ANNALES
UNIVERSITATIS SCIENTIARUM BUDAPESTINENSIS DE ROLANDO EÖTVÖS NOMINATAE

SECTIO MATHEMATICA

TOMUS XII.

REDIGIT

Á. CSÁSZÁR

ADIUVANTIBUS

G. HAJÓS, F. KÁRTESZI, A. KÓSA, J. MOGYORÓDI, J. MOLNÁR, R. PÉTER, A. RÉNYI, P. SZÁSZ, J. SURÁNYI, P. TURÁN

1969

ANNALES
UNIVERSITATIS SCIENTIARUM BUDAPESTINENSIS DE ROLANDO EÖTVÖS NOMINATAE

SECTIO BIOLOGICA
incepit anno MCMLVII

SECTIO CHIMICA
incepit anno MCMLIX

SECTIO GEOGRAPHICA
incepit anno MCMLXVI

SECTIO GEOLOGICA
incepit anno MCMLVII

SECTIO HISTORICA
incepit anno MCMLVII

SECTIO IURIDICA
incepit anno MCMLIX

SECTIO MATHEMATICA
incepit anno MCMLVIII

SECTIO PHILOLOGICA
incepit anno MCMLVII

SECTIO PHILOSOPHICA ET SOCIOLOGICA
incepit anno MCMLXII

ÜBER EINE PARKETTIERUNG DES DREIDIMENSIONALEN HYPERBOLISCHEN RAUMES

Von

H. ZEITLER
(Weiden)

(Eingegangen am 17. April 1967)

§ 1. Einleitung

Der k-dimensionale hyperbolische Raum H^k soll durch reguläre Fundamentalpolyeder, die zueinander kongruent sind, lückenlos und ohne Überlappungen ausgefüllt werden. Weiter sollen zwei benachbarte Fundamentalpolyeder dabei entweder eine ganze Seitenfläche, eine Kante oder nur einen Eckpunkt gemeinsam haben. Wir sprechen dann von einer Parkettierung des H^k mit regulären Polyedern oder von einem Mosaik aus regulären Polyedern. Ein solches Mosaik können wir uns aus einem einzigen Fundamentalpolyeder durch fortgesetztes Anlagern kongruenter Polyeder entstanden denken.

F. KÁRTESZI [1] untersuchte die Parkettierung des H^2 mit regulären Dreiecken und J. HORVÁTH [2] die des H^2 mit beliebigen regulären Polygonen. Dabei wurden besondere Differenzengleichungen entwickelt und gewisse Grenzwerte betrachtet.

In der vorliegenden Arbeit behandeln wir Parkettierungen des H^3 mit regulären Polyedern. In einem speziellen Fall stellen wir wieder eine Differenzengleichung auf und untersuchen entsprechende Grenzwerte.

§ 2. Parkettierungsmöglichkeiten des H^3 mit regulären Polyedern

Zur Veranschaulichung bedienen wir uns bei den Überlegungen dieses Abschnitts des allgemeinen Poincaré-Modells. Im Mittelpunkt M der Grundkugel dieses Modells sollen sich Fundamentalpolyeder einer Parkettierung treffen. Die, von M ausgehenden hyperbolischen Polyederkanten sind jetzt gleichzeitig euklidische Strecken. Eine, zur Grundkugel des Modells konzentrische Kugel schneidet diese Kanten in Punkten, die ein reguläres euklidisches Polyeder bilden müssen. Wir sprechen vom charakteristischen Polyeder. Es kommen dafür also nur die fünf Platonischen Körper in Frage: Hexaeder, Tetraeder, Oktaeder, Dodekaeder und Jkosaeder (H, T, O, D, J).

Der Winkel α, den zwei benachbarte Eckpunkte des charakteristischen Polyeders mit M bilden, läßt sich mit Mitteln der euklidischen Geometrie berechnen. Wir erhalten:

H: $\alpha \approx 70°32'$, T: $\alpha \approx 109°28'$, O: $\alpha = 90°$, D: $\alpha \approx 41°48'$, J: $\alpha \approx 63°26'$.

Dieser Winkel α ist aber auch Winkel einer Seitenfläche eines hyperbolischen Fundamentalpolyeders. Nehmen wir an, es handle sich bei diesen Seitenflächen um reguläre N-ecke, so muß nach den Winkelsummensätzen der hyperbolischen Geometrie gelten:

$$N\alpha < (N-2) \cdot 180.$$

Daraus folgt speziell für verschiedene Werte von N:

$N=3$, $\alpha<60$; $N=4$, $\alpha<90$; $N=5$, $\alpha<108$; $N=6$, $\alpha<120$; $N>6$, $\alpha<\alpha_0$ dabei gilt $120<\alpha_0<180$.

Vergleichen wir dies mit den oben genannten Zahlenwerten, so zeigt sich z. B., daß es eine Parkettierung des H^3 mit regulären Polyedern, deren Seitenflächen reguläre Dreiecke sind, nur geben kann, wenn das charakteristische Polyeder ein Dodekaeder ist.

Alle, auf diesem Wege ausscheidenden Fälle sind in der Tabelle mit einem Kreuz bezeichnet.

	charakteristisches Polyeder				
	H	T	O	D	J
$N=3$	×	×	×	IV	×
$N=4$	○	×	×	○	I
$N=5$	○	×	III	○	II
$N\geq 6$	○	○	○	○	○

Mögliche Parkettierungen des H^3 mit regulären Polyedern.

Um noch weitere Fälle zu erkennen, die nicht brauchbar sind, bedienen wir uns des Eulerschen Polyedersatzes:

$$e+f-k = 2$$

e ist dabei die Eckenzahl, f die Seitenflächenzahl und schließlich k die Kantenzahl eines Polyeders. Nehmen wir zunächst an, das charakteristische Polyeder sei ein Jkosaeder. Dann gehen von einer Ecke des Fundamentalpolyeders drei

Kanten aus. Weil jede Kante doppelt zählt, folgt daraus $k = \frac{3e}{2}$. In jeder Kante des Fundamentalpolyeders treffen sich zwei Seitenflächen. Handelt es sich dabei um reguläre N-Ecke, so zählt jede dieser Flächen N-fach, und es ergibt sich $f = \frac{2k}{N} = \frac{3e}{N}$. Der Eulersche Satz, angewandt auf das Fundamentalpolyeder liefert dann:

$$e + \frac{3e}{N} - \frac{3e}{2} = 2 \quad \text{oder} \quad \frac{e}{2N}(6-N) = 2.$$

Daraus folgt $N < 6$. Nach dem vorhin Gesagten bleibt also nur noch übrig $N=4$, $N=5$.

Alle, auf diesem Wege ausscheidenden Fälle sind in der Tabelle mit einem Kreis bezeichnet.

Nach diesen Überlegungen sind also nur noch vier verschiedene Parkettierungen des H^3 mit regulären Polyedern denkbar.

Im Fall I ergibt sich mit der Eulerschen Formel $e + \frac{3}{4}e - \frac{3}{2}e = 2$ also $e = 8$. Damit weiter $f = \frac{3e}{4} = 6$, $k = \frac{3e}{2} = 12$. Das Fundamentalpolyeder ist also ein hyperbolisches Hexaeder. Die Seitenflächen dieses Polyeders sind reguläre hyperbolische Vierecke mit den Winkeln $\alpha \approx 63°26'$. Analog erkennen wir, daß es sich bei den regulären Fundamentalpolyedern in der Fällen II, III um hyperbolische Dodekaeder, im Fall IV dagegen um hyperbolische Jkosaeder handelt.

Weil bei I das einfachste Fundamentalpolyeder auftritt, werden wir im folgenden dieses spezielle Mosaik genauer untersuchen.

Vorher stellen wir noch fest, daß die regulären Seitenflächenpolygone mit den vorgeschriebenen Winkeln α und die dazugehörigen regulären Fundamentalpolyeder wirklich konstruiert werden können. Durch fortgesetztes Anlagern solcher Fundamentalpolyeder lassen sich dann die entsprechenden Parkettierungen tatsächlich auch herstellen.

§ 3. Aufstellung einer Differenzengleichung für das Hexaedermosaik

Der Fall I in unserer Tabelle führt auf eine Parkettierung des H^3 mit speziellen regulären Hexaedern. Weil das charakteristische Polyeder ein Jkosaeder ist, treffen sich in jedem Eckpunkt dieses Mosaiks 20 und an jeder Kante 5 Fundamentalhexaeder.

a) *Die konzentrischen Gürtel.* Bei fortgesetztem Anlagern von Fundamentalhexaedern an ein Ausgangshexaeder p_0 wird dieses von konzentrischen Gürteln umgeben. Wir bezeichnen die Umgrenzungspolyeder des i-ten Gürtels mit p_i und p_{i-1}. Der i-te Gürtel besteht dann aus allen zu p_0 kongruenten Fundamentalhexaedern des Mosaiks, die mit p_{i-1} entweder eine ganze Seitenfläche, eine Kante oder aber nur einen Eckpunkt gemeinsam haben. Wir bezeichnen diese drei verschiedenen Fundamentalhexaeder mit H_F, H_K und H_E. Alle Seitenflächen dieser Fundamentalhexaeder des i-ten Gürtels, die mit p_{i-1} in keinem einzigen

Punkt übereinstimmen, bilden das Umgrenzungspolyeder p_i. Damit haben wir eine Definition des i-ten Gürtels.

b) *Die Punkte* P_F, P_K, P_E. Es gibt auf dem Umgrenzungspolyeder p_i drei Arten von Eckpunkten.

Die Punkte P_F. Ein H_F steht mit seiner Grundfläche $A\,B\,C\,D$ in p_{i-1}. Die Gegenpunkte $\bar{A}\,\bar{B}\,\bar{C}\,\bar{D}$ dieses Hexaeders sind P_F Punkte. Von jedem Punkt dieser Art geht also eine Kante durch den i-ten Gürtel hindurch nach p_{i-1}. Längs dieser Kanten treffen sich je 5 H_F des i-ten Gürtels, also gehen von einem P_F in p_i 5 Kanten aus (Figur 1).

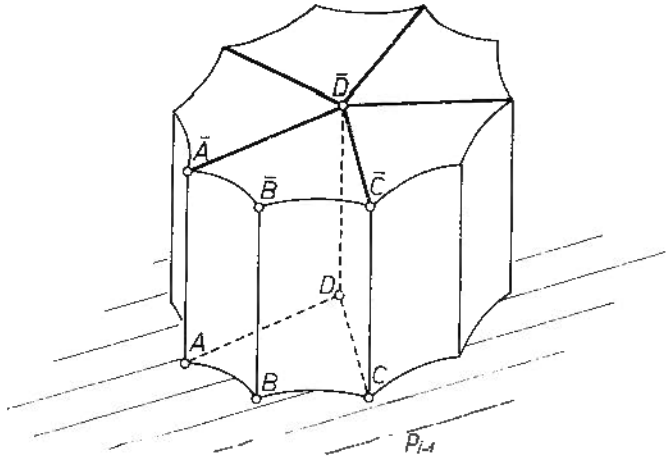

Fig. 1

Die Punkte P_E. Ein H_E steht mit einer Ecke A in p_{i-1}. Der Gegenpunkt $\bar{A}$ dieses Hexaeders ist ein P_E Punkt. Von Punkten dieser Art gehen also in p_i drei Kanten aus, die ein und demselben Fundamentalhexaeder angehören (Figur 2).

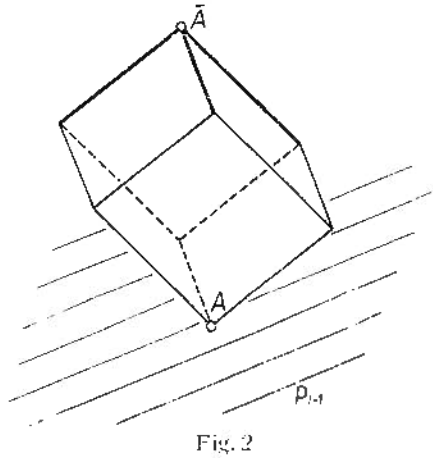

Fig. 2

Die Punkte P_K. Ein H_K steht mit einer Kante $A\,B$ in p_{i-1}. Die Gegenpunkte $\bar{A}$, $\bar{B}$ dieses Hexaeders sind P_K Punkte. An die durch $A\,\bar{A}$ bestimmte Seitenfläche des Hexaeders grenzt ein H_E. Also gehen von einem P_K in p_i vier Kanten aus. Längs zweier solcher Kanten treffen sich zwei Fundamentalhexaeder des i-ten Gürtels (Figur 3).

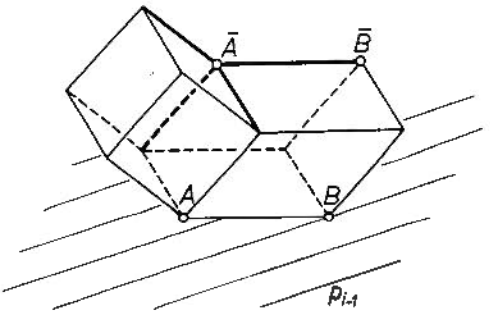

Fig. 3

c) *Zuordnung der Eckpunkte aus p_i, p_{i-1} und Anzahl der Fundamentalhexaeder im i-ten Gürtel.*

P_E in p_{i-1}. Über den drei, von einem solchen Punkt ausgehenden Seitenflächen gibt es je ein H_F, also entsteht je ein P_F in p_i. Weil an jeder Kante 5 Fundamentalpolyeder zusammenstoßen, kommen dazu noch je Kante 2 H_K, also je ein P_F und $2P_K$ in p_i. Da sich weiter in P_E 20 Fundamentalhexaeder treffen, müssen noch $10H_E$ dazugefügt werden. Überlegungen am charakteristischen Jkosaeder zeigen, daß dadurch $3P_F$, $10P_E$ und $12P_K$ in p_i entstehen. Jedem P_E in p_{i-1} sind also insgesamt zugeordnet:
Punkte in p_i: $9P_F$, $18P_K$, $10P_E$,
Fundamentalhexaeder im i-ten Gürtel: $3H_F$, $6H_K$, $10H_E$.

P_K in p_{i-1}. Über den vier, von einem solchen Punkt ausgehenden Seitenflächen gibt es je ein H_F, also entsteht je ein P_F in p_i. Zu zwei Kanten kommen je ein H_K, zu den beiden anderen Kanten je $2H_K$ dazu, insgesamt also $6P_K$, $2P_F$ in p_i. Schließlich müssen noch $8H_E$ dazugefügt werden. Überlegungen am charakteristischen Jkosaeder zeigen wieder, daß dadurch $2P_F$, $8P_E$, $9P_K$ in p_i entstehen. Jedem P_K in p_{i-1} sind also insgesamt zugeordnet:
Punkte in p_i: $8P_F$, $15P_K$, $8P_E$,
Fundamentalhexaeder im i-ten Gürtel: $4H_F$, $6H_K$, $8H_E$.

P_F in p_{i-1}. Über den 5, von einem solchen Punkt ausgehenden Seitenflächen gibt es je ein H_F, also entsteht je ein P_F in p_i. Zu jeder Kante, die von P_F in p_{i-1} ausgeht kommt je ein H_K dazu, also je ein P_K in p_i. Schließlich müssen noch $5H_E$ dazugefügt werden. Überlegungen am charakteristischen Jkosaeder zeigen wieder, daß dadurch $5P_E$, $1P_F$, $5P_K$ in p_i entstehen. Jedem P_F in p_{i-1} sind also insgesamt zugeordnet:
Punkte in p_i: $6P_F$, $10P_K$, $5P_E$,
Fundamentalhexaeder im i-ten Gürtel: $5H_F$, $5H_K$, $5H_E$.

