\tau + m_2)^{\frac{3}{2}} |m_1\tau + m_2|^s}.$$

§ 2

Die auftretenden Reihen $\varphi(\tau, s; v, \zeta)$ haben die Gestalt

$$\varphi(\tau, s; v, \zeta) = 2 \sum_{\substack{m_1 \in \mathfrak{M} \\ (m_1, m_2) = 1}} \frac{\varepsilon(m_1, m_2)}{(m_1\tau + m_2)^r |m_1\tau + m_2|^s},$$

wo $\mathfrak{M}$ eine gewisse Menge natürlicher Zahlen ist und

$$\varepsilon(m_1, m_2 + t m_1) = \varepsilon(m_1, m_2)$$

mit einer natürlichen Zahl t gilt, die als minimal mit dieser Eigenschaft angenommen werden mag und dann eindeutig durch ε bestimmt ist. Mit Hilfe der Formel

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+\omega)^r |m+\omega|^s} = \sum_{n=-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{e^{-2\pi i n x}\,dx}{(x+\omega)^r |x+\omega|^s}, \qquad \mathfrak{Im}\,\omega > 0,$$

gewinnt man daraus die Entwicklung

$$\varphi(\tau, s; v, \zeta) = \frac{2}{t^{r+s}} \sum_{n=-\infty}^{\infty} T_n(s; \mathfrak{M}, \varepsilon) A_n\left(s, \frac{\tau}{t}\right),$$

wo

$$A_n(s, \omega) = \int_{-\infty}^{\infty} \frac{e^{-2\pi i n x}\, dx}{(x+\omega)^r |x+\omega|^s},$$

$$T_n(s; \mathfrak{M}, \varepsilon) = \sum_{m \in \mathfrak{M}} \frac{1}{m^{r+s}} \sum_{\substack{j \bmod tm \\ (j,m)=1}} \varepsilon(m, j)\, e^{\frac{2\pi i n j}{tm}}$$

ist.

Hier braucht nur der Fall $r = \frac{3}{2}$ betrachtet zu werden. Dann gilt nach [2]:

1. $A_n(s, \omega)$ ist ganze Funktion in s für $n \neq 0$,

2. $A_0(s, \omega)$ ist regulär für $\Re s > -\frac{1}{2}$,

3. $A_n(s, \omega) = O(e^{-\delta |n|})$ für $|n| \to \infty$ mit passendem $\delta > 0$, gleichmäßig in s, wenn s in einem beschränkten Bereich variiert, und

$$4.\ A_n(0, \omega) = \begin{cases} 0, \text{ falls } n \leq 0, \\ \dfrac{(2\pi)^{\frac{3}{2}} e^{-\frac{3\pi i}{4}} n^{\frac{1}{2}} e^{2\pi i n \omega}}{\Gamma(\frac{3}{2})}, \text{ falls } n > 0. \end{cases}$$

Die in $T_n(s; \mathfrak{M}, \varepsilon)$ auftretenden Summen über j lassen sich auf das Symbol

$$K(m, n) = e^{\frac{\pi i}{4}(m-1)} \sum_{\substack{j \bmod m \\ (j,m)=1}} \left(\frac{j}{m}\right) e^{\frac{2\pi i n j}{m}}$$

zurückführen, welches für positive, ganze, ungerade m und ganze n erklärt ist und

$$K(m_1 m_2, n) = K(m_1, n)\, K(m_2, n) \quad \text{für} \quad (m_1, m_2) = 1$$

erfüllt. Überdies besitzt $K(m, n)$ die folgenden Werte, wenn m eine ungerade Primzahlpotenz ist (vgl. [1]):

$$K(p^\nu, n) = \begin{cases} 0, & \text{falls} \quad p^{\nu-1} \nmid n, \\ p^{\nu-\frac{1}{2}} \left(\dfrac{\frac{2n}{p^{\nu-1}}}{p}\right), & \text{falls} \quad p^{\nu-1} | n,\ p^\nu \nmid n,\ \nu \equiv 1 \bmod 2, \\ 0, & \text{falls} \quad p^{\nu-1} | n,\ p^\nu | n,\ \nu \equiv 1 \bmod 2, \\ -p^{\nu-1}, & \text{falls} \quad p^{\nu-1} | n,\ p^\nu \nmid n,\ \nu \equiv 0 \bmod 2, \\ \varphi(p^{\nu-1}), & \text{falls} \quad p^{\nu-1} | n,\ p^\nu | n,\ \nu \equiv 0 \bmod 2. \end{cases}$$