Bezeichnen wir die Anzahl der P_F, P_K, P_E in p_i bzw. in p_{i-1} mit f_i, k_i, e_i bzw. $f_{i-1}, k_{i-1}, e_{i-1}$, so lassen sich die vorliegenden Ergebnisse, wie folgt zusammenfassen:

$$
\begin{aligned}
f_i &= 9e_{i-1} + 8k_{i-1} + 6f_{i-1}, \\
k_i &= 18e_{i-1} + 15k_{i-1} + 10f_{i-1}, \qquad (1)\\
e_i &= 10e_{i-1} + 8k_{i-1} + 5f_{i-1}.
\end{aligned}
$$

Beachtet man auch noch, daß H_E einfach, H_K doppelt und H_F vierfach zählen, so ergibt sich für die Anzahl z_i von Fundamentalhexaedern im i-ten Gürtel

$$z_i = (10e_{i-1} + 8k_{i-1} + 5f_{i-1}) + \frac{1}{2}(6e_{i-1} + 6k_{i-1} + 5f_{i-1}) + \frac{1}{4}(3e_{i-1} + 4k_{i-1} + 5f_{i-1})$$

$$z_i = \frac{1}{4}(55e_{i-1} + 48k_{i-1} + 35f_{i-1}). \qquad (2)$$

d) *Aufstellung einer Differenzengleichung für z_i.*
Wir suchen nach einer Differenzengleichung der Form

$$z_i = \alpha z_{i-1} + \beta z_{i-2} + \gamma z_{i-3}.$$

(2) läßt sich mit anderen Indizes schreiben

$$z_{i-2} = \frac{1}{4}(55e_{i-3} + 48k_{i-3} + 35f_{i-3}). \qquad (3)$$

Die Gleichungen (1) werden jetzt mit passendem Index in (2) eingesetzt. Dann wird der Index rechts auf $(i-3)$ gebracht und es ergibt sich

$$z_{i-1} = \frac{1}{4}(1729e_{i-3} + 1440k_{i-3} + 965f_{i-3}). \qquad (4)$$

Werden die Gleichungen (1) zweimal hintereinander mit passendem Index in (2) eingesetzt, so erhalten wir

$$z_i = \frac{1}{4}(51\,895e_{i-3} + 43\,152k_{i-3} + 28835f_{i-3}). \qquad (5)$$

Auflösung der Gleichungen (1) nach $e_{i-1}, f_{i-1}, k_{i-1}$ liefert

$$
\begin{aligned}
e_{i-1} &= 10e_i - 8k_i + 5f_i, \\
k_{i-1} &= -18e_i + 15k_i - 10f_i, \\
f_{i-1} &= 9e_i - 8k_i + 6f_i.
\end{aligned}
$$

Gehen wir damit in Gleichung (2) hinein, so ergibt sich, mit passendem Index geschrieben, folgende Gleichung

$$z_{i-3} = \frac{1}{4}(e_{i-3} + 5f_{i-3}) \qquad (6)$$

Einsetzen von (5), (4), (3) und (6) in die hypothetische Differenzengleichung gestattet Koeffizientenvergleich. Wir bekommen die Gleichungen

$$51\,895 = 1729\alpha + 55\beta + \gamma,$$
$$43\,152 = 1440\alpha + 48\beta,$$
$$28\,835 = 965\alpha + 35\beta + 5\gamma.$$

Daraus errechnet sich

$$\alpha = 31,\ \beta = -31,\ \gamma = 1.$$

Die gesuchte Differenzengleichung lautet also:

$$z_i = 31z_{i-1} - 31z_{i-2} + z_{i-3}. \tag{7}$$

§ 4. Auswertung der Differenzengleichung

Wir untersuchen zunächst die, zu (7) gehörende charakteristische Gleichung

$$\alpha^3 = 31\alpha^2 - 31\alpha + 1.$$

Sie hat drei voneinander verschiedene, reelle und positive Wurzeln, nämlich

$$\alpha_1 = 15 + 4\sqrt{14},\ \alpha_2 = 1,\ \alpha_3 = 15 - 4\sqrt{14}.$$

Es gilt

$$\alpha_1 > \alpha_2 > \alpha_3.$$

Die allgemeine Lösung von (7) hat also ([3], S.95) das Aussehen

$$z_i = C_1\alpha_1^i + C_2 + C_3\alpha_3^i.$$

Die Konstanten C_1, C_2, C_3 werden dabei durch die Anfangswerte von z_i bestimmt.

Wir wenden uns nun dem Grenzwert $\lim\limits_{i\to\infty} \frac{z_{i+1}}{z_i}$ zu.

Nach den Sätzen über Differenzengleichungen ([3], S.104) ist für $C_1 \neq 0$ dieser Grenzwert gleich der absolut größten Wurzel unserer charakteristischen Gleichung. Es gilt also

$$\lim_{i\to\infty} \frac{z_{i+1}}{z_i} = \alpha_1 = 15 + 4\sqrt{14}. \tag{8}$$

Der Fall $C_1 = 0$ kann gar nicht eintreten. Wäre etwa $C_1 = 0$, dann müßte gelten $C_3 \neq 0$. Sonst hätten wir $z_i = C_2$ und dies wäre ein Widerspruch zur geometrischen Bedeutung von z_i. Mit $C_1 = 0$ und $C_3 \neq 0$ ergäbe sich

$$z_1 = C_2 + C_3\alpha_3,\quad z_2 = C_2 + C_3\alpha_3^2,\quad z_3 = C_2 + C_3\alpha_3^3.$$

Daraus würde folgen:

$$\frac{z_2 - z_3}{z_1 - z_2} = \alpha_3.$$

Dies ist erneut ein Widerspruch. Denn die rechte Seite dieser Gleichung ist eine irrationale, die linke dagegen wegen der geometrischen Bedeutung von z_i eine rationale Zahl.

Es läßt sich noch zeigen, daß aus (8) folgt

$$\lim_{i\to\infty} \frac{z_i}{1+z_1+\ldots+z_i} = \lim_{i\to\infty} \frac{z_i}{w_i} = \frac{\alpha_1 - 1}{\alpha_1} = 4\sqrt{14}-14,$$

und schließlich weiter

$$\lim_{i\to\infty} \frac{w_{i+1}}{w_i} = \alpha_1 = 15+4\sqrt{14}.$$

Für die Größen w_i ergibt sich, wegen $w_i - w_{i-1} = z_i$ durch Einsetzen in (7) die Differenzengleichung:

$$w_i = 32w_{i-1} - 62w_{i-2} + 32w_{i-3} - w_{i-4}.$$

§ 5. Ausblick

In einer weiteren Untersuchung müssen jetzt noch die Fälle II, III und IV der Tabelle untersucht werden. Schließlich ist auch eine Behandlung „asymptotischer" Parkettierungen notwendig. In diesem Falle sind die Fundamentalpolyeder asymptotisch, d.h. ihre Eckpunkte liegen unendlich fern.

Literatur

[1] F. Kárteszi, Eine Bemerkung über das Dreiecksnetz der hyperbolischen Ebene, *Publ. Math. Debrecen*, 5 (1957), 142–146.
[2] J. Horváth, Über die regulären Mosaiken der hyperbolischen Ebene, *Annales Univ. Sci. Budapest*, Sectio Mathematica, 7 (1964), 49–53.
[3] H. Meschkowski, *Differenzengleichungen*, Göttingen (1959).
Zur allgemeinen Orientierung über Parkettierungsprobleme:
[4] H. S. M. Coxeter, *Regular Polytopes*, London (1948).
[5] L. Fejes Tóth, *Reguläre Figuren*, Budapest (1965).

QUADRATIC INEQUALITIES AMONG PROBABILITIES

By

J. GALAMBOS

Department of Mathematics, University of Ghana, Legon

(Received September 9, 1968)

1. A general method to prove quadratic inequalities among probabilities

There are well known methods to prove linear inequalities among probabilities: the method of indicators of M. LOÉVE and a general method due to A. RÉNYI, (the best available references are [5], complements to Chapter 1, and [6] p. 28). It was possible to use Rényi's approach to generalize the method for quadratic inequalities (see [3]). We shall now give another generalization of the method mentioned which is applicable to a wider class of quadratic inequalities.

To formulate our method we need some notations.

Let $S = (\Omega, \mathcal{A}, P)$ denote a probability space. Denote by $S_2(p, q)$ the probability space S when Ω contains two elements: ω_1 and ω_2 and $\mathcal{A}$ consists of four events Ω, $\alpha = \{\omega_1\}$, $\beta = \{\omega_2\}$ and 0 (empty set), further $P(\alpha) = p = 1-q = 1-P(\beta)$.

Let $A_1, A_2, \ldots$ be arbitrary events in S, i.e. $A_i \in \mathcal{A}$. Then a function $F(A_1, \ldots, A_n)$ of the variables $A_1, \ldots, A_n$ is called a Boolean function (of the events $A_1, \ldots, A_n$) if it can be expressed by a finite number of the Boolean operations: addition, multiplication and taking complements.

Our method is given in

THEOREM 1. Let $F_1, \ldots, F_s$ be s Boolean functions of the events $A_1, \ldots, A_n$. If the quadratic expression

$$Q = \sum_{i=1}^{s} \sum_{j=1}^{s} a_{ij} P(F_i) P(F_j); \quad (a_{ij} \text{ are real}) \tag{1}$$

is of the form

$$Q = up^2 + rpq + vq^2, \; u \geq 0, \; r \geq 0, \; v \geq 0 \tag{2}$$

on $S_2(p, q)$, then $Q \geq 0$ on any probability space S.

REMARK 1. The condition that Q in (1) is homogeneous quadratic form of the variables $P(F_i)$, $i = 1, 2, \ldots, s$, is not a restriction, since Ω itself is a Boo-

lean function and thus putting $F_{s+1} = \Omega$ and multiplying all linear terms in an inhomogeneous quadratic expression by $P(F_{s+1}) = P(\Omega) = 1$ we obtain a homogeneous quadratic expression of the variables $P(F_1), \ldots, P(F_s), P(F_{s+1})$ from any inhomogeneous quadratic form of the variables $P(F_1), \ldots, P(F_s)$.

Proof of Theorem 1. It is similar to that of our general method in [3]. Introduce the notation

$$A^1 = A \text{ and } A^{-1} = \text{complement of } A.$$

Let $e_1, \ldots, e_n$ be functions taking two values $+1$ and -1. (These can be defined on the non-negative integers $0, 1, \ldots, 2^n-1$ and can, e.g., be expressed by the digits in their diadic expansion). Then

$$B_{n,m} = A_1^{e_1(m)} A_2^{e_2(m)} \ldots A_n^{e_n(m)} \quad (0 \leq m \leq 2^n - 1)$$

are called the basic Boolean function of the variables $A_1, \ldots, A_n$. Clearly different basic Boolean functions are mutually exclusive. Let F_j be a Boolean function. The expression

$$F_j = \sum_{m \in M_j} B_{n,m} \tag{3}$$

where M_j is a subset of $\{0, 1, \ldots, 2^n-1\}$ is called the canonical form of F_j. (Every Boolean function has a unique canonical form. This can be seen by dissolving the brackets in F_j, then multiplying both sides of (3) by $\prod_{i=1}^{n} (A_i + A_i^{-1})$ and dissolving again the brackets. The uniqueness follows from the fact that different basic Boolean functions are exclusive.)
From (1) and (3)

$$Q = \sum_{k=0}^{2^n-1} \sum_{t=0}^{2^n-1} b_{kt} P(B_{n,k}) P(B_{n,t}) \tag{4}$$

where

$$b_{kt} = \sum_{\substack{(i,j) \\ k \in M_i \\ t \in M_j}} \sum a_{ij}$$

or putting

$$c_k = b_{kk}, \; c_{kt} = b_{kt} + b_{tk} \qquad (t \neq k)$$

we get

$$Q = \sum_{k=0}^{2^n-1} c_k P^2(B_{n,k}) + \sum_{0 \leq k < t \leq 2^n-1} \sum c_{kt} P(B_{n,k}) P(B_{n,t}). \tag{4a}$$

Fix a pair (k, t), $k < t$, of integers $0, 1, \ldots, 2^n-1$ and choose the values of the events A_m as follows

$$A_m = \Omega \text{ if } e_m(k) = e_m(t) = 1$$
$$A_m = 0 \text{ if } e_m(k) = e_m(t) = -1$$
$$A_m = \alpha \text{ if } e_m(k) = 1, \; e_m(t) = -1$$
$$A_m = \beta \text{ if } e_m(k) = -1, \; e_m(t) = 1.$$

For this special choice of the values of the A's we get

$$B_{n,k} = \alpha,\ B_{n,t} = \beta, \quad B_{n,m} = 0, \text{ if } m \neq t, k \tag{5}$$

i.e. for this choice, in view of (4a) and (5),

$$Q = c_k p^2 + c_t q^2 + c_{kt} pq.$$

But according to our assumption (2) it then follows that

$$c_k \geq 0, \quad c_t \geq 0, \quad c_{kt} \geq 0. \tag{6}$$

Since k and t were arbitrary integers from the set $0, 1, \ldots, 2^n - 1$, in view of (4a) and (6) the proof is completed.

2. Applications of Theorem 1.

We shall prove an inequality for the probability that at least k in a sequence of events occur.

Let $A_1, A_2, \ldots, A_n$ be events in a probability space S and let $E_k^{(n)}$ denote the event that at least k among the A's occur.

Put

$$S_t^{(n)} = \sum_{1 \leq i_1 < \ldots < i_t \leq n} \ldots \sum P(A_{i_1} \ldots A_{i_t}). \tag{7}$$

We now prove

THEOREM 2.

$$P(E_k^{(n)}) \geq \frac{(S_1^{(n)} - k + 1) S_k^{(n)}}{(k+1) S_{k+1}^{(n)} + k S_k^{(n)}}. \tag{8}$$

PROOF. Put

$$Q = [(k+1) S_{k+1}^{(n)} + k S_k^{(n)}]\, P(E_k^{(n)}) - (S_1^{(n)} - k + 1) S_k^{(n)}. \tag{9}$$

Applying Theorem 1 we have to consider Q on $S_2(p, q)$.

Let m, n_1 and n_2 denote the number of A's which are equal to Ω, α and β, respectively ($m + n_1 + n_2 \leq n$, and the remaining $n - m - n_1 - n_2$ A's are equal to 0).

Clearly

$$S_t^{(n)} = \binom{m+n_1}{t} p + \binom{m+n_2}{t} q \tag{10}$$

and

$$P(E_k^{(n)}) = \begin{cases} 1 & \text{if } m + n_1 \geq k,\ m + n_2 \geq k \\ p & \text{if } m + n_1 \geq k,\ m + n_2 < k \\ q & \text{if } m + n_1 < k,\ m + n_2 \geq k \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

Thus by simple computation we get from (9), (10) and (11)

$$Q = up^2 + rpq + vq^2 \tag{12}$$

where

$$u = \begin{cases} (k-1)\binom{m+n_1}{k} & \text{if } m+n_1 \geq k \\ 0 & \text{otherwise} \end{cases} \tag{12a}$$

$$v = \begin{cases} (k-1)\binom{m+n_2}{k} & \text{if } m+n_2 \geq k \\ 0 & \text{otherwise} \end{cases} \tag{12b}$$

$$r = \begin{cases} (n_1-n_2)\left[\binom{m+n_1}{k} - \binom{m+n_2}{k}\right] + (k-1)\left[\binom{m+n_1}{k} + \binom{m+n_2}{k}\right] & \text{if } m+n_1 \geq k,\ m+n_2 \geq k \\ [k-1-(m+n_2)]\binom{m+n_1}{k} & \text{if } m+n_1 \geq k,\ m+n_2 < k \\ [k-1-(m+1)]\binom{m+n_2}{k} & \text{if } m+n_1 < k,\ m+n_2 \geq k \\ 0 & \text{otherwise} \end{cases} \tag{12c}$$

(12) and (12a, b, c) show that the condition (2) of Theorem 1 is satisfied thus, by theorem 1, $Q \geq 0$ on any probability space S what was to be proved.

Remark 2. For $k = 1$ we obtain an inequality discovered in [1] and [8] and sharpened in [2] and [4]. In [2] an interesting application of this inequality — a generalization of the Borel—Cantelli lemma due to P. Erdős and A. Rényi — is given.

Corollary 1. Let $A_1, A_2, \ldots$ be an infinite sequence of events on a given probability space S, and let the event that at least k among the A's occur be denoted by E_k. Then

$$P(E_k) \geq \limsup_{n=+\infty} \frac{(S_1^{(n)} - k + 1)S_k^{(n)}}{(k+1)S_{k+1}^{(n)} + kS_k^{(n)}} \tag{13}$$

where $S_k^{(n)}$ is defined in (7).

Proof. Let $E_k^{(n)}$ denote the event as before then we have

$$E_k^{(k)} \subseteq E_k^{(k+1)} \subseteq \ldots, \text{ and } \lim_{n=+\infty} P(E_k^{(n)}) = P(E_k).$$

Thus (13) follows immediately from (8).

COROLLARY 1a. Let $A_1, A_2, \ldots$ be an infinite sequence of exchangeable events then

$$P(E_k) \geq \frac{P_1 P_k}{P_{k+1}} \tag{14}$$

where

$$P_t = P(A_{i_1} A_{i_2} \ldots A_{i_t}).$$

Since now

$$S_k^{(n)} = \binom{n}{k} P_k.$$

(14) is obtained immediately from (13).

REMARK 3. In case when $\lim_{n=+\infty} S_1^{(n)} = \sum_{i=1}^{+\infty} P(A_i) < +\infty$ for k large enough (13) becomes trivial, namely its right hand side will be negative. However, for this case it was not aimed to gain an inequality since for this case an exact expression for $P(E_k)$ had been given in [7].

As another application of Theorem 1 we can prove the inequality of

THEOREM 3.

$$kS_k^{(n)} \leq S_1^{(n)} S_{k-1}^{(n)} + k(k-1)\binom{n}{k} \frac{S_2 - \binom{S_1}{1}}{\binom{n}{2}}. \tag{14}$$

Since the proof demands easy calculations only (by making use of (10) and Theorem 1) it is omitted.

(14) is a reversal of the inequality we proved in [3]. Namely we obtained in [3] that

$$kS_k^{(n)} \geq S_1^{(n)} S_{k-1}^{(n)} - (k-1) S_{k-1}^{(n)}. \tag{15}$$

Introduce the function

$$p_k(n) = \frac{S_k^{(n)}}{\binom{n}{k}}.$$

Thus we obtained from (14) and (15).

COROLLARY 2.

$$|p_k(n) - p_1^k(n)| = O(p_2(n) - p_1^2(n)) + O\left(\frac{1}{n}\right); \quad (k \text{ fixed}). \tag{16}$$

This last statement says that the pairwise independence "in average" coincides with the mutually independence "in average". This, of course, contains, as a special case, the well known fact that if an infinite sequence of exchangeable

events is pairwisely independent, then this forms a mutually independent sequence. It would be interesting to improve the speed of convergence in (16) (imposing perhaps some additional conditions on the sequence A_i), we could thus obtain limit theorems for certain classes of events.

References

[1] CHUNG, K. L. and ERDŐS, P., On the application of the Borel–Cantelli lemma, *Trans. Amer. Math. Soc.*, **72** (1952), 179–186.

[2] DAWSON, D. A. and SANKOFF, D., An inequality for probabilities, *Proc. Amer. Math. Soc.*, **18** (1967), 504–507.

[3] GALAMBOS, J. and RÉNYI, A., On quadratic inequalities in the theory of probability, *Studia Scient. Math. Hungarica*, **3** (1968), 351–358.

[4] GALLOT, S., A bound for the maximum of a number of random variables, *J. Appl. Prob.*, **3** (1966), 556–558.

[5] LOÈVE, M., *Probability theory*, Van Nostrand, New York, 3rd edition, 1963.

[6] RÉNYI A. *Wahrscheinlichkeitsrechnung, mit einem Anhang über Informationstheorie*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1962.

[7] TAKÁCS, L., On the method of inclusion and exclusion, *J. Amer. Stat. Assoc.*, **62** (1967), 102–113.

[8] WHITTLE, P., *Le calcul des probabilités et ses applications*, CNRS. Paris, 1959.

ON ORDINARY LINEAR DIFFERENTIAL EQUATIONS IN BANACH SPACE

By

F. SZIGETI

Eötvös Loránd University, Budapest

(Received September 10, 1968)

In the present paper we deal with ordinary linear differential equations

$$Ly = y^{(n)} + A_{n-1}(s)y^{(n-1)} + \dots + A_0(s)y = f(s) \tag{1}$$

The range of $f(s)$ is in B — shortly: it is B-valued — the ranges of the $A_i(s)$-s are in $L(B, B)$ — shortly: it is $L(B, B)$-valued. Assume that the $f(s)$, $A_i(s)$, $(i=0, 1, \dots, n-1)$ are p-integrable in the sense of BOCHNER [1]. The solutions are sought among the functions of the form

$$y(s) = \sum_{i=0}^{n-1} \eta_i \frac{(s-a)^i}{i!} + \int_a^s \frac{(s-t)^{n-1}}{(n-1)!} \varphi(t)\, dt \tag{2}$$

where $\eta_i \in B$, $\varphi(t) \in L_p[a, b]$.

We shall use the notation $W_p^n[a, b]$ for the space of functions of the form (2), because this is a generalization of the Soboleff space of one variable [8]. W_p^n forms a Banach space with the norms

$$\|\varphi\|_{W_p^n} = \sum_{i=0}^{n} \|\varphi^{(i)}\|_{L_p} \tag{3}$$

$$\|\varphi\|^*_{W_p^n} = \sum_{i=0}^{n-1} |\varphi^{(i)}(a)| + \|\varphi^{(n)}\|_{L_p}. \tag{4}$$

The norms (3) and (4) are equivalent (for the finite dimensional case see [4], [6]). We mention that for the finite dimensional case we have one further norm equivalent to (3) and (4) (see [6]):

$$\|\varphi\|^{**}_{W_p^n} = \|\varphi\|_{L_p} + \|\varphi^{(n)}\|_{L_p}. \tag{5}$$

The equation (1) for the finite dimensional case was discussed by J. GY. OBÁDOVICS in his candidate dissertation [4].

The B-valued function $y(s)$ is called a solution of the Cauchy-problem of equation (1) (... "of equation (1)" will be omitted in the text) if

1. $y(s) \in W_p^n(B, [a, b])$

2. $Ly(s) = f(s)$ a.e. on $[a, b]$

3. $y^{(i)}(a) = \eta_i \quad \eta_i \in B \quad (i = 0, 1, \ldots, n-1)$.

THEOREM 1. *The Cauchy-problem has exactly one solution.*

PROOF. If $y(s)$ is a solution of Cauchy's problem, then it satisfies the equation

$$Ky^{(n)} + y^{(n)} = g(s) \tag{6}$$

where

$$g(s) = f(s) - \sum_{i=0}^{n-1} \left(\sum_{j=0}^{i} A_j(s) \frac{(s-a)^{i-j}}{(i-j)!} \right) \eta_i,$$

$$K\varphi = \int_a^s \left(\sum_{i=1}^{n} A_{n-i}(s) \frac{(s-t)^{i-1}}{(i-1)!} \right) \varphi(t)\, dt,$$

and $K \in L(L_p[a, b], L_p[a, b])$.

This is an immediate consequence of equation (2) and the equations derived from that by derivation:

$$y^{(j)}(s) = \sum_{i=j}^{n-1} \eta_i \frac{(s-a)^{i-j}}{(i-j)!} + \int_a^s \frac{(s-t)^{n-j-1}}{(n-j-1)!} y^{(n)}(t)\, dt.$$

Conversely, if $\varphi(s) \in L_p$ is a solution of equation (6), then

$$y(s) = \sum_{i=0}^{n-1} \eta_i \frac{(s-a)^i}{i!} + \int_a^s \frac{(s-t)^{n-1}}{(n-1)!} \varphi(t)\, dt$$

is a solution of the Cauchy-problem. Moreover, $y(s)$ is the only function for which $y^{(n)} = \varphi(s)$ a.e. on $[a, b]$.

It follows at once, the following inequalities hold for every $\varphi \in L_p$, where:

$$T(s) = \sum_{i=1}^{n} \| A_{n-i}(s) \| \frac{(b-a)^{i-1}}{(i-1)!}.$$

$$|K\varphi| \leq T(s) \int_a^s |\varphi(t)|\, dt$$

$$|K\varphi| \leq T(s)(s-a)^{1/q} \|\varphi\|_{L_p}.$$

One proves easily by induction that

$$\|K^i\| \leq \frac{[(b-a)^{1/q} \|T\|_{L_p}]^i}{(i!)^{1/q}}.$$

The series $\sum_{i=0}^{\infty} \frac{[(b-a)^{1/q}\|T\|_{L_p}]^i}{(i!)^{1/q}}$ is convergent, so the series $\sum_{i=0}^{\infty}(-K)^i$ is absolutely convergent. It follows that $(K+I)^{-1}$ exists and it is a bounded operator in $L_p[a, b]$. So there exists exactly one solution of (6); according to the remark above the theorem is proved.

THEOREM 2. *The solution of Cauchy's problem can be prepreresented in the following form:*

$$y(s) = \varphi_0(s) + \sum_{i=0}^{n-1} \Phi_i(s)\eta_i \tag{7}$$

where φ_0 is the solution of the following Cauchy-problem:

$$\begin{aligned} &1.\ \varphi_0 \in W_p^n(B, [a, b]), \\ &2.\ L\varphi_0 = f, \\ &3.\ \varphi_0^{(i)}(a) = 0 \quad (i = 0, 1, \ldots, n-1). \end{aligned} \tag{8}$$

Φ_i is the solution of the i-th Cauchy-problem:

$$\begin{aligned} &1.\ \Phi_i(s) \in W_p^n(L(B, B), [a, b]), \\ &2.\ \mathbf{L}\Phi_i(s) = \Phi_i^{(n)}(s) + \sum_{j=0}^{n-1} A_j(s)\Phi_i^{(j)}(s) = 0, \quad \text{a.e.} \\ &3.\ \Phi_i^{(j)}(a) = \delta_{ij} I \quad (j = 0, 1, \ldots, n-1), \\ &\quad (i = 0, 1, \ldots, n-1). \end{aligned} \tag{9}$$

PROOF. Let $A \in L(B, B)$ and define the operator $\mathbf{A}$ on $L(B, B)$, so: if $X \in L(B, B)$, then $\mathbf{A}X = AX$. It is obvious that $\|\mathbf{A}\| = \|A\|$, so from $A(s) \in L_p$ it follows $\mathbf{A}(s) \in L_p$.

Now we use Theorem 1 and get that the Cauchy-problems (9) have exactly one solution, say $\Phi_i(s)$

If $A(s) \in L_p(L(B, B), [a, b])$, $\eta \in B$, then $A(s)\eta \in L_p(B, [a, b])$ and $\int_a^b A(t)\,dt\,\eta = \int_a^b A(t)\eta\,dt$ (see [2]), so we get:

$$\begin{aligned} &1.\ \Phi_i\eta_i \in W_p^n(B, [a, b]), \\ &2.\ L(\Phi_i\eta_i) = (\mathbf{L}\Phi_i)\eta_i = 0, \\ &3.\ (\Phi_i\eta_i)^{(j)}(a) = \Phi_i^{(j)}(a)\eta_i = \delta_{ij}\eta_i, \quad (j = 0, 1, \ldots, n-1). \end{aligned}$$

The solution of Cauchy's problem (8) is denoted by φ_0. Obviously $\varphi_0 + \sum_{i=0}^{n-1} \Phi_i\eta_i$ is the only solution of Cauchy's problem of equation (1). So we proved the theorem.

Further we deal with the following problem: Let satisfy $y(s)$:

$$
(10)\qquad \begin{aligned} &1.\ y\in W_p^n(B,[a,b]),\\ &2.\ Ly=f,\\ &3.\ Fy=\gamma \text{ where } F\in L(W_p^n, B'), \end{aligned}
$$

B' is a Banach space, $\gamma\in B'$.

This problem is called generalized boundary-valued problem, because problem (10) is a generalization of the ordinary boundary valued problem:

$$
(11)\qquad 3')\quad M\begin{pmatrix} y(a)\\ y'(a)\\ \cdot\\ \cdot\\ \cdot\\ y^{(n-1)}(a)\end{pmatrix}+N\begin{pmatrix} y(b)\\ y'(b)\\ \cdot\\ \cdot\\ \cdot\\ y^{(n-1)}(b)\end{pmatrix}=\begin{pmatrix}\gamma_0\\ \gamma_1\\ \cdot\\ \cdot\\ \cdot\\ \gamma_{n-1}\end{pmatrix}.
$$

We shall use the notation $\oplus^n B$ for the $B\oplus B\oplus\ldots\oplus B$ (n-times), the notation A for the operator $(F\Phi_0,\ldots,F\Phi_{n-1})$. Obviously A is defined on the space $\oplus^n B$, and if we introduce the following norm in $\oplus^n B$:

$$
\|\xi\| = \|(\xi_1,\ldots,\xi_n)\| = \sqrt{\sum_{i=1}^{n}\|\xi_i\|^2}
$$

we get a Banach space $\oplus^n B$.

$$
\|A\xi\| \le \sum_{i=0}^{n-1}\|F\Phi_i\xi_{i+1}\| \le \|F\|\sqrt{\sum_{i=0}^{n-1}\|\Phi_i\|^2_{W_p^n}}\sqrt{\sum_{i=1}^{n}\|\xi_i\|^2},
$$

so

$$
A\in L(\oplus^n B, B')
$$

is true.

THEOREM 3. *To have exactly one solution for the generalized boundary value problem it is necessary and sufficient that the following equations should hold:*

$$
\operatorname{Ker} A = 0 \quad \textit{and} \quad \operatorname{Im} A = B'
$$

PROOF. If we use Theorem 2, obviously the conditions are necessary. If $\operatorname{Ker} A = 0$ and $\operatorname{Im} A = B'$, then for arbitrary $\gamma\in B'$ the equation $A\xi = \gamma - F\varphi_0$ has exactly one solution $\xi = (\xi_1,\ldots,\xi_n)$. Then the function $\varphi_0 + \sum_{i=0}^{n-1}\Phi_i\xi_{i+1}$ is exactly one solution of problem 10.

Consider a boundary problem of the form

$$
Ly = 0\ Fy = 0.
$$

(Both conditions are homogeneous.)

Then $y(s) = 0$ is always a trivial solution. On the other hand with $y(s)$, $\lambda y(s)$ is also a solution (λ is taken of the field of real or complex numbers.) We say, the problem has exactly one solution if any two non-trivial solutions can be transformed in each other by a scalar multiplier. So it is clear:

THEOREM 4. *To have exactly one solution for the "totally homogeneous" case it is necessary and sufficient that*

$$\dim \operatorname{Ker} A = 1.$$

The solution can be written with the aid of a non-zero element of Ker A, ($\xi \in \operatorname{Ker} A$) in the following form:

$$y(s) = \sum_{i=0}^{n-1} \Phi_i(s)\xi_{i+1}.$$

Now we deal with the solutions $y(s) \in W_p^n(B, [a, b])$ satisfying the boundary condition (11). A simple calculation shows that

$$A = (F\Phi_0, F\Phi_1, \ldots, F\Phi_{n-1}) = M + NW, \tag{12}$$

where $W = (\Phi_i^{(j)}(b))_{i=0,j=0}^{n-1}$ is a bounded linear transformation of the space $\oplus^n B$. (12) can be written in the following form, too:

$$A = (M, N)\begin{pmatrix} I \\ W \end{pmatrix}.$$

From now on B is an n-dimensional Banach space. Theorem 3 gives directly: for the existence of exactly one solution it is necessary that $\dim B' = m \cdot n$ should hold. Suppose, this condition to be satisfied in the future. We show: $\dim \operatorname{Im}\begin{pmatrix} I \\ W \end{pmatrix} = nm$. The inequality $\leq$ follows from the fact that the mapped space is of dimension mn. On the other hand the rank of I is just $m \cdot n$. This proves $\geq$. Now $\dim \operatorname{Ker}(M, N) \geq mn$, because (M, N) maps a space of dimension $2nm$ in a space of dimension $n \cdot m$. On the other hand $\operatorname{Ker} A = 0$ is equivalent to

$$\operatorname{Ker}(M, N) \cap \operatorname{Im}\begin{pmatrix} I \\ W \end{pmatrix} = 0$$

which shows that $\dim \operatorname{Ker}(M, N) = nm$ or more precisely

$$\operatorname{Ker}(M, N) \oplus \operatorname{Im}\begin{pmatrix} I \\ W \end{pmatrix} = \oplus^{2n} B.$$

Conversely this guarantees exactly one solution for $A\xi = \gamma - Fq_0$, or which is the same, for the boundary problem. Thus we proved

THEOREM 5. *The boundary problem* (11) *has exactly one solution for the m-dimensional Banach space if and only if*

$$\operatorname{Ker}(M, N) \oplus \operatorname{Im}\begin{pmatrix} I \\ W \end{pmatrix} = \oplus^{2n} B.$$

Let us have a look at the "totally homogeneous" case with conditions (11). Clearly it holds

$$\dim \operatorname{Ker} A = \dim \operatorname{Ker} (M, N) \cap \operatorname{Im} \begin{pmatrix} I \\ W \end{pmatrix} + \dim \operatorname{Ker} \begin{pmatrix} I \\ W \end{pmatrix}$$

so we get from Theorem 4.

THEOREM 6. *The "totally homogeneous" boundary problem of form* (11) *has exactly one solution if and only if*

$$\dim \operatorname{Ker} (M, N) \cap \operatorname{Im} \begin{pmatrix} I \\ W \end{pmatrix} + \dim \operatorname{Ker} \begin{pmatrix} I \\ W \end{pmatrix} = 1.$$

Bibliography

[1] BOCHNER, Integrationen von Functionen, deren Werte die Elemente eines Vektorraumes sind, *Fund. Mat.*, **20** (1933).

[2] YOSIDA, K., *Functional Analysis*, Springer Verlag, 1965.

[3] LANG, S., *Introduction to Differentiable Manifolds*, New York, London, 1962.

[4] OBÁDOVICS J. GY., L_p együtthatós differenciálegyenlet-rendszerekre vonatkozó kezdeti és peremértékproblémák általános vizsgálata, (candidate dissertation).

[5] PETTIS, On Integration in Vector Spaces, *Trans. Amer. Math. Soc.*, **44** (1938), 277–304.

[6] SZIGETI F., A Kondrasov-tételről, *Mat. Lapok*, **19** (1968), 135–141.

[7] КРЕЙН С. Г., *Линейные дифференциальные уравнения в банаховом пространстве*, Наука, 1967.

[8] СОБОЛЕВ С. Л., Некоторые применения функционального анализа в математической физике, ЛГУ, 1950.

ON AN ALGORITHM FOR ADDITIVE REPRESENTATION OF INTEGERS BY PRIME NUMBERS

By

I. KÁTAI

Department of Algebra and Theory of Numbers, Eötvös Loránd University, Budapest

(Received September 30, 1968)

1. Let $p_1 = 1$, $p_2 = 2$, $p_3 = 3$, $p_4 = 5$, ... and in general let p_{i+1} denote the ith prime number.

Every natural number n can be written in the form

$$n = p_{i_1} + p_{i_2} + \ldots + p_{i_r} \qquad (i_1 \geq i_2 \geq \ldots \geq i_r), \tag{1.1}$$

where p_{i_1} is the greatest p not greater than n, and in general p_{i_k} is the greatest p not greater than $n-(p_{i_1}+\ldots+p_{i_{k-1}})$. This representation is unique.

Let us denote by $\alpha(n)$ the length of this representation, i.e. for n in (1.1) let $\alpha(n) = r$. Let $\alpha(0) = 0$.

The aim of this paper is to examine the behaviour of $\alpha(n)$. Namely we investigate the asymptotic and the order of the sums

$$B_k(x) = \sum_{0 \leq n \leq x} \alpha^k(n). \tag{1.2}$$

Let $\log_k x$ denote the kth iterated of $\log x$. For the sake of brevity let $x_k = \log_k x$ $(k = 1, 2, \ldots)$.

Let $L(x)$ be a function on $x \geq 1$ defined as that integer k for which $1 \leq x_k < e$.

Let $c, c_1, c_2, \ldots$ be suitable positive numerical constants, $\varepsilon, \varepsilon_1, \ldots$ be arbitrary small positive constants, not necessarily the same at every occurence.

Using the theorem of HOHEISEL [1] stating that $p_{i+1} - p_i < cp_i^{\Theta}$ $(\Theta < 1$, constant) we easily deduce

$$\alpha(n) < c \log_2 n + c_1. \tag{1.3}$$

Hence the inequality

$$B_k(x) < cxx_2^k + c_1 x \tag{1.4}$$

follows.

I think, that

$$B_k(x) = (1+o(1))xL^k(x) \qquad (x \to \infty) \tag{1.5}$$

holds for all k.

Presently we prove this only on the unproved Riemann hypothesis. (1.5) follows from a weaker conjecture too, namely from the density-hypothesis in the form $N(\sigma, T) \leq c_1 T^{2(1-\sigma)}(\log T)^{c_2}$ (here $N(\sigma, T)$ denotes the number of zeros of $\zeta(s)$ in the strip $\operatorname{Re} s \geq \sigma$, $|\operatorname{Im} s| \leq T$).