Die Reduktion liefert in den fünf betrachteten Fällen:

1. $\mathfrak{M} = \{m \mid m > 0,\ m \equiv 1 \bmod 2\},\ t = 8$:

$$\sum_{\substack{j \bmod 8m \\ (j,m)=1}} \left(\frac{j}{m}\right) e^{-\frac{\pi i}{4}(mj+m+1)+\frac{2\pi i n j}{8m}} = \begin{cases} 8\, e^{\frac{3\pi i}{2}} \left(\frac{-2}{m}\right) K(m,n), & \text{falls } n \equiv 1 \bmod 8, \\ 0, \text{ sonst.} \end{cases}$$

2. $\mathfrak{M} = \{m \mid m > 0,\ m \equiv \pm 1 \bmod 6\},\ t = 12$:

$$\sum_{\substack{j \bmod 12m \\ (j,m)=1}} \left(\frac{2j}{m}\right) e^{-\frac{\pi i}{12}(2mj+3m+3)+\frac{2\pi i n j}{12m}} = \begin{cases} 12\, e^{\frac{3\pi i}{2}} \left(\frac{-6}{m}\right) K(m,n), & \text{falls } n \equiv 1 \bmod 12, \\ 0, \text{ sonst.} \end{cases}$$

3. $\mathfrak{M} = \{m \mid m > 0,\ m \equiv \pm 2 \bmod 12\},\ t = 12$:

$$\sum_{\substack{j \bmod 12m \\ (j,m)=1}} \left(\frac{j}{\frac{1}{2}m}\right) e^{-\frac{\pi i}{24}(mj+3m+8)+\frac{2\pi i n j}{12m}} = \begin{cases} 12\,(-1)^{\frac{n-1}{4}}\, e^{-\frac{7\pi i}{12}} \left(\frac{-6}{\frac{1}{2}m}\right) K\left(\frac{m}{2}, n\right), & \text{falls } n \equiv 1 \bmod 12, \\ 0, \text{ sonst.} \end{cases}$$

4. $\mathfrak{M} = \{m \mid m > 0,\ m \equiv \pm 1 \bmod 6\},\ t = 3$:

$$\sum_{\substack{j \bmod 3m \\ (j,m)=1}} \left(\frac{2j}{m}\right) e^{-\frac{\pi i}{12}(8mj+3m+3)+\frac{2\pi i n j}{3m}} = \begin{cases} 3\, e^{\frac{3\pi i}{2}} \left(\frac{-6}{m}\right) K(m,n), & \text{falls } n \equiv 1 \bmod 3, \\ 0, \text{ sonst.} \end{cases}$$

5. $\mathfrak{M} = \{m \mid m > 0,\ m \equiv \pm 4 \bmod 12\},\ t = 6$:

Es sei $m = 2^h \cdot m_0,\ m_0 \equiv \pm 1 \bmod 6,\ h \geq 2$:

$$\sum_{\substack{j \bmod 6m \\ (j,m)=1}} \left(\frac{2m}{j}\right) e^{-\frac{\pi i}{12}(2mj+9j-1)+\frac{2\pi i n j}{6m}} = (-1)^{h+1} \cdot 2^h \cdot 3 \cdot e^{\frac{\pi i}{12}} \left(\frac{-3}{m_0}\right) K(m_0, n)\, \Delta(h,n).$$

Dabei ist für ganze h, n und $h \geq 2$

$$\Delta(h,n) = \delta\left(\frac{n+1}{3}\right) \delta\left(\frac{B+h+1}{2}\right) \cos\frac{B\pi}{4},$$

$$B = B(h,n) = \frac{n}{2^{h-2}} - 1,$$

$$\delta(x) = \begin{cases} 1, & \text{falls } x \text{ ganz rational,} \\ 0, & \text{sonst.} \end{cases}$$

$\Delta(h, n)$ verschwindet daher für ungerade n. Die Summen

$$H_n(s) = \sum_{h \geq 2} \frac{(-1)^{h+1} \Delta(h, n)}{2^{h(\frac{1}{2}+s)}}, \quad n \text{ ganz},$$

sind nur formal unendlich, da die $h \geq 2$, für die $\Delta(h, n) \neq 0$, eine nur von n abhängige obere Schranke besitzen.

In den genannten fünf Fällen ergeben sich nun die Produktentwicklungen:

$$1.\ T_n(s; \mathfrak{M}, \varepsilon) = 8 e^{\frac{3\pi i}{2}} \prod_{p>2} \left(\sum_{\nu=0}^{\infty} \left(\frac{-2}{p^\nu} \right) \frac{K(p^\nu, n)}{p^{\nu(\frac{3}{2}+s)}} \right), \qquad n \equiv 1 \bmod 8,$$

$$2.\ T_n(s; \mathfrak{M}, \varepsilon) = 12 e^{\frac{3\pi i}{2}} \prod_{p>3} \left(\sum_{\nu=0}^{\infty} \left(\frac{-6}{p^\nu} \right) \frac{K(p^\nu, n)}{p^{\nu(\frac{3}{2}+s)}} \right), \qquad n \equiv 1 \bmod 12,$$

$$3.\ T_n(s; \mathfrak{M}, \varepsilon) = \frac{12}{2^{\frac{3}{2}+s}} e^{-\frac{7\pi i}{12}} (-1)^{\frac{n-1}{4}} \prod_{p>3} \left(\sum_{\nu=0}^{\infty} \left(\frac{-6}{p^\nu} \right) \frac{K(p^\nu, n)}{p^{\nu(\frac{3}{2}+s)}} \right), \quad n \equiv 1 \bmod 12,$$

$$4.\ T_n(s; \mathfrak{M}, \varepsilon) = 3 e^{\frac{3\pi i}{2}} \prod_{p>3} \left(\sum_{\nu=0}^{\infty} \left(\frac{-6}{p^\nu} \right) \frac{K(p^\nu, n)}{p^{\nu(\frac{3}{2}+s)}} \right), \qquad n \equiv 1 \bmod 3,$$

$$5.\ T_n(s; \mathfrak{M}, \varepsilon) = 3 e^{\frac{\pi i}{12}} H_n(s) \prod_{p>3} \left(\sum_{\nu=0}^{\infty} \left(\frac{-3}{p^\nu} \right) \frac{K(p^\nu, n)}{p^{\nu(\frac{3}{2}+s)}} \right), \qquad n \equiv -1 \bmod 3.$$

Im letzten Fall kann man wegen $H_n(s) = 0$ für $n \equiv 1 \bmod 2$ $2n$ statt n schreiben und findet wegen

$$\left(\frac{2}{p^\nu} \right) K(p^\nu, 2n) = K(p^\nu, n) \qquad \text{für} \qquad p > 2:$$

$$T_{2n}(s; \mathfrak{M}, \varepsilon) = 3 e^{\frac{\pi i}{12}} H_{2n}(s) \prod_{p>3} \left(\sum_{\nu=0}^{\infty} \left(\frac{-6}{p^\nu} \right) \frac{K(p^\nu, n)}{p^{\nu(\frac{3}{2}+s)}} \right), \qquad n \equiv 1 \bmod 3.$$