THEOREM 1. *For every fixed* $k \geq 0$

$$\liminf_{x\to\infty} \frac{B_k(x)}{xL^k(x)} \geq 1. \tag{1.6}$$

THEOREM 2. *Assume the validity of the Riemann-conjecture. Then for every fixed* $k \geq 0$

$$\lim_{x\to\infty} \frac{B_k(x)}{xL^k(x)} = 1 \tag{1.7}$$

holds.

Since

$$\Delta_2(x) \overset{\text{def}}{=} \sum_{n\leq x} (\alpha(n) - L(x))^2 = B_2(x) - 2L(x)B_1(x) + xL^2(x),$$

thus from (1.7) $\Delta_2(x) = o(xL^2(x))$ follows. Consequently the following assertion holds.

THEOREM 3. *Assuming the validity of the Riemann-conjecture and allowing a set of zero-density of natural numbers, on the rest we have*

$$\lim_{n\to\infty} \frac{\alpha(n)}{L(n)} = 1. \tag{1.8}$$

We note, that from the famous conjecture of H. CRAMER [2] stating that $p_{i+1} - p_i < c(\log p_i)^2$ it would follow that

$$\limsup_{n\to\infty} \frac{\alpha(n)}{L(n)} = 1.$$

2. For the proof of Theorems 1 and 2 we need some lemmas.

Let $d_i = p_{i+1} - p_i$ and

$$\varrho_d(x) = \sum_{\substack{d_i = d \\ p_{i+1} \leq x}} 1.$$

Then by the Brun or Selberg sieve we have (see [1])

$$\varrho_d(x) < c\frac{x}{x_1^2} \prod_{p|d} (1 + 1/p). \tag{2.1}$$

The following assertion is due to H. CRAMER [2].

LEMMA 1. On the Riemann conjecture we have

$$\frac{1}{x}\sum_{\substack{d_n>h\\ p_n\le x}} d_n = O\left(\frac{\log^3 x}{h\log h}\right). \tag{2.2}$$

This result was improved by A. SELBERG later [3].

We shall use the following

LEMMA 2. Let $H_k(x)$ be a non-decreasing function defined for $x\ge c_1$, satisfying the inequality

$$H_k(x)\le(1+\varepsilon)kL^{k-1}(x)+H_k(x_1^5) \quad \text{for} \quad x\ge c_2. \tag{2.3}$$

Then

$$\limsup_{x\to\infty}\frac{H_k(x)}{xL^k(x)}\le 1+\varepsilon. \tag{2.4}$$

Similarly, if $K_k(x)$ is a non-decreasing function for $x\ge c_1$, satisfying

$$K_k(x)\ge(1-\varepsilon)kL^{k-1}(x)+K_k(x_1^{1/2}) \quad \text{for} \quad x\ge c_2, \tag{2.5}$$

then

$$\liminf_{x\to\infty}\frac{K_k(x)}{xL^k(x)}\ge 1-\varepsilon. \tag{2.6}$$

We prove only (2.4). The proof of (2.6) is very similar and so can be omitted.

Let T be a positive fixed integer and x be large. Let $y_1(x)=x_1^5$, $y_j(x)=(\log y_{j-1}(x))^5$. For $x\ge c_2$ we have

$$y_l(x)<x_{l-1} \quad \text{for} \quad l=1,2,\ldots,T. \tag{2.7}$$

Repeating the inequality (2.3) T times we have

$$H_k(x)\le(1+\varepsilon)k\left\{\sum_{j=1}^{T-1}L^{k-1}(y_j(x))+L^{k-1}(x)\right\}+H_k(y_T(x))\le$$

$$\le(1+\varepsilon)k\left\{2L^{k-1}(x)+\sum_{j=2}^{T-2}L^{k-1}(x_{j-1})\right\}+H_k(x_{T-1}).$$

Taking into account that $L(x_j)=L(x)-j$, and that $L^{k-1}(x)=o(L^k(x))$ $(x\to\infty)$ we have

$$H_k(x)-H_k(x_{T-1})\le(1+\varepsilon)(1+\varepsilon_1)\{L^k(x)-L^k(x_{T-1})\},$$

with an arbitrary $\varepsilon_1>0$, if $x>c_1(\varepsilon_1)$.

Applying this inequality for x_{T-1} instead of x, and after this for $x_{2(T-1)}$, and so on, we have

$$H_k(x)\le(1+\varepsilon)(1+\varepsilon_1)L^k(x)+c,$$

for all $x\ge 1$. Hence (2.4) immediately follows.

Now we prove Theorem 1 and 2.

Let $p_{j-1} \leq x < p_{j-2}$. Then for (1.2) we have

$$B_k(x) = \sum_{i=1}^{j} \sum_{p_i \leq n < p_{i+1}} \alpha^k(n) + \sum_{p_{j+1} \leq n \leq x} \alpha^k(n) = \sum \sum_i + \sum_A, \text{ say.}$$

By (1.3) and the Hofreisel theorem we have

$$\sum_A = O(x^\theta)$$

with a constant $\theta < 1$. Furthermore

$$\sum_i = \sum_{r=0}^{d_i - 1} (\alpha(\nu) + 1)^k = \sum_{l=0}^{k} \binom{k}{l} B_l(d_i - 1),$$

where we use the notation $B_0(x) = [x+1]$.

Thus we have

$$B_k(x) = \sum_{l=0}^{k-1} \binom{k}{l} \sum_d B_l(d-1)\, \varrho_d(x) + \sum_d B_k(d-1)\, \varrho_d(x) + O(x^\theta). \tag{2.8}$$

Now we prove (1.6) by induction. The relation (1.6) evidently holds for $k = 0$. Suppose that this holds for all $k \leq R-1$. From (2.8) it follows that

$$B_R(x) \geq (1-\varepsilon) L^{R-1}(x) \sum_{d > \sqrt{x_1}} d\varrho_d(x) + \inf_{y \geq \sqrt{x_1}} \frac{B_R(y)}{y} \sum_{d > \sqrt{x_1}} (d-1)\varrho_d(x), \tag{2.9}$$

with an arbitrary positive ε for all large x.

Using (2.1) we have

$$\sum_{d > \sqrt{x_1}} d\varrho_d(x) \geq x - \frac{cx}{x_1},$$

and thus from (2.9)

$$\frac{B_R(x)}{x} \geq (1-\varepsilon) L^{R-1}(x) + \inf_{y > \sqrt{x_1}} \frac{B_R(y)}{y}$$

follows. Taking

$$K_R(x) = \inf_{y \geq x} \frac{B_R(y)}{y}$$

we obtain (2.5), and thus by Lemma 2 (2.6) holds. Since ε is an arbitrary constant, thus (1.6) holds for $k = R$.

Concerning (1.7) we need to prove, that

$$\limsup_{x \to \infty} \frac{B_k(x)}{xL^k(x)} \leq 1 + \varepsilon \tag{2.10}$$

for all $\varepsilon > 0$. Since the proof is analogous to that of (1.6) we only sketch it.

Assuming that (2.10) is valid for all $k \leq R-1$, from (2.10) we deduce

$$B_R(x) \leq \left(1+\frac{\varepsilon}{2}\right) RL^{R-1}(x) + \sum_{d \leq x_1^5} B_R(d-1)\varrho_d(x) + \sum_{d > x_1^5} B_R(d-1)\varrho_d(x) \tag{2.11}$$

for large x. Using Lemma 1 and (1.4) we have

$$\sum_{d > x_1^5} B_R(d-1)\varrho_d(x) = O(x/x_1).$$

Introducing the notation

$$H_R(x) = \max_{y \leq x} \frac{B_R(y)}{y}$$

from (2.11) we have

$$H_R(x) \leq (1+\varepsilon)RL^{R-1}(x) + H_R(x_1^5),$$

if x is large enough. Hence by Lemma 2 (2.10) follows, and this by induction finishes the proof of (1.7).

References

[1] K. Prachar, *Primzahlverteilung*, Springer, 1957.

[2] H. Cramer, On the order of magnitude of the difference between consecutive primes, *Acta Arithm.*, **2** (1937), 23–46.

[3] A. Selberg, On the normal density of primes in small intervals and the difference between consecutive primes, *Arch. Math. Naturvid.*, **47** (6) (1943), 87–105.

A NOTE ON A PAPER OF GORDON AND ROGERS

By

I. KÁTAI

Department of Algebra and Theory of Numbers, Eötvös Loránd University, Budapest

(Received September 30, 1968)

1. Introduction

Let $\tau(n)$ denote the number of divisors of n, $\mu(n)$ the *Möbius*-function. The letters $p, p_1, \ldots$ stand for prime numbers. $c, c_1, \ldots$ denote suitable positive constants, $\varepsilon, \varepsilon_1, \ldots$ arbitrary small positive constants, not necessarily the same in every place. Let γ denote the *Euler*-constant. (a, b) denotes the highest common divisor of a and b.

Let

$$(1.1)-(1.2) \qquad D(x, u) = \sum_{\substack{n \le x \\ (n,u)=1}} |\mu(n)|\tau(n), \qquad E(x, u) = \sum_{\substack{n \le x \\ (n,u)=1}} \frac{|\mu(n)|\tau(n)}{n}.$$

The problem of estimating the sums (1.1), (1.2) was investigated by R. Gordon and K. Rogers in [1]. They proved, that

$$D(x, u) = Ax \log x + Bx + R_1(x), \tag{1.3}$$

$$E(x, u) = \frac{1}{2} A \log^2 x + (A+B) \log x + G + R_2(x), \tag{1.4}$$

where

$$A = \prod_{p|u} \frac{p}{p+2} \prod_{p} \frac{(p-1)^2(p+2)}{p_3}, \tag{1.5}$$

$$B = A\left\{(2\gamma - 1) + 2 \sum_{p|u} \frac{\log p}{p-1} + 6 \sum_{p \nmid u} \frac{(p-1)\log p}{p^2(p+2)}\right\}. \tag{1.6}$$

Furthermore using the notation

$$K(u) = \exp\left\{\frac{c\sqrt{\log 3u}}{\log\log 3u}\right\} \tag{1.7}$$

the inequalities

$$(1.8)-(1.9) \qquad R_1(x) = O(x^{1/2+\varepsilon}K(u)),\ R_2(x) = O(x^{-1/2+\varepsilon}K(u)),$$

$$(1.10) \qquad G = O(K(u))$$

are satisfied.

The aim of this paper is to give an improvement of this result.

THEOREM. *The relations* (1.3), (1.4) *hold with* (1.5)–(1.7), (1.10) *and with*

$$(1.11) \qquad R_1(x) = O(x^{1/2}(\log x)^3K(u)),$$

$$(1.12) \qquad R_2(x) = O(x^{-1/2}(\log x)^3K(u))$$

instead of (1.8), (1.9).

The method of the proof is simple and was applied by the author for other problems, e.g. in [2].

2. Lemmas

Let $D(x)$ and $\Delta(x)$ defined by

$$(2.1) \qquad D(x) = \sum_{n\le x}\tau(n) = x\log x + (2\gamma-1)x + \Delta(x).$$

As it is known we have

$$(2.2) \qquad |\Delta(x)| < c\sqrt{x}.$$

Let $\omega(n)$ and $\Omega(n)$ denote the number of different and all prime factors of n, i.e. for $n = p_1^{\alpha_1}\dots p_r^{\alpha_r}$ let $\omega(n) = r$, $\Omega(n) = \alpha_1+\dots+\alpha_r$. Let $\lambda(n) = (-1)^{\Omega(n)}$.

Let $\mathcal{B}_u$ denote the set of those natural numbers all prime divisors of which are divisors of u.

Let $\mathcal{A}$ denote the set of the natural numbers, in the canonical prime-decomposition of which all exponent is 2 or 3.

Let $f(m)$ be a multiplicative function on the set $\mathcal{A}$ defined by $f(p^2) = -3$, $f(p^3) = 2$.

In what follows the letters k and m are reserved for elements of $\mathcal{B}_u$ and $\mathcal{A}$, respectively.

We prove

LEMMA 1.

$$(2.3) \qquad D(x, u) = \sum_{km\le x}\lambda(k)2^{\Omega(k)}f(m)D(x/km).$$

PROOF. To prove (2.3) we use the uniqueness of Dirichlet-series expansions. This can be verified in a simple elementary way, too.

As it is easy to see

$$\sum_{\substack{n=1\\(n,u)=1}}^{\infty}\frac{|\mu(n)|\tau(n)}{n^s} = \prod_{p\nmid u}\left(1+\frac{2}{p^s}\right) = \prod_{p}\left(1+\frac{2}{p^s}\right)\prod_{p|u}\left(1+\frac{2}{p^s}\right)^{-1}.$$

Further we have

$$\prod_p \left(1+\frac{2}{p^s}\right) = \prod_p \left(1-\frac{1}{p^s}\right)^{-2} \prod_p \left(1-\frac{1}{p^s}\right)^2 \left(1+\frac{2}{p^s}\right).$$

Since

$$(2.4) \qquad H(s) \overset{\text{def}}{=} \prod_{p|u} \left(1+\frac{2}{p^s}\right)^{-1} \prod_p \left(1-\frac{1}{p^s}\right)^2 \left(1+\frac{2}{p^s}\right) = \sum_k \frac{\lambda(k)2^{\Omega(k)}}{k^s} \sum_m \frac{f(m)}{m^s},$$

thus we have

$$\sum_{\substack{n=1\\(n,u)=1}}^{\infty} \frac{|\mu(n)|\tau(n)}{n^s} = \zeta^2(s)H(s) = \left\{\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}\right\}\left\{\sum_{k,m} \frac{\lambda(k)2^{\Omega(k)}f(m)}{(km)^s}\right\}.$$

Multiplying the last two s ries and comparing the coefficients we obtain (2.3).

LEMMA 2. *We have*

$$(2.5) \qquad (H(1)=) \sum_{k,m} \frac{\lambda(k)2^{\Omega(k)}f(m)}{km} = A,$$

and

$$(2.6) \qquad (-H'(1)=) \sum_{k,m} \frac{\lambda(k)2^{\Omega(k)}f(m)\log km}{km} = AB-(2\gamma-1)A$$

(*see* (1.5), (1.6)).

PROOF. (2.5) is obvious from (2.4). (2.6) from (2.4) by logarithmical differentiation follows.

Now we introduce the following notations.

$$(2.7)-(2.8) \qquad \sum\nolimits_1(x) = \sum_{km\le x} \frac{2^{\Omega(k)}|f(m)|}{km}, \quad \sum\nolimits_2(x) = \sum_{km\le x} 2^{\Omega(k)}|f(m)|\left|\Delta\left(\frac{x}{km}\right)\right|,$$

$$(2.9) \qquad \sum\nolimits_3(x) = \sum_{km\le x} \frac{2^{\Omega(k)}|f(m)|\log km}{km},$$

$$(2.10)-(2.11) \qquad S_u = \sum_k \frac{2^{\Omega(k)}}{k^{1/2}}, \qquad \theta(y) = \sum_{m\le y} |f(n)|.$$

LEMMA 3. *The following inequalities hold.*

$$(2.12)-(2.13) \qquad \theta(y) \le c\sqrt{y}\log^2 y, \quad S_u \le K(u),$$

$$(2.14)-(2.15) \qquad \sum\nolimits_1(x) \le \frac{c\log x}{\sqrt{x}} K(u), \qquad \sum\nolimits_3(x) \le \frac{c\log^2 x}{\sqrt{x}} K(u),$$

$$(2.16) \qquad \sum\nolimits_2(x) \le c\sqrt{x}\log^3 x K(u).$$

PROOF. As it is easy to see every m element of $\mathcal{A}$ can be uniquely written in the form $m = u^2v^2$, $|\mu(uv)| = 1$, and $|f(m)| = 2^{\omega(v)}3^{\omega(u)}$. Hence by (2.11)

$$\theta(y) \leq \sum_{v^2 \leq y} 2^{\omega(v)} \sum_{u^2 \leq y/v^2} 3^{\omega(u)}.$$

Observing that $\sum_{u \leq z} 3^{\omega(u)} = O(z \log^2 z)$, hence (2.12) rapidly follows.

The sum (2.10) can be written as the product

$$S_u = \prod_{p|u} \left(1 + \frac{2}{p^{1/2}} + \frac{2^2}{p} + \dots\right).$$

Hence

$$S_u \leq \exp\left(c_1 \sum_{p|u} 1/\sqrt{p}\right)$$

follows. Denoting by q_i the i'th prime number and using that $c_2 i \log 2i < q_i < c_3 i \log 2i$, by a simple computation we have

$$\sum_{p|u} 1/\sqrt{p} \leq \sum_{i=1}^{\omega(u)} q_i^{-1/2} \leq c_4 \sqrt{\omega(u)/\sqrt{\log \omega(u)}}.$$

Taking into account that $\omega(u) \leq c_5 \log 3u/\log\log 3u$, hence (2.13) immediately follows.

To prove (2.14) for the sum (2.7) we use the inequalities (2.12)–(2.13).

$$\sum\nolimits_1(x) = \sum_k \frac{2^{\Omega(k)}}{k} \sum_{m \leq x/k} \frac{|f(m)|}{m} \leq \sum_k \frac{2^{\Omega(k)}}{k} \sum_{l=0}^{\infty} \frac{k}{x2^l} \sum_{m \leq \frac{x}{k} 2^{l+1}} f(m) \leq$$

$$\leq \sum_k \frac{2^{\Omega(k)}}{k} \sum_{l=0}^{\infty} \frac{\log x + \log 2^{l+1}}{\left(\frac{x}{k} 2^l\right)^{1/2}} \leq c \frac{\log x}{\sqrt{x}} S_u.$$

Hence by (2.13) we deduce (2.14).

Since

$$\sum\nolimits_3(x) \leq \sum_{l=0}^{\infty} \sum_{x2^l \leq km \leq x2^{l+1}} \frac{2^{\Omega(k)} |f(m)| \, 2^l \log x}{km} \leq \sum_{l=0}^{\infty} 2^l \log x \sum\nolimits_1(x2^l),$$

thus by (2.14) the inequality (2.15) rapidly follows.