In dem Produkt

$$P_n(s) = \prod_{p>2} \psi_p^{(n)}(s), \qquad \psi_p^{(n)}(s) = \sum_{\nu=0}^{\infty} \left(\frac{-2}{p^\nu} \right) \frac{K(p^\nu, n)}{p^{\nu(\frac{3}{2}+s)}},$$

sind die Faktoren $\psi_p^{(n)}(s)$ mit $p > 2$, $p \nmid n$:

$$\psi_p^{(n)}(s) = \frac{1 - p^{-(2+2s)}}{1 - \left(\frac{d}{p} \right) p^{-(1+s)}}, \qquad d = d(-n),$$

wo d die Diskriminante des quadratischen Zahlkörpers $\mathrm{P}(\sqrt{-n})$ bedeutet. Daher ist

$$P_n(s) = \frac{L(1+s, \chi_d)}{\zeta(2+2s)} U_n(s),$$

wo $L(s, \chi)$ die Dirichletsche L-Reihe zum (eigentlichen) Charakter χ, χ_d denjenigen Charakter, der für positive Argumente x mit $\left(\frac{d}{x}\right)$ übereinstimmt, und $\zeta(s)$ die ζ-Funktion des rationalen Zahlkörpers bedeuten. Dabei ist $U_n(s)$ das endliche Produkt

$$U_n(s) = \frac{1 - \left(\frac{d}{2}\right) 2^{-(1+s)}}{1 - 2^{-(2+2s)}} \prod_{\substack{p>2 \\ p|d}} \frac{\psi_p^{(n)}(s)}{1 - p^{-(2+2s)}} \prod_{\substack{p>2 \\ p|n \\ p\nmid d}} \frac{\psi_p^{(n)}(s)}{1 + \left(\frac{d}{p}\right) p^{-(1+s)}}, \qquad d = d(-n),$$

mit

$$\frac{\psi_p^{(n)}(s)}{1 - p^{-(2+2s)}} = \sum_{\nu=0}^{\frac{h-1}{2}} p^{-\nu(1+2s)} \qquad \text{für} \quad p > 2,\ p|d,$$

$$\frac{\psi_p^{(n)}(s)}{1 + \left(\frac{d}{p}\right) p^{-(1+s)}} = \left(1 - \left(\frac{d}{p}\right) p^{-(1+s)}\right) \sum_{\nu=0}^{\frac{h}{2}-1} p^{-\nu(1+2s)} + p^{-\frac{h}{2}(1+2s)}$$
$$\text{für} \quad p > 2,\ p|n,\ p\nmid d,$$

wo h durch $p^h | n$, $p^{h+1} \nmid n$ bestimmt ist.

Das andere Produkt

$$Q_n(s) = \prod_{p>3} \left(\sum_{\nu=0}^{\infty} \left(\frac{-6}{p^\nu}\right) \frac{K(p^\nu, n)}{p^{\nu(\frac{3}{2}+s)}} \right),$$

welches nur für $(n, 3) = 1$ auftritt, läßt sich wegen

$$\left(\frac{3}{p^\nu}\right) K(p^\nu, n) = K(p^\nu, 3n), \qquad p > 3,$$

auf $P_n(s)$ zurückführen, wobei man findet

$$Q_n(s) = \frac{L(1+s, \chi_d)}{\zeta(2+2s)} \cdot \frac{U_{3n}(s)}{1 - 3^{-(2+2s)}}, \qquad (n, 3) = 1,$$

wo aber jetzt $d = d(-3n)$ in χ_d zu verstehen ist.

Beachtet man, daß in allen hier betrachteten Fällen nur solche n auftreten, für die $d \neq 1$ ist, so folgt, daß sämtliche L-Reihen im Punkte $s = 0$ regulär sind. Ferner gilt ersichtlich etwa für

$$-\tfrac{1}{4} \leq \Re s \leq 1,$$
$$-1 \leq \Im s \leq 1$$

gleichmäßig in s:

$$T_n(s; \mathfrak{M}, \varepsilon) = O(|n|^\varkappa), \qquad (|n| \to \infty),$$

mit einer geeigneten Konstanten $\varkappa > 0$. Im Fall 5. oben beachte man dazu $H_{2n}(s) = O(\log|n|)$. In Verbindung mit den O-Abschätzungen für die $A_n(s, \omega)$ ergibt sich, daß sämtliche Funktionen $\varphi(\tau, s; v, \zeta)$ bei $s = 0$ regulär sind. Damit ist die analytische Fortsetzung geleistet.

Die Koeffizienten der Nullwerte $\varphi(\tau, 0; v, \zeta)$ wachsen nur wie eine feste Potenz von n. Daher wachsen diese Funktionen bei Annäherung an die reelle Achse gleichmäßig in x $(\tau = x + iy)$ nur wie eine feste Potenz von y, woraus geschlossen werden kann, daß sie ganze Modulformen der Schar $\{\Gamma_0[8], -\frac{3}{2}, v_0\}$ bzw. der Schar $\{\Gamma_0[12], -\frac{3}{2}, v_\mu\}$ $(\mu = 1$ oder $2)$ sind.

Unter Einführung der Klassenzahl $h(d)$ des Körpers $P(\sqrt{d})$ vermittels

$$L(1, \chi_d) = \frac{2\pi h(d)}{w\sqrt{|d|}}, \qquad d < 0,$$

wo w die Anzahl der Einheitswurzeln in diesem Körper bedeutet, mit der Abkürzung

$$B_n(d) = \frac{6h(d)}{w\sqrt{|d|}}\sqrt{n}, \qquad n > 0,$$

und nach einer Änderung der konstanten Vorfaktoren lauten die Fourier-Entwicklungen dieser Nullwerte, die jetzt mit

$$\varphi(\tau; v, \zeta) = \text{const} \cdot \varphi(\tau, 0; v, \zeta)$$

bezeichnet werden, folgendermaßen:

1. $\varphi(\tau; v_0, 0) = \sum\limits_{n>0,\, n\equiv 1 \bmod 8} B_n(d)\, U(n)\, e^{\frac{2\pi i n\tau}{8}}, \qquad d = d(-n),$

2. $\varphi(\tau; v_1, 0) = \frac{1}{2}\sqrt{3} \sum\limits_{n>0,\, n\equiv 1 \bmod 12} B_n(d)\, U(3n)\, e^{\frac{2\pi i n\tau}{12}}, \qquad d = d(-3n),$

3. $\varphi(\tau; v_1, \frac{1}{2}) = \frac{1}{2}\sqrt{3} \sum\limits_{n>0,\, n\equiv 1 \bmod 12} (-1)^{\frac{n-1}{4}} B_n(d)\, U(3n)\, e^{\frac{2\pi i n\tau}{12}},$
$d = d(-3n),$

4. $\varphi(\tau; v_2, 0) = \frac{1}{2}\sqrt{3} \sum\limits_{n>0,\, n\equiv 1 \bmod 3} B_n(d)\, U(3n)\, e^{\frac{2\pi i n\tau}{3}}, \qquad d = d(-3n),$

5. $\varphi(\tau; v_2, \frac{1}{4}) = \frac{1}{2}\sqrt{3} \sum\limits_{n>0,\, n\equiv 1 \bmod 3} \sqrt{2}\, H(2n)\, B_n(d)\, U(3n)\, e^{\frac{2\pi i n\tau}{3}},$
$d = d(-3n).$

Dabei wurden die Nullwerte der Funktionen $H_n(s)$, $U_n(s)$ durch

$$H(n) = H_n(0), \qquad U(n) = U_n(0)$$

bezeichnet. Die Summen $H_n(0)$ lassen sich nun in geschlossener Form darstellen. Schreibt man nämlich für $n \equiv -1 \bmod 3$

$$\sqrt{8}\, H_n(0) = \sum_{\nu=0}^{\infty} \frac{\Delta(3+2\nu, n)}{2^\nu} - \sum_{\nu=0}^{\infty} \frac{\sqrt{2}\,\Delta(2+2\nu, n)}{2^\nu}$$

und sind zu n die natürlichen Zahlen n_0, σ erklärt durch

$$n = 4^\sigma \cdot n_0, \qquad 4 \nmid n_0,$$

so ergibt sich

$$\sqrt{2}\,H(n) = \delta\left(\frac{n-2}{6}\right)\left[\frac{\varrho(n_0)}{2^{\sigma+1}} - 1\right]$$

mit

$$\varrho(n_0) = \delta\left(\frac{n_0-2}{8}\right)(-1)^{\frac{n_0-2}{8}} - \delta\left(\frac{n_0}{2}\right)\left(\frac{2}{n_0-1}\right) - 2(-1)^{n_0} + 4.$$