Finally we estimate the sum in (2.8). Since $|\Delta(x/km)| < c \frac{x^{1/2}}{\sqrt{km}}$ we have

$$\sum\nolimits_2(x) \leq \sqrt{x} \left\{\sum_k \frac{2^{\Omega(k)}}{k^{1/2}}\right\} \left\{\sum_{m \leq x} \frac{|f(m)|}{m^{1/2}}\right\} \leq \sqrt{x} S_u \sum_{2^r \leq x} 2^{-r/2} \sum_{m \leq 2^{r+1}} |f(m)| =$$

$$= \sqrt{x} S_u \sum_{2^r \leq x} 2^{-r/2} \theta(2^{r+1}).$$

Using the estimations (2.12), (2.13) we deduce (2.16).

This completes the proof of our Lemma.

3. Proof of the Theorem

By the results of the section **2** we rapidly deduce the Theorem. Using Lemma 1 and (2.1) we have

$$D(x, u) = \sum_{km \le x} \lambda(k) 2^{\Omega(k)} f(m) \left\{ \frac{x}{km} \log \frac{x}{km} + (2\gamma - 1) \frac{x}{km} \right\} + O\left(\sum\nolimits_2(x)\right) =$$

$$= \sum + O\left(\sum\nolimits_2(x)\right).$$

Further by Lemma 2 we have

$$\sum = (x \log x + (2\gamma - 1)x) \sum_{km \le x} \frac{\lambda(k) 2^{\Omega(k)} f(m)}{km} - x \sum_{km \le x} \frac{\lambda(k) 2^{\Omega(k)} f(m) \log km}{km} =$$

$$= (x \log x + (2\gamma - 1)x) \{A + O(\sum\nolimits_1(x))\} - x\{B + (2\gamma - 1)A + O(\sum\nolimits_3(x))\}.$$

Thus

$$D(x, u) = Ax \log x + Bx + O(x \log x \sum\nolimits_1(x)) + O(x \sum\nolimits_3(x)) + O(\sum\nolimits_2(x)).$$

Consequently by (2.15), (2.16), (2.17) we obtain (1.3), (1.5), (1.6), (1.11).

The relations (1.4), (1.5), (1.6), (1.10), (1.12) hence rapidly follows by partial summation.

References

[1] R. Gordon and K. Rogers, Sums of the divisor function, *Canad. J. Math.*, **61** (1964), 151–158.

[2] I. Kátai, A remark on H. Delange's paper "Sur un theoreme de Rényi", *MTA III. Osztály Közleményei*, **16** (1966), 269–273, (in Hungarian).

CHARACTERIZATION OF ADDITIVE FUNCTIONS BY ITS LOCAL BEHAVIOUR

By

I. KÁTAI

Department of Algebra and Theory of Numbers, Eötvös Loránd University, Budapest

(Received September 30, 1968)

1. In [1] I proved the following result.

(*A*) *If $f(n)$ is restrictedly additive and*

$$(H_1) \qquad \varliminf_{n\to\infty} \big(f(n+1)-f(n)\big) \geq 0,$$

or

$$(F_1) \qquad \varlimsup_{n\to\infty} \big(f(n+1)-f(n)\big) \leq 0,$$

then it is a constant multiple of $\log n$.

This assertion is proved, independently by A. MÁTÉ, too [2].

Let

$$(1.1) \qquad \Delta^1 f(n) = \Delta f(n) = f(n+1)-f(n),$$

$$(1.2) \qquad \Delta^k f(n) = \Delta^{k-1} f(n+1) - \Delta^{k-1} f(n) \qquad \text{for } k = 2, 3, \ldots.$$

We prove the

THEOREM. *If $f(n)$ is restrictedly additive and*

$$(H_k) \qquad \varliminf_{n\to\infty} \Delta^k f(n) \geq 0,$$

or

$$(F_k) \qquad \varlimsup_{n\to\infty} \Delta^k f(n) \leq 0$$

for some natural number k, then $f(n)$ is a constant multiple of $\log n$.

2. The idea of the proof is the following. From (H_1) or (F_1) the assertion follows by (A). We shall prove, that from the assumption (H_k) resp. (F_k) follows the inequality (F_{k-1}) resp. (H_{k-1}) for $k \geq 2$. After proving this the Theorem follows by induction on k.

Let

$$\Delta_2^1 f(n) = \Delta_2 f(n) = f(n+2) - f(n), \tag{2.1}$$

$$\Delta_2^k f(n) = \Delta_2^{k-1} f(n+2) - \Delta_2^{k-1} f(n) \qquad \text{for } k = 2, 3, \ldots. \tag{2.2}$$

LEMMA 1. *The following identity holds.*

$$\Delta_2^k f(n) = \sum_{j=0}^{k} \binom{k}{j} \Delta^k f(n+j). \tag{2.3}$$

This identity is a trivial one for $k = 1$. The proof goes by induction on k, and so we omit it.

LEMMA 2. *For every odd n holds the identity*

$$\Delta_2^k f(n) = \sum_{j=0}^{k} \binom{k}{j} \Delta_2^k f(2n+2j). \tag{2.4}$$

PROOF. For $k = 1$

$$\Delta_2^1 f(n) = f(n+2) - f(n) = f(2n+4) - f(2n) = \Delta_2^1 f(2n) + \Delta_2^1 f(2n+2),$$

and thus (2.4) holds. Let now suppose that (2.4) holds for $k \leq K$. Then

$$\Delta_2^{K+1} f(n) = \Delta_2^K f(n+2) - \Delta_2^K f(n) = \sum_{j=0}^{K} \binom{K}{j} \Delta_2^K (2n+4+2j) -$$

$$- \sum_{j=0}^{K} \binom{K}{j} \Delta_2^K f(2n+2j) = \sum_{j=0}^{K} \binom{K}{j} \{\Delta_2^{K+1} f(2n+2j) + \Delta_2^{K+1} f(2n+2j+2)\} =$$

$$= \sum_{j=0}^{K+1} \binom{K+1}{j} \Delta_2^K f(2n+2j),$$

and so (2.4) holds for $k = K+1$ too.

In the sequel let $\varepsilon(n)$, $\varepsilon_1(n)$, $\varepsilon_2(n)$, ... denote suitable sequences of positive numbers tending to zero monotonically for $n \to \infty$.

Let now suppose (H_k) holds. Hence it follows that

$$\Delta^{k-1} f(n+1) \geq \Delta^{k-1} f(n) - \varepsilon(n). \tag{2.5}$$

From Lemma 1 it follows, that

$$\Delta_2^{k-1} f(n+1) \geq \Delta_2^{k-1} f(n) - \varepsilon_1(n). \tag{2.6}$$

Using Lemma 2 with $k-1$ instead of k and the inequality (2.6) we have

$$\Delta_2^{k-1} f(n) \geq 2^{k-1} \Delta_2^{k-1} f(2n) - 2^{k-1} \varepsilon_2(n), \tag{2.7}$$

when n is an odd number.

Let now x be an integer and

$$\varrho(x) = \max_{x \leq n \leq 2x} \Delta_2^{k-1} f(n).$$

Using the inequalities (2.6), (2.7) we have

$$\varrho(2x) \leq \frac{\varrho(x)}{2^{k-1}} + \varepsilon_3(x).$$

From this inequality we obtain easily that

$$\overline{\lim_{n\to\infty}}\, \Delta_2^{k-1} f(n) \leq 0. \tag{2.8}$$

Using the representation (2.3) of $\Delta_2^{k-1} f(n)$ and the inequality (2.5) we have

$$\Delta_2^{k-1} f(n) \geq 2^{k-1}\, \Delta^{k-1} f(n) - \varepsilon_1(n).$$

Taking into account the inequality (2.8) we obtain that

$$\overline{\lim}\, \Delta^{k-1} f(n) \leq 0,$$

i.e. that (F_{k-1}) holds.

The deduction of (H_{k-1}) from (F_k) can be performed in a similar way, or immediately follows from the previous proof repeating this for $-f(n)$ instead of $f(n)$.

References

[1] I. Kátai, A remark on additive arithmetical functions, *Annales Univ. Sci. Budapest*, Sectio Math., **8** (1965), 65–69.

[2] A. Máté, A new proof of a theorem of P. Erdős, *Proc. Amer. Math. Soc.*, **8** (1967), 159–162.

A CONTRIBUTION TO BLOCH'S THEOREM

By

G. PETRUSKA

I. Department of Analysis of the Eötvös Loránd University, Budapest

(Received October 22, 1968)

1. Let D denote the unit disc $\{z: |z| < 1\}$ and $f(D)$ the set $\{w: w = f(z), |z| < 1\}$, where $f(z)$ is any function defined in D.

According to the classical result of Bloch, if the function $f(z) = \sum_{k=0}^{\infty} c_k z^k$ is regular in D and $|f'(0)| \geq 1$ then $f(D)$ contains a disc of radius ϱ, $\varrho \geq \gamma$, where γ in an absolute contanst. (See, e.g. [1].)

W. SEIDEL and L. J. WALSH proved a generalization in [2], where the assumption $|f'(0)| = |c_1| \geq 1$ was substituted by $|c_p| \geq 1$, but their constant γ_p depended on p (and only on p). (Actually they proved a sharper result.)

P. TURÁN has observed ([4]) that an essentially stronger theorem holds:

THEOREM 1. *Let $f(z) = \sum_{k=0}^{\infty} c_k z^k$ be regular in $|z| < 1$ and for an integer $p \geq 1$, $\sum_{k=p}^{2p} |c_k|^2 \geq 1$. Then $f(D)$ contains a disc of radius $\varrho \geq \gamma^*$, where γ^* is an absolute constant.* (That is γ^* does not depend even on p).

He stated the problem: what can be said under the weaker assumption

$$\sum_{k=p}^{p^2} |c_k|^2 \geq 1?$$

It is shown in a paper of P. UNGÁR ([3]), that $\sum_{k=1}^{\infty} |c_k|^2 \geq 1$ does not imply any assertion of Bloch type. In this paper we are going to give a short proof of Theorem 1, and we show that this result can not be improved, as it is stated in

THEOREM 2. *Let $\{\nu_p\}_{p=1}^{\infty}$ be a sequence of positive integers, $\nu_p \to +\infty$ arbitrari-*

ly slowly. There exists a sequence of functions $f_p(z) = \sum_{k=0}^{\infty} c_k^{(p)} z^k$, $p = 1, 2, \ldots$ *regular in* D, *such that* $\sum_{k=p}^{p+r_p} |c_k^{(p)}|^2 \geq 1$, *but* $\varrho_p \to 0$, *where*

$$\varrho_p = \sup \{\varrho\colon \text{there exists a } D_\varrho \subset f(D)\},$$

where D_ϱ *is a disc of radius* ϱ.

2. Proof of Theorem 1. Let $f(z) = \sum_{k=0}^{\infty} c_k z^k$ be regular in $|z| < 1$, and $|f'(a)| \geq b$, $|a| = y < 1$, $b > 0$. If $g(z) = \dfrac{1}{b(1-r^2)} f\left(\dfrac{z+a}{1+\bar{a}z}\right)$, then $|g'(0)| \geq 1$ and by the Bloch's theorem $f(D)$ covers a disc of radius at least $\gamma b(1-r^2)$. Let $\sum_{k=p}^{q} |c_k|^2 \geq 1$, where $q > p > 1$ are integers.

By the Parseval formula

$$\frac{1}{2\pi}\int_0^{2\pi} |f'(re^{it})|^2\, dt = \sum_{k=1}^{\infty} k^2 |c_k|^2 r^{2(k-1)} \geq \sum_{k=p}^{q} k^2 |c_k|^2 r^{2(q-1)} \geq$$

$$\geq p^2 r^{2(q-1)} \sum_{k=p}^{q} |c_k|^2 \geq p^2 r^{2(q-1)}; \quad 0 \leq r < 1.$$

Hence $|f'(re^{it_0})|^2 \geq p^2 r^{2(q-1)}$ for some $0 \leq t_0 < 2\pi$. That is $|f'(re^{it_0})| \geq p r^{q-1}$. By our previous remark, $f(D)$ contains a disc of radius at least $\gamma p r^{q-1}(1-r^2)$, for every $0 \leq r < 1$. Trivial calculation shows that this lower estimation is maximal in r when $r = \left(\dfrac{q-1}{q+1}\right)^{1/2}$.

That is, $f(D)$ contains a disc of radius ϱ,

$$\varrho \geq \gamma p \left(1 + \frac{2}{q-1}\right)^{-\frac{q-1}{2}} \cdot \frac{2}{q+1} > \frac{\gamma}{e}\, \frac{2p}{q+1}.$$

If $q = 2p$, $\dfrac{2p}{2p+1} \geq \dfrac{2}{3}$, and we obtain $\varrho > \dfrac{2\gamma}{3e}$.

The theorem is proved, moreover the estimation $\gamma^* > \dfrac{2\gamma}{3e} \geq \dfrac{\sqrt{3}}{6e}$, where γ is the Bloch's constant, $\gamma \geq \dfrac{\sqrt{3}}{4}$.

3. To prove Theorem 2 we need a function $f(z) = \sum_{k=0}^{\infty} c_k z^k$ regular in D and having the properties

(i) $\sum_{k=0}^{\infty} |c_k|^2 = +\infty$

(ii) $f(D)$ does not contain any disc of radius > 1.

It is proved implicitely in [3] that there exist functions with the above properties.

Now we give a simple elementary construction, almost the same as in [3], which results our required function. Let D_1 be the curvilinear triangle in the unit disc, bounded by three circular arcs which are tangent to each other in points $e^{2\pi i\frac{k}{3}}$, $k = 0, 1, 2$. Let $f(z)$ map D_1 onto T, where T denotes an arbitrary equilateral triangle. We may suppose that the vertices of T correspond to those of D_1. Reflecting D_1 on its sides we obtain three new circular triangles and by the principle of reflection the extended $f(z)$ maps these domains onto the reflected images of T.

(Reflection in a circular arc means as usual the inversion with respect to the circle containing the arc.)

Using repeatedly the principle of reflection we extend $f(z)$ to the whole unit disc. $f(D)$ is the full w-plane from which the points obtained by repeated reflection from vertices of T are removed. We shall refer to these points as vertices. Obviously $f(D)$ can not cover any disc of radius $> \frac{l}{\sqrt{3}} = 1$, if $l = \sqrt{3}$ is the length of sides of T. Let $f(z) = \sum_{k=0}^{\infty} c_k z^k$. The assumption $\sum_{k=0}^{\infty} |c_k|^2 < +\infty$ leads to a contradiction as follows.

It is well known that the relation $\sum_{k=0}^{\infty} |c_k|^2 < +\infty$ implies the existence of the radial limit $f(e^{i\varphi}) = \lim_{r\to 1-0} f(re^{i\varphi})$ for almost every φ. If $e^{i\varphi}$ is not a vertex of a circular triangle obtained by repeated inversion, the radius $re^{i\varphi}$, $0 \le r \le 1$ meets infinitely many of inverted arcs and accordingly the curve $f(re^{i\varphi})$, $0 \le r < 1$ meets infinitely often linear segments corresponding by reflection to the sides of T.

There exist at least two (moreover six) different terms in the sequence of intersected segments. In fact, the neighbouring terms are certainly different being images of different sides of a circular triangle by a one-to-one mapping.

Therefore, if $\lim_{r\to 1} f(re^{i\varphi})$ exists, it must be the joining point of (at least) two different segments, that is $f(e^{i\varphi})$ is a vertex. The set of vertices is denumerable and so the limit function $f(e^{i\varphi})$ has to be constant on a set of positive measure. By the well known theorem of M. and F. Riesz $f(z)$ would be constant in D.

4. Proof of Theorem 2. Let $f(z)$ be the function constructed in sec. **3**, $s_k = \sum_{n=1}^{k} |c_n|^2$. (Being $f'(z) \neq 0$, we have $s_k \neq 0$, $k = 1, 2, \ldots$.)

Now let us define our sequence in the following way:

$$f_p(z) = \frac{1}{\sqrt{s_{r_p}}} f(z^p).$$

If we write $f_p(z) = \sum_{k=0}^{\infty} c_k^{(p)} z^k$, then

$$\sum_{k=p}^{p+r_p} |c_k^{(p)}|^2 = \frac{1}{s_{r_p}} \sum_{k=1}^{r_p} |c_k|^2 = 1.$$

Of course, $f_p(D) = \frac{1}{\sqrt{s_{r_p}}} f(D)$ and we see that $f_p(D)$ does not contain any disc of radius $> \frac{1}{\sqrt{s_{r_p}}}$ and by (i) of sec. **3**, $\frac{1}{\sqrt{s_{r_p}}} \to 0$.

References

[1] E. LANDAU, *Darstellung und Begründung einige neuerer Ergebnisse der Funktionentheorie*, Berlin, Springer, 1929.

[2] W. SEIDEL – L. J. WALSH, On the derivatives of functions analytic in the unit circle and their radii of univalence and of p-valence, *Trans. of Amer. Math. Soc.*, 17(1942), 128 – 216.

[3] P. UNGÁR, Bloch Circles of Univalent Functions, *Comm. on Pure and Appl. Math.*, **18** (1965), 313 – 318.

[4] P. TURÁN, Problem 153., *Matematikai Lapok*, **52** (1966), 215.

ÜBER WALSH-FOURIERREIHEN MIT NICHTNEGATIVEN PARTIALSUMMEN

Von

F. SCHIPP

II. Lehrstuhl für Analysis der Eötvös Loránd Universität, Budapest

(Eingegangen am 30. Oktober 1968.)

Es sei $\{\varphi_n(t)\}$ $(n = 0, 1, 2, \ldots)$ ein im Intervall $[0, 1]$ definiertes Funktionensystem mit

$$|\varphi_n(t)| \leq 1 \qquad (t \in [0, 1]; \quad n = 0, 1, 2, \ldots), \tag{1}$$

ferner sei $\{\psi_n(t)\}$ $(n = 0, 1, 2, \ldots)$ das von $\{\varphi_n(t)\}$ erzeugte W-System. D. h., es ist $\psi_0(t) \equiv 1$, und für

$$n = \sum_{i=0}^{\infty} n_i 2^i \qquad (n_i = 0, 1)$$

ist

$$\psi_n(t) = \prod_{\substack{i \\ n_i = 1}} \varphi_i(t). \tag{2}$$

Ist $\{\psi_n(t)\}$ orthogonal und gleichnormiert, d.h. gilt

$$\int_0^1 \psi_n(t)\psi_m(t)\,dt = \delta_{n,m} c \text{ [1]} \qquad (n, m > 0)$$

mit einer positiven Konstante c, so nennen wir $\{\varphi_n(t)\}$ ein gleichnormiert stark multiplikativ orthogonales System (GSMS).[2]

Es sei $\{r_n(t)\}$ $(n = 0, 1, 2, \ldots)$ das Rademachersche System, d.h.

$$r_0(t) = \begin{cases} 1 & (0 \leq t < 1/2), \\ -1 & (1/2 \leq t < 1), \end{cases} \qquad r_0(t+1) = r_0(t), \tag{3}$$
$$r_n(t) = r_0(2^n t) \qquad (n = 1, 2, \ldots).$$

[1] $\delta_{n,m}$ bezeichnet das Kroneckersche Symbol: $\delta_{n,m} = \begin{cases} 1 & (n = m), \\ 0 & (n \neq m). \end{cases}$

[2] Siehe ALEXITS [1], S. 165.

Es ist bekannt, daß die Funktionen $\{r_n(t)\}$ im Intervall $[0, 1]$ ein GSMS bilden und das von ihnen erzeugte W-System das bekannte Walshsche Orthogonalsystem ist, dessen Elemente wir mit $\{W_n(t)\}$ $(n = 0, 1, 2, \ldots)$ bezeichnen.

S. Sidon [2] hat gezeigt, daß es eine Walsh-Reihe

$$\sum_{\nu=0}^{\infty} a_\nu W_\nu(t) \tag{4}$$

existiert, deren Partialsummen $S_n(t) = \sum_{\nu=0}^{n-1} a_\nu W_\nu(t)$ der Bedingung

$$\int_0^1 |S_n(t)|\,dt < K \qquad (n = 1, 2, \ldots) \tag{5}$$

genügen, deren Koeffizienten aber nicht gegen Null streben.

Daraus folgt, daß die Reihe (4) keine Walsh-Fourierreihe ist. Man kann fragen, ob die stärkere Bedingung

$$S_n(t) = \sum_{\nu=0}^{n-1} c_\nu W_\nu(t) \geq 0 \qquad (n = 1, 2, \ldots) \tag{6}$$

schon nach sich zieht, daß $\sum_{\nu=0}^{\infty} c_\nu W_\nu(t)$ eine Walsh-Fourierreihe ist?

In dieser Arbeit beantworten wir diese Frage. Es gilt nämlich der folgende

Satz. *Es existiert eine Walsh-Nullreihe*[3] $S(t) = \sum_{\nu=0}^{\infty} c_\nu W_\nu(t)$ *welche der Bedingung* (6) *genügt.*

Da eine Teilfolge der Partialsummen der Walsh-Fourier-Entwicklung von $f(x) \in L[0, 1]$ fast überall gegen $f(x)$ konvergiert ([3]), deshalb ist $S(t)$ keine Walsh-Fourierreihe.

Analoge Sätze gelten für trigonometrische Reihen [4] und Haar-Reihen [5].

1. Hilfssätze

Zum Beweis unseres Satzes benutzen wir einige Hilfssätze.

Hilfssatz 1. *Es sei*

$$D_{2^n}(t; k) = \prod_{\nu=0}^{n-1} \left[1 + r_\nu\left(\frac{k}{2^n}\right) r_\nu(t)\right] \tag{1.1}$$

$$(k = 0, 1, 2, \ldots, 2^n - 1; \quad n = 1, 2, \ldots)$$

[3] D.h. es ist $\lim_{n\to\infty} S_n(t) = 0$ fast überall in $[0, 1]$ und $\limsup_{\nu\to\infty} c_\nu > 0$.

und

$$P_n(t) = \sum_{k=0}^{2^n-1} W_{2^n+k\cdot 2^n}(t) D_{2^n}(t;k) \qquad (n = 1, 2, \ldots) \tag{1.2}$$

Dann gilt

a) $P_n(t) = \sum_{l=0}^{2^{2n}+2^n-1} b_l^{(n)} W_l(t)$

$$(b_l = 0;\ 0 \leq l < 2^n;\ b_l = \pm 2^{-n},\ 2^n \leq l < 2^{2n}+2^n), \tag{1.3}$$

b) $|P_n(t)| \equiv 1 \qquad (t \in [0, 1], \quad n = 1, 2, \ldots),$

c) $\left|\sum_{l=0}^{s} b_l^{(n)} W_l(t)\right| \leq 2 \qquad (t \in [0, 1], \quad 0 \leq s \leq 2^{2n}+2^n, \quad n = 1, 2, \ldots).$

Beweis von Hilfsatz 1. Die Behauptung (1.3) *b)* folgt unmittelbar aus den Gleichungen[4]

$$D_{2^n}(t;k) = \begin{cases} 2^n & \left\{t \in \left[\frac{k}{2^n}, \frac{k+1}{2^n}\right)\right\}, \\ 0 & \left\{t \in [0, 1),\ t \notin \left[\frac{k}{2^n}, \frac{k+1}{2^n}\right)\right\} \end{cases}$$

$$(k = 0, 1, 2, \ldots, 2^n-1; \quad n = 1, 2, \ldots).$$

Die Relationen (1.3) *a)* und *c)* ergeben sich aus

$$P_n(t) = \frac{1}{2^n} \sum_{k=0}^{2^n-1} W_{2^n+k\cdot 2^n}(t) D_{2^n}(t;k) = \frac{1}{2^n} \sum_{k=0}^{2^n-1} W_{2^n+k\cdot 2^n}(t) \sum_{m=0}^{2^n-1} W_m\left(\frac{k}{2^n}\right) W_m(t) =$$

$$= \frac{1}{2^n} \sum_{k=0}^{2^n-1} \sum_{m=0}^{2^n-1} W_m\left(\frac{k}{2^n}\right) W_{2^n+k2^n+m}(t).$$

Hilfssatz 2. *Es sei*

$$\varphi_i(t) = P_{2^{(i+1)^2}}(t) \qquad (i = 0, 1, 2, \ldots). \tag{1.4}$$

Dann bilden die Funktionen $\{\varphi_i(t)\}$ $(i = 0, 1, 2, \ldots)$ *ein GSMS.*

Beweis von Hilfssatz 2. Die Behauptung des Hilfssatzes folgt unmittelbar aus (1.3) *a)*, *b)* und (1.4).
Aus Hilfssatz 2 und aus (1.3) *b)* folgt, daß die Funktionen $\{\varphi_n(t)\}$ $(n = 0, 1, 2, \ldots)$ beschränk und mit derselben Verteilung vollständig unabhängig sind, und so gilt

Hilfssatz 3.

$$\operatorname{mes}\left\{\limsup_{n\to\infty} \frac{\varphi_0(t)+\varphi_1(t)+\ldots+\varphi_{n-1}(t)}{\sqrt{2n \log\log n}} = 1\right\} = 1, \tag{1.5}$$

[4] Siehe [3].

$$\text{(1.6)} \qquad \operatorname{mes}\left\{\liminf_{n\to\infty} \frac{\varphi_0(t)+\varphi_1(t)+\ldots+\varphi_{n-1}(t)}{\sqrt{2n\log\log n}} = -1\right\} = 1.$$

(Siehe: [6], S. 337–340)

HILFSSATZ 4. *Es sei*

$$\text{(1.7)} \qquad f_n(t) = \prod_{i=0}^{n-1}\left(1-\frac{1}{4}\varphi_i(t)\right) \qquad (n = 1, 2, \ldots).$$

Dann gilt

$$\text{(1.8)} \qquad \lim_{n\to\infty} f_n(t) = 0$$

fast überall in $[0, 1]$.

BEWEIS VON HILFSSATZ 4. Auf Grund der Voraussetzungen sind die Funktionen

$$\text{(1.9)} \qquad F_n(t) = \int_0^t f_n(u)\,du \qquad (t\in[0, 1];\ n = 1, 2, \ldots)$$

monoton zunehmend, weiterhin gilt

$$F_n(0) = 0,\ F_n(1) = 1 \qquad (n = 1, 2, \ldots).$$

Aus einem Satz von HELLY ([7], S. 137.) folgt, daß eine Teilfolge $F_{n_j}(t)$ $(n_1<n_2<\ldots)$ existiert, welche im Intervall $[0, 1]$ überall konvergiert. Es sei

$$F(t) = \lim_{j\to\infty} F_{n_j}(t).$$

Offensichtlich ist $F(t)$ auch monoton zunehmend.

Zu jedem $n(=0, 1, 2, \ldots)$ und $t\in[0, 1]$ gibt es ein (maximales) dyadisches Intervall $I_n(t) = [\alpha_n(t), \beta_n(t))$ $(t\in I_n(t))$ derart, daß $\varphi_n(u) = \text{const.}$ $(u\in I_n(t))$ ist. Offensichtlich gilt auch

$$\text{(1.10)} \qquad \begin{aligned} &\varphi_m(u) = \text{const.} && (u\in I_n(t),\ m\leq n),\\ &f_{n+1}(u) = \text{const.} && (u\in I_n(t)),\\ &\int_{I_n(t)} \varphi_m(u)\,du = 0 && (m>n). \end{aligned}$$

Daraus folgt, daß für $\gamma_n = \alpha_n, \beta_n$

$$F_{n+k}(\gamma_n)-F_{n+1}(\gamma_n) = \int_0^{\gamma_n} (f_{n+k}(u)-f_{n+1}(u))\,du =$$

$$\int_0^{\gamma_n} f_n(u)\left\{-\frac{1}{4}\varphi_{n+1}(u)-\frac{1}{4}\varphi_{n+2}(u)+\frac{1}{4^2}\varphi_{n+1}(u)\varphi_{n+2}(u)+\ldots\right\}du = 0$$

$$(k = 2, 3, \ldots;\quad n = 0, 1, 2, \ldots)$$

besteht, und so ist

$$F_{n+1}(\gamma_n) = F_{n+2}(\gamma_n) = \ldots = F(\gamma_n). \tag{1.11}$$

Aus (1.11) auf Grund von (1.10) für nicht dyadisch rationalen t ergibt sich

$$\frac{F(\beta_n(t)) - F(\alpha_n(t))}{\beta_n(t) - \alpha_n(t)} = \frac{F_{n+1}(\beta_n(t)) - F_{n+1}(\alpha_n(t))}{\beta_n(t) - \alpha_n(t)} = F'_{n+1}(t) = f_{n+1}(t)$$

$$(n = 0, 1, 2, \ldots),$$

und so gilt für fast allen $t \in [0, 1]$

$$\lim_{n\to\infty} f_n(t) = F'(t).$$

Wir zeigen nun, daß fast überall $\lim\limits_{n\to\infty} f_n(t) = 0$ besteht. Auf Grund der Ungleichung $1 + u < e^u$ bekommen wir

$$0 \leqq f_n(t) = \prod_{\nu=0}^{n-1} \left(1 - \frac{1}{4}\varphi_\nu(t)\right) < e^{-\sum\limits_{\nu=0}^{n-1} \frac{1}{4}\varphi_\nu(t)}.$$

Da nach Hilfssatz 3

$$\operatorname{mes}\left\{t : \limsup_{n\to\infty} \left(\sum_{\nu=0}^{n-1} \frac{1}{4}\varphi_\nu(t)\right) = +\infty\right\} = 1$$

ist, deshalb gilt

$$\liminf_{n\to\infty} f_n(t) = 0 \quad (\text{f.ü.a. in } [0, 1]),$$

womit Hilfssatz 4 bewiesen ist.

2. Beweis des Satzes

Es sei

$$S(t) = \prod_{i=0}^{\infty} \left(1 - \frac{1}{4}\varphi_i(t)\right), \quad f_m(t) = \prod_{i=0}^{m-1} \left(1 - \frac{1}{4}\varphi_i(t)\right) \tag{2.1}$$

$$(m = 1, 2, \ldots).$$

Da nach (1.3) *a)* (1.4) und (2.1) jedes Glied von $\varphi_m(t)$ eine Rademachersche Funktion enthaltet, deren Index größer als $2^{(m+1)^2} - 1$ ist, und da die Indexe der Rademacherschen Funktionen, die in $f_m(t)$ vorkommen, kleiner als $2^{m^2+1} + 1$ sind, bekommen wir aus (2.1), durch Multiplikation, eine Walsh-Reihe, in welche die einzelnen Funktionen $W_\nu(t)$ höchstens je einmal vorkommen.

Es sei

$$S(t) = \sum_{\nu=0}^{\infty} c_\nu W_\nu(t), \tag{2.2}$$

$$S_n(t) = \sum_{r=0}^{n-1} c_r W_r(t) \qquad (n = 1, 2, \ldots),$$

$$N_m = 2^{(m+1)^2} \qquad (m = 0, 1, 2, \ldots).$$

Dann auf Grund von (1.3) *b)*, (1.4), (2.1) und Hilfssatz 4 gilt

$$S_{N_m}(t) = f_m(t) \geq \frac{1}{2^m} \quad (m = 1, 2, \ldots),$$

$$\lim_{m\to\infty} S_{N_m}(t) = 0 \qquad (\text{f.ü.a. in } [0, 1]). \tag{2.3}$$

Ist $N_m \leq n \leq N_{m+1}$, dann ist $S_n(t)$ von der Gestalt

$$S_n(t) = S_{N_m}(t)\left\{1 - \frac{1}{4}\left\{\sum_{l=0}^{\lambda_n-1} b_l^{(\varrho_m)} W_l(t)\right\}\right\} -$$

$$- \frac{1}{4} b_{\lambda_n}^{(\varrho_m)} W_{\lambda_n}(t) \sum{}' c_l W_l(t) = A_n(t) + B_n(t) \tag{2.4}$$

$$(\varrho_m = 2^{(m+1)^2}, \quad N_m \leq \lambda_n \leq N_m^2 + N_m),$$

wobei sich die Summation in Σ' auf gewiße $l(\leq N_m)$ bezieht.

Aus (1.3) *c)* und (2.3) folgt

$$\frac{1}{2^{m+1}} \leq A_n(t) \leq 2S_{N_m}(t) \qquad (N_m \leq n \leq N_{m+1};\ m = 1, 2, \ldots). \tag{2.5}$$

Da endlich auf Grund (1.3) *a)*, (1.4) und (2.1)

$$|W_{\lambda_n}(t) \sum{}' c_l W_l(t)| \leq \sum_{l=0}^{N_m-1} c_l \leq \sum_{c_l \geq 0} 1 \leq \tag{2.6}$$

$$\leq \prod_{i=0}^{m-1} 2^{2(i+1)^2+2} \leq 2^{2(m^2+1)+2m} \leq 2^{(m+1)^2-m}$$

ilt, und $|b_{\lambda_n}^{(\varrho_m)}| \geq 2^{-\varrho_m}(N_m \leq \lambda_n \leq N_m^2 + N_m)$ besteht, deshalb bekommen wir aus (2.4), (2.5) und (2.6) die Ungleichungen

$$0 \leq \frac{1}{2^{m+1}} - \frac{1}{2^{m+2}} \leq S_n(t) \leq 2S_{N_m}(t) + \frac{1}{2^{m+2}}.$$

Daraus und aus (2.3) folgt die Behauptung unseres Satzes.

Literaturverzeichnis

[1] G. Alexits, *Konvergenzprobleme der Orthogonalreihen*, (Budapest, 1960).
[2] S. Sidon, Über orthogonale Entwicklungen, *Acta Sci. Math.*, **10** (1941–43), 206–253.
[3] N. J. Fine, On the Walsh funktions, *Trans. Amer. Math. Soc.*, **65** (1949), 372–414.
[4] Y. Katznelson, Trigonometric series with positive partial sums, *Bull. Amer. Math. Soc.*, **71** (1965), 718–719.
[5] L. G. Pál–L. Schipp, On the Haar- and Schauder-series, *Acta Sci. Math* (Im Druck.).
[6] A. Rényi, *Wahrscheinlichkeitsrechnung* (Berlin, 1962).
[7] A. Zygmund, *Trigonometric series*, Vol. I., (Cambridge, 1959).

ÜBER DIE DIVERGENZ DER WALSH-FOURIERREIHEN

Von

F. SCHIPP

II. Lehrstuhl für Analysis der Eötvös Loránd Universität, Budapest

(Eingegangen am 30. Oktober 1968)

Einleitung

Es sei $\{r_n(x)\}$ $(n = 0, 1, 2, \ldots)$ das Rademachersche System, $\{\psi_n(x)\}$ $(n = 0, 1, 2, \ldots)$ das Walshsche System und

$$D_n(x) = \sum_{\nu=0}^{n-1} \psi_\nu(x) \qquad (n = 1, 2, \ldots)$$

die n-te Walsh-Dirichletsche Kernfunktion[1]. Ist

$$n = \sum_{i=0}^{\infty} n_i 2^i \qquad (n_i = 0, 1),$$

dann gilt

$$D_n(x) = \psi_n(x) \sum_{i=0}^{\infty} n_i r_i(x) D_{2^i}(x) \qquad (n = 1, 2, \ldots), \tag{1}$$

wobei noch

$$D_{2^i}(x) = \prod_{\nu=0}^{i-1} (1 + r_\nu(x)) = \begin{cases} 2^i (x \in [0, 2^{-i})), \\ 0 \ (x \in [2^{-i}, 1)) \end{cases} \qquad (i = 0, 1, 2, \ldots) \tag{2}$$

besteht[2].