$\varrho(n_0)$ hängt nur ab von der Restklasse n_0 mod 16, und zwar nach dem Schema

n_0 mod 16	1	2	3	5	6	7	9	10	11	13	14	15
$\varrho(n_0)$	6	2	6	6	3	6	6	0	6	6	3	6

§ 3

Die in § 1 genannten linearen Scharen ganzer Modulformen lassen sich jetzt beziehungsweise erzeugen

$S[\{\Gamma_0[8], -\frac{3}{2}, v_0\}]$ durch $\varphi(\tau; v_0, 0)$ und $\vartheta_1(\tau, 1, 4)$,

$S[\{\Gamma_0[12], -\frac{3}{2}, v_1\}]$ durch $\varphi(\tau; v_1, 0)$, $\varphi(\tau; v_1, \frac{1}{2})$ und $\vartheta_1(\tau, 1, 6)$,

$S[\{\Gamma_0[12], -\frac{3}{2}, v_2\}]$ durch $\varphi(\tau; v_2, 0)$, $\varphi(\tau; v_2, \frac{1}{4})$ und $\vartheta_1(\tau, 2, 6)$.

Die Berechnung der ersten zwei bzw. drei Koeffizienten liefert dann für die übrigen in § 1 genannten Formen die Darstellungen

$$2\Theta_0\left(\tau\left|\begin{matrix}0&0&1\\4&4&4\end{matrix}\right.\right) = \varphi(\tau; v_0, 0) + \vartheta_1(\tau, 1, 4),$$

$$2\Theta_0\left(\tau\left|\begin{matrix}1&2&2\\4&4&4\end{matrix}\right.\right) = \varphi(\tau; v_0, 0) - \vartheta_1(\tau, 1, 4),$$

$$2\Theta_0\left(\tau\left|\begin{matrix}0&0&1\\2&6&6\end{matrix}\right.\right) = \varphi(\tau; v_1, 0) + \vartheta_1(\tau, 1, 6),$$

$$2\Theta_0\left(\tau\left|\begin{matrix}1&1&3\\2&6&6\end{matrix}\right.\right) = \varphi(\tau; v_1, 0) - \varphi(\tau; v_1, \tfrac{1}{2}),$$

$$2\Theta_0\left(\tau\left|\begin{matrix}0&2&3\\2&6&6\end{matrix}\right.\right) = \varphi(\tau; v_1, 0) - \vartheta_1(\tau, 1, 6),$$

$$2\Theta_0\left(\tau\left|\begin{matrix}0&0&2\\2&6&6\end{matrix}\right.\right) = 2\varphi(\tau; v_2, 0) - 2\varphi(\tau; v_2, \tfrac{1}{4}),$$

$$2\Theta_0\left(\tau\left|\begin{matrix}1&0&1\\2&6&6\end{matrix}\right.\right) = 2\varphi(\tau; v_2, 0) + \vartheta_1(\tau, 2, 6),$$

$$2\Theta_0\left(\tau\left|\begin{matrix}1&2&3\\2&6&6\end{matrix}\right.\right) = 2\varphi(\tau; v_2, 0) - \vartheta_1(\tau, 2, 6).$$

Aus ihnen ergeben sich durch Vergleich der Koeffizienten auf beiden Seiten die folgenden Darstellungssätze, in denen $A\left(n\,\middle|\,\begin{matrix}a_1\,a_2\,a_3\\k_1\,k_2\,k_3\end{matrix}\right)$ die Anzahl der Darstellungen der natürlichen Zahl n durch die Form $Q_1=n_1^2+n_2^2+n_3^2$ mit den Nebenbedingungen $n_i\equiv a_i \bmod k_i$ und $B\left(n\,\middle|\,\begin{matrix}a_1\,a_2\,a_3\\k_1\,k_2\,k_3\end{matrix}\right)$ die entsprechenden Anzahlen für die Form $Q_2=3n_1^2+n_2^2+n_3^2$ bedeuten:

$$2A\left(n\,\middle|\,\begin{matrix}0&0&1\\4&4&4\end{matrix}\right)=\delta\left(\frac{n-1}{8}\right)\left\{B_n(d)\,U(n)+\delta(\sqrt{n})\left(\frac{-1}{\sqrt{n}}\right)\sqrt{n}\right\},$$

$$2A\left(n\,\middle|\,\begin{matrix}1&2&2\\4&4&4\end{matrix}\right)=\delta\left(\frac{n-1}{8}\right)\left\{B_n(d)\,U(n)-\delta(\sqrt{n})\left(\frac{-1}{\sqrt{n}}\right)\sqrt{n}\right\},$$
$$(d=d(-n)).$$

$$2B\left(n\,\middle|\,\begin{matrix}0&0&1\\2&6&6\end{matrix}\right)=\delta\left(\frac{n-1}{12}\right)\left\{\tfrac{1}{2}\sqrt{3}\,B_n(d)\,U(3n)+\delta(\sqrt{n})\left(\frac{\sqrt{n}}{3}\right)\sqrt{n}\right\},$$

$$2B\left(n\,\middle|\,\begin{matrix}1&1&3\\2&6&6\end{matrix}\right)=\delta\left(\frac{n-13}{24}\right)\sqrt{3}\,B_n(d)\,U(3n),$$

$$2B\left(n\,\middle|\,\begin{matrix}0&2&3\\2&6&6\end{matrix}\right)=\delta\left(\frac{n-1}{12}\right)\left\{\tfrac{1}{2}\sqrt{3}\,B_n(d)U(3n)-\delta(\sqrt{n})\left(\frac{\sqrt{n}}{3}\right)\sqrt{n}\right\},$$
$$(d=d(-3n)).$$

$$2B\left(4n\,\middle|\,\begin{matrix}0&0&2\\2&6&6\end{matrix}\right)=\delta\left(\frac{n-1}{3}\right)\sqrt{3}\left(1-\sqrt{2}H(2n)\right)B_n(d)\,U(3n),$$

$$2B\left(4n\,\middle|\,\begin{matrix}1&0&1\\2&6&6\end{matrix}\right)=\delta\left(\frac{n-1}{3}\right)\left\{\sqrt{3}\,B_n(d)\,U(3n)+\delta(\sqrt{n})\cdot 2\left(\frac{\sqrt{n}}{3}\right)\sqrt{n}\right\},$$

$$2B\left(4n\,\middle|\,\begin{matrix}1&2&3\\2&6&6\end{matrix}\right)=\delta\left(\frac{n-1}{3}\right)\left\{\sqrt{3}\,B_n(d)\,U(3n)-\delta(\sqrt{n})\cdot 2\left(\frac{\sqrt{n}}{3}\right)\sqrt{n}\right\},$$
$$(d=d(-3n)).$$

Ist insbesondere $n=m^2$ ein Quadrat $(m>0)$, so sind die auftretenden Diskriminanten $d=d(-n)$ bzw. $d=d(-3n)$, Klassenzahlen $h(d)$ und Einheitswurzelanzahlen w explizit angebbar und unabhängig von n. Dann spezialisieren sich die Formeln für die Darstellungsanzahlen $A\left(n\,\middle|\,\begin{matrix}a_1\,a_2\,a_3\\k_1\,k_2\,k_3\end{matrix}\right)$ und $B\left(n\,\middle|\,\begin{matrix}a_1\,a_2\,a_3\\k_1\,k_2\,k_3\end{matrix}\right)$ zu den folgenden Ausdrücken, in denen nun nur noch elementare Funktionen auftreten:

$$n=m^2\equiv 1 \bmod 8:$$

$$2A\left(m^2\,\middle|\,\begin{matrix}0&0&1\\4&4&4\end{matrix}\right)=m\left\{\tfrac{3}{4}\,U(m^2)+\left(\frac{-1}{m}\right)\right\},$$

$$2A\left(m^2\,\middle|\,\begin{matrix}1&2&2\\4&4&4\end{matrix}\right)=m\left\{\tfrac{3}{4}\,U(m^2)-\left(\frac{-1}{m}\right)\right\}.$$