[1] In dieser Arbeit benutzen wir die in [1] eingeführte Bezeichnungen.

[2] Siehe z. B. [2].

Wir bezeichnen mit

$$S_n(f;\, x) = \sum_{\nu=0}^{n-1} c_\nu(f)\psi_\nu(x) = \int_0^1 f(x \overset{\circ}{+} t) D_n(t)\, dt \tag{3}$$

$$\left(c_\nu(f) = \int_0^1 f(t)\psi_\nu(t)\, dt \right)$$

die n-te Partialsumme der Walsh—Fourier-Entwicklung von $f(x)$, mit

$$\omega_p(f;\, \delta) = \sup_{0 \leq h \leq \delta} \left\{ \int_0^1 |f(x \overset{\circ}{+} h) - f(x)|^p\, dx \right\}^{1/p} \qquad (p \geqq 1)$$

den $L_p - W$-Stetigkeitsmodul der Funktion $f(x)$.

In dieser Arbeit werden wir die folgenden Sätze beweisen.

SATZ 1. *Genügt die Funktion $f(x) \in L\,[0, 1]$ der Strukturellen Bedingung*

$$\sum_{i=0}^{\infty} \int_0^1 \int_0^1 |f(x \overset{\circ}{+} u) - f(x)|\, D_{2^i}(u)\, du\, dx < \infty, \tag{4}$$

so konvergiert die Entwicklung (3) *fast überall.*

Daraus ergibt sich

SATZ 2. *Ist*

$$\sum_{n=1}^{\infty} \frac{\omega_1\left(f;\, \frac{1}{n}\right)}{n} < \infty, \tag{5}$$

dann konvergiert die Entwicklung (3) *fast überall.*

Aus Satz 2 folgt, daß z. B. im Falle $\omega_1(f;\, \delta) = O\left(\log \frac{1}{\delta}\right)^{-1-\varepsilon}$ $(\varepsilon > 0)$ die Walsh-Fourierreihe von $f(x)$ fast überall konvergiert.

Wir werden zeigen, daß die Funktion $\left(\log \frac{1}{\delta}\right)^{-1-\varepsilon}$ durch $\left(\log \log \frac{1}{\delta}\right)^{-1}$ nicht ersetz werden kann. Es gilt nämlich

SATZ 3. *Es existiert eine Funktion $F_1(x) \in L[0, 1]$, welche die Forderung*

$$\omega_1(F_1;\, \delta) = O\left(\frac{1}{\log \log \frac{1}{\delta}} \right) \tag{6}$$

erfüllt, deren Walsh-Fourierreihe aber überall divergiert.

Analoge Sätze gelten für Fourierreihen (Siehe: [3], S. 172, [4]).

Wir geben noch eine andere strukturelle Bedingung für die Konvergenz der Walsh-Fourierreihe.

SATZ 4. *Genügt die Funktion $f(u)\in L[0,1]$ für $x\in E$ der strukturellen Bedingung*

$$\frac{1}{h}\int_0^h |f(x\overset{\circ}{+}u)-f(x)|\,du = O\left(\frac{1}{\log\frac{1}{h}}\right), \tag{7}$$

so konvergiert die Entwicklung (3) *auf E fast überall.*

Wir werden zeigen, daß Satz 4 nicht verschärft werden kann. Es gilt nämlich

SATZ 5. *Sei $\varrho(u)\geqq 0$ eine nicht abnehmende Funktion, welche der Bedingung*

$$\lim_{u\to+0}\varrho(u)\log 1/u = +\infty \tag{8}$$

genügt, so gibt es eine Funktion $F_2(x)\in L[0,1]$, welche in fast allen $x\in[0,1]$ die Forderung

$$\frac{1}{h}\int_0^h |F_2(x\overset{\circ}{+}u)-F_2(x)|\,du = O(\varrho(h)) \tag{9}$$

erfüllt, deren Walsh-Fourierreihe aber fast überall divergiert.

J. MARCINKIEWICZ [5] hat analoge Sätze für Fourierreihen bewiesen.

Endlich beweisen wir

SATZ 6. *Es seien $\Phi(u)$ und $\Lambda(u)$ $(u\in(0,+\infty))$ nicht abnehmende stetige Funktionen, welche der Bedingung*

$$\begin{aligned} &\Phi(u).\Lambda(u) = \log\log u \qquad (u\in(2,+\infty)),\\ &\Phi(u) = \Lambda(u) = 0 \qquad (u\in[0,2]) \end{aligned} \tag{10}$$

genügen. Es sei weiterhin $\{\lambda_n\}$ $(n=1,2,\ldots)$ eine positive, monoton nicht abnehmende Zahlenfolge mit $\lim\limits_{n\to\infty}\lambda_n=\infty$, $\lambda_n = o(\Lambda(n))$. Dann existiert eine Funktion $F_3(x)$, welche die Forderung

$$\int_0^1 |F_3(x)|\,\Phi(|F_3(x)|)\,dx < \infty \tag{11}$$

erfüllt und fast überall der Bedingung

$$\limsup_{n\to\infty}\frac{|S_n(f;x)|}{\lambda_n} > 0 \tag{12}$$

genügt.

Dieser Satz ist eine Verallgemeinerung eines Satzes des Verfassers. Einen analogen Satz hat K. TANDORI [6] für trigonometrische Fourierreihen erwähnt.

§ 1. Beweis der Sätze 1–3

Beweis von Satz 1. Aus der Bedingung (4) folgt, daß in fast allen $x \in [0, 1]$

$$\sum_{i=0}^{\infty} \int_0^1 |f(x \overset{\circ}{+} u) - f(x)| D_{2^i}(u)\, du < \infty \tag{1.1}$$

gilt. Es sei $\varepsilon > 0$ eine beliebige Zahl. Dann, auf Grund von (1.1) gibt es einen Index $i_0 = i_0(\varepsilon, x)$ derart, daß

$$\sum_{i=i_0+1}^{\infty} \int_0^1 |f(x \overset{\circ}{+} u) - f(x)| D_{2^i}(u)\, du < \varepsilon$$

besteht. Daraus, und aus (1) und (3) erhalten wir

$$|S_n(f; x) - f(x)| = \left| \int_0^1 \big(f(x \overset{\circ}{+} u) - f(x)\big) D_n(u)\, du \right| \leqq$$

$$\leqq \sum_{i=0}^{i_0} \left| \int_0^1 \eta_n(u) \big(f(x \overset{\circ}{+} u) - f(x)\big) r_i(u) D_{2^i}(u)\, du \right| +$$

$$+ \sum_{i=i_0+1}^{\infty} \int_0^1 |f(x \overset{\circ}{+} u) - f(x)| D_{2^i}(u)\, du \leqq$$

$$\leqq \sum_{i=0}^{i_0} c_n(\varphi_{i,x}) + \varepsilon \qquad \big(\varphi_{i,x}(u) = (f(x \overset{\circ}{+} u) - f(x))\, r_i(u) D_{2^i}(u)\big),$$

woraus sich auf Grund der Gleichungen $\lim\limits_{n \to \infty} c_n(\varphi_{i,x}) = 0$ $(i = 0, 1, 2, \ldots)$ die Behauptung von Satz 1 ergibt.

Beweis von Satz 2. Aus (5) folgt

$$\sum_{i=0}^{\infty} \omega_1(f; 2^{-i}) < \infty,$$

woraus sich auf Grund der Ungleichung

$$\int_0^1 \int_0^1 |f(x \overset{\circ}{+} u) - f(x)| D_{2^i}(u)\, du\, dx = \int_0^1 D_{2^i}(u) \left(\int_0^1 |f(x \overset{\circ}{+} u) - f(x)|\, dx \right) du =$$

$$= 2^i \int_0^{2^{-i}} \left(\int_0^1 |f(x \overset{\circ}{+} u) - f(x)|\, dx \right) du \leqq \omega_1(f; 2^{-i})$$

und nach Satz 1 die Behauptung des Satzes 2 ergibt.

Zum Beweis der Sätze 3, 5 und 6 benutzen wir den folgenden Hilfssatz [2]:

HILFSSATZ 1. *Für jede Zahl* $k(=1, 2, \ldots)$ *kann man ein W-Polynom*

$$P_k(x) = 2^{-2k} \sum_{\nu=0}^{2^{2k}-1} D_{2^{2^{2k+1}}}(x \dotplus c_\nu^{(k)}) = \sum_{l=0}^{2^{2^{2k+1}}-1} a_l^{(k)} \psi_l(x) \tag{1.2}$$

$$\left| \frac{\nu}{2^{2k}} \leqq c_\nu^{(k)} < \frac{\nu+1}{2^{2k}}; \quad \nu = 0, 1, \ldots 2^{2k}-1, \quad k = 1, 2, \ldots \right|$$

und eine Folge $\{H_n^{(k)}\}$ $(n = 0, 1, 2, \ldots, 2^{2k}-1)$ *von meßbaren Mengen mit den folgenden Eigenschaften angeben:*

$$\begin{aligned}
&a) \quad H_n^{(k)} \cap H_{n'}^{(k)} = 0 \quad (n \neq n'), \quad \bigcup_{n=0}^{2^{2k}-1} H_n^{(k)} = [0, 1); \\
&b) \quad P_k(x) \geqq 0 \qquad (x \in [0, 1)); \\
&c) \quad \int_0^1 P_k(x)dx = 1; \\
&d) \quad \text{für } n = 0, 1, 2, \ldots, 2^{2k}-1 \text{ und } x \in H_n^{(k)} \text{ gilt} \\
&\qquad |S_\mu(P_k; x)| \geqq \frac{k}{3} - 1,
\end{aligned} \tag{1.3}$$

wobei $\mu = 2^{2^{2k}+n} + \sum_{\nu=0}^{k} 2^{2\nu}$ *ist.*

BEWEIS VON SATZ 3. Es sei $k_i = 2^i$, $N_i = 2^{2^{2k_i+1}}$ $(i = 1, 2, \ldots)$, und $N_0 = 1$. Bilden wir die (geklammerte) Walsh-Reihe

$$F_1(x) = \sum_{i=1}^{\infty} \frac{1}{k_i} \psi_{N_i}(x) P_{k_i}(x). \tag{1.4}$$

Da für jedes $i(=1, 2, \ldots)$ $2N_i - 1 < N_{i+1}$ gilt, kommen in den verschiedenen Gliedern die einzelnen Funktionen $\psi_\nu(x)$ höchstens je einmal vor.

Aus den Eigenschaften (1.3) *b)* und *c)* folgt

$$\sum_{i=1}^{\infty} \frac{1}{k_i} \int_0^1 |\psi_{N_i}(x) P_{k_i}(x)| \, dx = \sum_{i=1}^{\infty} \frac{1}{2^i} \int_0^1 P_{k_i}(x) \, dx < \infty,$$

und so konvergiert die Reihe (1.4) fast überall gegen eine Funktion $F_1(x) \in L[0, 1]$, weiterhin aus (1.4) durch Weglassen der Klammern erhalten wir die Walsh-Entwicklung von $F_1(x)$.

Wir zeigen nun, daß

$$\omega_1(F_1, \delta) = O\left(\frac{1}{\log \log \frac{1}{\delta}} \right) \tag{1.5}$$

gilt. Es sei $0<h\leqq 1$. Dann gibt es einen Index $i_0 = i_0(h)$ derart, daß $N_{i_0+1}^{-1} < h \leqq N_{i_0}^{-1}$ besteht. Da $\psi_{N_i}(x \dot{+} h)D_{N_i}(y \dot{+} h) = \psi_{N_i}(x)D_{N_i}(y)$ $(i<i_0)$ gilt, deshalb ist

$$\int_0^1 |F_1(x \dot{+} h) - F_1(x)|\,dx \leqq 2 \sum_{i=i_0}^{\infty} \frac{1}{k_i} \int_0^1 |\psi_{N_i}(x)P_{k_i}(x)|\,dx =$$

$$= 2 \sum_{i=i_0}^{\infty} \frac{1}{2^i} = \frac{4}{2^{i_0}} = O\left(\frac{1}{\log\log\frac{1}{h}}\right),$$

und so ist die Behauptung (1.5) bewiesen.

Endlich zeigen wir, daß die Walsh-Entwicklung von $F_1(x)$ in $[0, 1)$ überall divergiert. Auf Grund der Eigenschaft (1.3) *a)* der Mengen $H_n^{(k)}$ kann man zu jedem $x \in [0, 1)$ eine Indexfolge $n_i = n_i(x)$ derart angeben, daß $0 \leq n_i < 2^{2k_i}$ und $x \in H_{n_i}^{(k_i)}$ $(i = 1, 2, \ldots)$ besteht. Es sei $\mu_i = \mu_i(x) = 2^{2^{2k_i + n_i(x)}} + \sum_{r=0}^{k_i} 2^{2r}$. Dann, auf Grund von (1.4) und (1.3) *d)* ergibt sich für genügend große i die Ungleichung

$$|S_{N_i+\mu_i}(F_1;\, x) - S_{N_i}(F_1;\, x)| = \frac{1}{k_i} |\psi_{N_i}(x) S_{\mu_i}(x;\, P_{k_i})| \geqq \left(\frac{k_i}{3} - 1\right)\frac{1}{k_i} > \frac{1}{6}.$$

Damit haben wir den Satz 3 bewiesen.

§ 2. Beweis der Sätze 4, 5

Zum Beweis von Satz 4 benutzen wir den folgenden

Hilfssatz 2. *Es sei* $\{I_\nu\}$ $(\nu = 1, 2, \ldots)$ *ein System von disjunkten dyadische Intervalle mit* $I_\nu = \left[\frac{a_\nu}{2^{m_\nu}}, \frac{a_\nu+1}{2^{m_\nu}}\right)$ $(a_\nu < 2^{m_\nu}$, a_ν *ganz*), *und* $U = \bigcup_{\nu=1}^{\infty} I_\nu$, $V = [0, 1] - U$. *Ist* $g(x) \in L[0, 1]$ *eine Funktion, welche auf* V *den Wert* $g(x) = 0$ *hat und gilt*

$$\frac{1}{|I_\nu|} \int_{I_\nu} |g(u)|\,du = O\left(\frac{1}{m_\nu}\right), \tag{2.1}$$ [3]

so konvergiert die Walsh–Fourier-Entwicklung der Funktion $g(x)$ *auf* V *fast überall.*

[3] $|I_\nu|$ bedeutet das Lebesquesche Maß von I_ν.

BEWEIS VON HILFSSATZ 2. Es sei

$$g_n(x) = \begin{cases} \dfrac{1}{|I_\nu|} \displaystyle\int_{I_\nu} g(t)\psi_n(t)\,dt & (x \in I_\nu;\quad \nu = 1, 2, \ldots), \\ 0 & (x \in V); \end{cases}$$

$$G_n(x) = \sup_{\nu \geq n} |g_\nu(x)|; \tag{2.2}$$

$$G_n^*(x) = \begin{cases} m_\nu G_n(x) & (x \in I_\nu;\ \nu = 1, 2, \ldots), \\ 0 & (x \in V). \end{cases}$$

Offensichtlich gilt

$$G_1^*(x) \geq G_2^*(x) \geq \ldots, \quad \lim_{n\to\infty} G_n^*(x) = 0 \qquad (x \in [0, 1)),$$

weiterhin auf Grund von (2.1) und (2.2) ergibt sich

$$\int_0^1 G_n^*(x)\,dx = \sum_{\nu=1}^{\infty} m_\nu \int_0^1 G_n(x)\,dx \leq \sum_{\nu=1}^{\infty} m_\nu \int_{I_\nu} \left(\frac{1}{|I_\nu|} \int_{I_\nu} |g(u)|\,du \right) dx =$$

$$= \sum_{\nu=1}^{\infty} m_\nu \int_{I_\nu} |g(u)|\,du = O(1) \sum_{\nu=1}^{\infty} |I_\nu| = O(1).$$

Daraus folgt

$$\lim_{n\to\infty} \int_0^1 G_n^*(x)\,dx = 0. \tag{2.3}$$

Aus (1), (2), (3) und (2.2) ergibt sich

$$\int_0^1 (g_n(u) - \psi_n(u)g(u)) \sum_{\nu=1}^{\infty} n_i r_i(x \dot{+} u) D_{2^i}(x \dot{+} u)\,du = 0 \qquad (x \in V),$$

und so ist

$$|S_n(g; x)| \leq \sum_{i=0}^{\infty} \int_0^1 |g_n(u)| D_{2^i}(x \dot{+} u)\,du \qquad (x \in V).$$

Da

$$T_n(g; x) = \sup_{\nu \geq n} |S_\nu(g; x)| \leq \sum_{i=0}^{\infty} \int_0^1 G_n(u) D_{2^i}(x \dot{+} u)\,du \qquad (x \in V),$$

und

$$D_{2^i}(x \dot{+} u) = 0 \ \ (u \in I_\nu,\ x \in V,\ i \geq m_\nu), \quad \int_V D_{2^i}(x \dot{+} u)\,dx \leq 1$$

gilt, deshalb ist nach (2.3)

$$\int_V T_n(g;x)\,dx \leqq \sum_{i=0}^{\infty} \int_V \left(\int_0^1 G_n(u) D_{2^i}(x \dot{+} u)\,du \right) dx =$$

$$= \sum_{i=0}^{\infty} \int_0^1 G_n(u) \left(\int_V D_{2^i}(x \dot{+} u)\,dx \right) du = \sum_{i=0}^{\infty} \sum_{\nu=1}^{\infty} \int_{I_\nu} G_n(u) \left(\int_V D_{2^i}(x \dot{+} u)\,dx \right) du \leqq$$

$$\leqq \sum_{\nu=1}^{\infty} \left(\int_{I_\nu} G_n(u)\,du \right) \sum_{i=0}^{m_\nu - 1} 1 = \sum_{\nu=1}^{\infty} m_\nu \int_{I_\nu} G_n(u)\,du = \int_0^1 G_n^*(u)\,du \to 0 \qquad (n \to \infty).$$

Nach dem Satz von B. Levi ist also

$$\lim_{n\to\infty} T_n(g;x) = \limsup_{n\to\infty} |S_n(g;x)| = 0$$

fast überall auf V, womit Hilfssatz 2 bewiesen ist.