$n = m^2 \equiv 1 \bmod 12$:

$$2B\left(m^2 \left| \begin{matrix} 0 & 0 & 1 \\ 2 & 2 & 6 \end{matrix}\right.\right) = m\left\{\tfrac{1}{2}U(3m^2) + \left(\frac{m}{3}\right)\right\},$$

$$2B\left(m^2 \left| \begin{matrix} 0 & 2 & 3 \\ 2 & 6 & 6 \end{matrix}\right.\right) = m\left\{\tfrac{1}{2}U(3m^2) - \left(\frac{m}{3}\right)\right\}.$$

$n = m^2 \equiv 1 \bmod 3$:

$$2B\left(4m^2 \left| \begin{matrix} 0 & 0 & 2 \\ 2 & 6 & 6 \end{matrix}\right.\right) = m\, U(3m^2)\left(1 - \sqrt{2}\, H(2m^2)\right),$$

$$2B\left(4m^2 \left| \begin{matrix} 1 & 0 & 1 \\ 2 & 6 & 6 \end{matrix}\right.\right) = m\left\{U(3m^2) + 2\left(\frac{m}{3}\right)\right\},$$

$$2B\left(4m^2 \left| \begin{matrix} 1 & 2 & 3 \\ 2 & 6 & 6 \end{matrix}\right.\right) = m\left\{U(3m^2) - 2\left(\frac{m}{3}\right)\right\}.$$

Ist andererseits n kein Quadrat, so bleiben zwar d, $h(d)$ und w in den Formeln stehen, jedoch verschwinden dann die mit $\delta(\sqrt{n})$ behafteten Zusatzglieder in den Formeln für die Darstellungsanzahlen A, B.

Da der Ausdruck $1 - \sqrt{2} H(n)$ für kein ganzes n verschwindet, besitzt insbesondere jede natürliche Zahl n mit $n \equiv 4 \bmod 12$ mindestens eine Darstellung $n = 3n_1^2 + n_2^2 + n_3^2$ mit $n_1 \equiv 0 \bmod 2$, $n_2 \equiv 0 \bmod 6$, $n_3 \equiv 2 \bmod 6$.

In $\varphi(\tau; v_2, 0) - 2\varphi(\tau; v_2, \frac{1}{4})$ hat man eine Form

$$f(\tau) = \sum_{n>0,\ n\equiv 1 \bmod 3} a(n)\, e^{\frac{2\pi i n \tau}{3}} \in \{\Gamma_0[12], -\tfrac{3}{2}, v_2\}$$

mit $a(n) = 0$ genau für $n \equiv 7, 10 \bmod 12$. Daraus folgt etwa die Relation

$$4B\left(4n \left| \begin{matrix} 0 & 0 & 2 \\ 2 & 6 & 6 \end{matrix}\right.\right) = B\left(4n \left| \begin{matrix} 1 & 0 & 1 \\ 2 & 6 & 6 \end{matrix}\right.\right) + B\left(4n \left| \begin{matrix} 1 & 2 & 3 \\ 2 & 6 & 6 \end{matrix}\right.\right) \quad \text{für } n \equiv 7, 10 \bmod 12$$

zwischen Darstellungsanzahlen.

Literatur

[1] Petersson, H.: Über die Entwicklungskoeffizienten der ganzen Modulformen und ihre Bedeutung für die Zahlentheorie. Abh. Math. Sem. Hamburg **8**, 215—242 (1931). — [2] Maass, H.: Konstruktion ganzer Modulformen halbzahliger Dimension mit ϑ-Multiplikatoren in einer und zwei Variablen. Abh. Math. Sem. Hamburg **12**, 133—162 (1938). — [3] Petersson, H.: Über die Berechnung der Skalarprodukte ganzer Modulformen. Commentarii Mathematici Helvetici **22**, 168—199 (1949).

Darmstadt, Hermannstraße 29

(Eingegangen am 10. Mai 1955)