Beweis von Satz 4. Wir bezeichnen mit E_n $(n = 1, 2, \ldots)$ die Menge der Punkte $x \in E$, in welchen

$$2^\nu \int_0^{2^{-\nu}} |f(x \dot{+} u) - f(x)|\,du \leqq \frac{n}{\nu} \qquad (\nu \geqq n) \tag{2.4}$$

gilt. Offensichtlich ist $\lim_{n\to\infty} |E_n| = |E|$, weiterhin zu jeder Menge E_n gibt es ein System $\{I_\nu^{(n)}\}$ $(\nu = 1, 2, \ldots)$ von disjunkten dyadische Intervalle derart, daß

$$V_n = [0, 1] - \bigcup_{\nu=1}^{\infty} I_\nu^{(n)} = [0, 1] - U_n \subset E_n$$

gilt und $|E_n - V_n|$ beliebig klein ist. Es ist also genug zu zeigen, daß die Entwicklung (3) auf jeder Menge V_n fast überall konvergiert.

Es sei nun n fix und $V_n = V$, $I_\nu^{(n)} = I_\nu$, $U_n = U$. Für $x \in V$ bezeichne $E(x, \nu)$ $(\nu = n, n+1, \ldots)$ die Menge aller Punkte $z = x \dot{+} u$ $(0 \leqq u < 2^{-\nu})$, in welchen

$$|f(z) - f(x)| > \frac{4n}{\nu}$$

gilt. Dann ist

$$\frac{n}{\nu} \geqq 2^\nu \int_0^{2^{-\nu}} |f(x \dot{+} u) - f(x)|\,du \geqq 2^\nu \frac{4n}{\nu} |E(x, \nu)|,$$

also

$$|E(x, \nu)| \leqq 2^{-(\nu+2)}. \tag{2.5}$$

Es seien x und y zwei beliebigen Punkte aus V mit

$$\frac{1}{2^{\nu+1}} \leqq x \overset{\circ}{+} y < \frac{1}{2^{\nu}} \leqq \frac{1}{2^{n}}.$$

Auf Grund von (2.5) gilt $|E(x, \nu) \cup E(y, \nu)| < \frac{1}{2^{\nu+1}}$ und daher gibt es einen Punkt $\xi = x \overset{\circ}{+} u = y \overset{\circ}{+} v$ $(0 \leqq u, v < 2^{-\nu})$ derart, daß $\xi \notin E(x, \nu) \cup E(y, \nu)$ gilt. Das bedeutet so viel wie

$$|f(\xi) - f(x)| \leqq \frac{4n}{\nu}, \qquad |f(\xi) - f(y)| \leqq \frac{4n}{\nu},$$

woraus sich für ein beliebiges Punktepaar $x, y \in V$ die Ungleichung

$$|f(x) - f(y)| \leqq \frac{K}{\log \frac{1}{x \overset{\circ}{+} y}} \tag{2.6}$$

ergibt. Man kann annehmen, daß für die Darstellung von

$$U = \bigcup_{\nu=1}^{\infty} I_\nu \left| I_\nu = \left[\frac{a_\nu}{2^{m_\nu}}, \frac{a_\nu + 1}{2^{m_\nu}}\right)\right|$$

$$\left| I_\nu \overset{\circ}{+} \frac{1}{2^{m_\nu}} \right| \cap V \neq 0 \tag{2.7}$$

gilt. Wir führen nun eine Funktion $g(x)$ ein:

$$g(x) = \begin{cases} 0 & (x \in V), \\ f(x) - f(x_\nu) & (x \in I_\nu; \quad \nu = 1, 2, \ldots), \end{cases} \tag{2.8}$$

wobei $x_\nu \in \left| I_\nu \overset{\circ}{+} \frac{1}{2^{m_\nu}} \right| \cap V$ einen beliebige Punkt bedeutet.

Auf Grund der Ungleichung

$$\frac{1}{|I_\nu|} \int_{I_\nu} |g(u)| \, du \leqq \frac{1}{|I_\nu|} \int_{I_\nu \cup \left(I_\nu \overset{\circ}{+} 2^{-m_\nu}\right)} |g(u)| \, du = 2^{m_\nu} \int_0^{2^{-m_\nu+1}} |f(x_\nu \overset{\circ}{+} u) - f(x_\nu)| \, du \leqq \frac{K_1}{m_\nu}$$

erfüllt die Funktion $g(x)$ die Forderungen des Hilfssatzes 2, daher konvergiert ihre Walsh-Entwicklung auf V fast überall.

Betrachten wir nun die Funktion

$$h(x) = \begin{cases} f(x) & (x \in V), \\ f(x_\nu) & (x \in I_\nu; \quad \nu = 1, 2, \ldots), \end{cases}$$

wobei x_ν die in (2.8) eingeführten Punkten bedeuten. Auf Grund von (2.6) und (2.7) ergibt sich, daß die Funktion $h(x)$ der Bedingung

$$|h(x)-h(y)| \leqq \frac{K_2}{\log \frac{1}{x \dot{+} y}}$$

genügt, woraus nach einem Satz von L. G. PÁL ([7], Theorem 4.3) die Konvergenz der Walsh-Entwicklung von $f(x)$ in fast allen Punkten folgt.

Die Behauptung des Satzes folgt somit aus der Gleichung

$$f(x) = g(x)+h(x).$$

BEWEIS VON SATZ 5. Es sei $q(t)=\varrho(t)\log\frac{1}{t}$. Dann ist $\lim\limits_{t\to+0} q(t) = +\infty$ und man kann ohne Beschränkung der Allgemeinheit annehmen, daß die Funktion $q(t)$, und so die Funktion $\varrho(t)/t$ $(0<t\leqq 1)$ auch, monoton nicht wachsend ist. Daraus folgt die Ungleichung

$$\alpha\varrho(t) = \alpha t\,\frac{\varrho(t)}{t} < \alpha t\,\frac{\varrho(\alpha t)}{\alpha t} = \varrho(\alpha t) \tag{2.9}$$

$$(0<\alpha\leqq 1;\quad 0<t\leqq 1).$$

Auf Grund der Relation $\lim\limits_{t\to+0} q(t) = +\infty$ gibt es eine Nullfolge $\{\varepsilon_k\}$ $(k = 1, 2, \ldots; 0\leqq\varepsilon_k<1)$ derart, daß

$$\lim_{k\to\infty} \varepsilon_k^3\, \varrho\left(\frac{1}{2^{2k}}\right) k = +\infty \tag{2.10}$$

besteht. Es sei $f_k(x) = \varepsilon_k^3\varrho\left(\frac{1}{2^{2k}}\right)P_k(x)$ $(k=1, 2, \ldots)$, wobei $P_k(x)$ die in Hilfssatz 1 eingeführte Funktion bedeutet. Wir bezeichnen mit $l(x)$ $(0<x<1)$ die natürliche Zahl, welche der Bedingung $\frac{1}{2^{l(x)+1}} < x \leqq \frac{1}{2^{l(x)}}$ genügt, mit $J_r(x)$ das dyadische Intervall von der Länge 2^{-r}, welche den Punkt x enthaltet und mit E_k die Menge

$$E_k = \bigcup_{r=0}^{2^{2k}-1} J_{m_k}(c_r^{(k)}) \qquad (k = 1, 2, \ldots), \tag{2.11}$$

wobei $m_k=\min\left\{l\left(\frac{\varepsilon_k}{2^{2k}}\right),\ 2^{2k}-1\right\}$ und $c_r^{(k)}$ die in (1.2) eingeführte Zahlen bedeuten.

Wir zeigen, daß

$$\frac{1}{h}\int_0^h |f_k(x \dot{+} u)-f_k(x)|\,du < 2\varrho(h)\varepsilon_k \tag{2.12}$$

$$(0<h\leqq 1,\ x\notin E_k;\ k = 1, 2, \ldots)$$

gilt. Für $x \notin E_k$ besteht $f_k(x) = 0$. Daraus folgt, daß für $0 \leqq u < h < \frac{1}{2^{m_k}}$ die Gleichung $f_k(x \overset{\circ}{+} u) = 0$ $(x \notin E_k)$ besteht und so ist die Behauptung (2.12) für $0 < h \leqq \frac{1}{2^{m_k}}$ richtig.

Ist $\frac{1}{2^{m_k}} < h \leqq \frac{1}{2^{2k}}$, dann auf Grund von (2), (1.2), (2.9), (2.10) und (2.11) für $x \notin E_k$ ergibt sich:

$$\frac{1}{h}\int_0^h |f_k(x \overset{\circ}{+} u) - f_k(x)|\, du = \varepsilon_k^3 \varrho\left(\frac{1}{2^{2k}}\right) \frac{1}{h}\int_0^h P_k(x \overset{\circ}{+} u)\, du \leqq$$

$$\leqq \varepsilon_k^3 \varrho\left(\frac{1}{2^{2k}}\right) 2^{m_k} \int_0^{2^{-2k}} P_k(x \overset{\circ}{+} u)\, du = \varepsilon_k^3 \varrho\left(\frac{1}{2^{2k}}\right) \frac{\varepsilon_k}{2^{2k}} 2^{m_k} < \varepsilon_k^2 \varrho\left(\frac{1}{2^{2k}}\right) <$$

$$< \varepsilon_k \varrho\left(\frac{\varepsilon_k}{2^{2k}}\right) < \varepsilon_k \varrho\left(\frac{1}{2^{m_k}}\right) < \varepsilon_k \varrho(h).$$

Ist endlich $\frac{1}{2^{2k}} \leqq h \leqq 1$, dann aus (1.2) folgt

$$\frac{1}{h}\int_0^h |f(x \overset{\circ}{+} u) - f(x)|\, du \leqq 2^{l(h)+1}\left(\int_0^{2^{-l(h)}} P_k(x \overset{\circ}{+} u)\, du\right) \varepsilon_k^3 \varrho\left(\frac{1}{2^{2k}}\right) =$$

$$= 2 \cdot 2^{l(h)}\left(\int_{J_{l(h)}(x)} P_k(u)\, du\right) \varepsilon_k^3 \varrho\left(\frac{1}{2^{2k}}\right) = 2\varepsilon_k^3 \varrho\left(\frac{1}{2^{2k}}\right) < 2\varepsilon_k \varrho\left(\frac{1}{2^{2k}}\right) < 2\varepsilon_k \varrho(h),$$

womit (2.12) bewiesen ist.

Es sei k_i $(k_1 < \ldots < k_i < \ldots)$ eine Folge mit $\sum_{i=1}^{\infty} \varepsilon_{k_i} < 1$, $N_i = 2^{2^{2k_i+1}}$ und wir bilden die Reihe

$$F_2(x) = \sum_{i=1}^{\infty} f_{k_i}(x) \cdot \psi_{N_i}(x). \tag{2.13}$$

Aus den Eigenschaften (1.3) *b)* und *c)* folgt

$$\sum_{i=1}^{\infty} \int_0^1 |\psi_{N_i}(x) f_{k_i}(x)|\, dx = \sum_{i=0}^{\infty} \varepsilon_{k_i}^3 \varrho\left(\frac{1}{2^{2k_i}}\right) < \varrho\left(\frac{1}{2^{2k_1}}\right) \sum_{i=1}^{\infty} \varepsilon_{k_i} < \varrho\left(\frac{1}{2^{2k_1}}\right).$$

Hieraus bekommen wir, daß die Reihe (2.13) auf einer Menge H, mit $|H| = 1$ gegen eine integrierbare Funktion $F_2(x)$ konvergiert, weiterhin kann man zeigen, daß die Reihe (2.13) die Walsh-Entwicklung der Funktion $F_2(x)$ ist.

Es sei $E = H - \bigcap_{i=1}^{\infty} \bigcup_{j=1}^{\infty} E_{k_j}$. Offensichtlich gilt $|E| = 1$. Wir zeigen jetzt, daß $F_2(x)$ für $x \in E$ die Forderung (9) erfüllt.

Ist $x \in E$, dann gibt es einen Index $s = s(x)$ derart, daß $x \notin E_{k_i}$ $(i > s)$ gilt. Daraus und aus (2.12) folgt

$$\frac{1}{h}\int_0^h |F_2(x \dot{+} u) - F_2(x)|\, du \leq \frac{1}{h}\int_0^h \sum_{i=1}^{s} |f_{k_i}(x \dot{+} u) - f_{k_i}(x)|\, du +$$

$$+ \sum_{i=s+1}^{\infty} \frac{1}{h}\int_0^h |f_{k_i}(x \dot{+} u) - f_{k_i}(x)|\, du \leq$$

$$\leq \frac{1}{h}\sum_{i=1}^{s}\int_0^h |f_{k_i}(x \dot{+} u) - f_{k_i}(x)|\, du + 2\varrho(h) \sum_{i=s+1}^{\infty} \varepsilon_{k_i}.$$

Da endlich für genügend kleines u $f_{k_i}(x \dot{+} u) = f_{k_i}(x)$ $(i = 1, 2, \ldots s)$ gilt, bekommen wir die zu bewiesende Behauptung (9).

Die Divergenz der Walsh-Fourierreihe von $F_2(x)$ folgt unmittelbar aus

$$S_{N_i} + \mu_i(F_2; x) - S_{N_i}(F_2; x) =$$

$$= \varepsilon_{k_i}^3 \varrho\left(\frac{1}{2^{2k_i}}\right) \psi_{N_i}(x) S\mu_i(x; P_{k_i}) \geq \left(\frac{k_i}{3} - 1\right) \varepsilon_{k_i}^3 \varrho\left(\frac{1}{2^{2k_i}}\right) \to +\infty,$$

$$(i \to \infty),$$

wobei $n_i = n_i(x) < 2^{2k_i}$ die Indexfolge bedeutet, welche der Bedingung $x \in H_{n_i}^{(k_i)}$ $(i = 1, 2, \ldots)$ genügt und $\mu_i = \mu_i(x) = 2^{2^{2k_i - n_i(x)} + \sum_{r=0}^{k_i} 2^{2r}}$ gesetz wird.

Beweis von Satz 6. Es sei $\lambda_N = \varepsilon_N \cdot l(N)$ $(N = 1, 2, \ldots)$. Auf Grund der Relationen

$$\varepsilon_N \to 0 \quad (N \to \infty), \qquad \frac{\varepsilon_N}{\Phi(N)} \to 0 \quad (N \to \infty),$$

$$\frac{\varepsilon_N \cdot N}{\log N \Phi(N)} = \frac{\varepsilon_N \cdot l(N) N}{\log N \cdot \log\log N} = \frac{\lambda_N \cdot N}{\log N \cdot \log\log N} \to \infty \qquad (N \to \infty)$$

gibt es eine Indexfolge $N_i = 2^{2^{2k_i - 1}}$ $(k_1 < k_2 < \ldots)$ derart, daß

$$\sum_{i=1}^{\infty} \varepsilon_{N_i} = \infty,$$

$$\frac{\varepsilon_{N_i} \cdot N_i}{2^{2k_i} \Phi(N_i)} < \frac{1}{2} \frac{\varepsilon_{N_{i+1}} \cdot N_{i+1}}{2^{2k_{i+1}} \Phi(N_{i+1})} \qquad (i = 1, 2, \ldots), \tag{2.14}$$

$$\frac{\varepsilon_{N_i}}{\Phi(N_i)} < \frac{1}{2} \qquad (i = 1, 2, \ldots)$$

bestehen.

Bilden wir die Reihe

$$F_3(x) = \sum_{i=1}^{\infty} \frac{\varepsilon_{N_i}\psi_{N_i}(x)P_{k_i}(x)}{\Phi(N_i)}, \tag{2.15}$$

wobei $P_{k_i}(x)$ die im Hilfssatz 1 eingeführte Funktion bedeutet. Aus (1.3) *b)*, *c)* und (2.14) folgt, daß die Partialsummen

$$S_{N_n}(x) = \sum_{i=1}^{n-1} \frac{\varepsilon_{N_i}\psi_{N_i}(x)P_{k_i}(x)}{\Phi(N_i)} \tag{2.16}$$

fast überall gegen eine Funktion $F_3(x) \in L[0, 1]$ konvergieren, weiterhin ergibt sich, daß die Reihe (2.15) die Walsh-Entwicklung der Funktion $F_3(x)$ ist.

Wir zeigen jetzt, daß $F_3(x)$ der Bedingung (11) genügt. Es sei

$$A_i = \{x : x \in [0, 1],\ P_{k_i}(x) > 0\} \qquad (i = 1, 2, \ldots),$$

$$B_j^{(n)} = A_j - \bigcup_{i=j+1}^{n} A_i \quad (j = 1, 2, \ldots n-1), \quad A_n = B_n^{(n)} \tag{2.17}$$

$$(n = 1, 2, \ldots).$$

Dann gilt

$$\bigcup_{j=1}^{n} B_j^{(n)} = \bigcup_{j=1}^{n} A_j, \quad B_j^{(n)} \cap B_{j'}^{(n)} = \emptyset \qquad (j \neq j'), \tag{2.18}$$

weiterhin aus (1.2), (2.14), (2.16) und (2.17) ergibt sich

$$|B_j^{(n)}| \leqq |A_j| = \frac{2^{2k_j}}{N_j},$$

$$|S_{N_{n+1}}(x)| \leqq \sum_{i=1}^{j} \frac{\varepsilon_{N_i}P_{k_i}(x)}{\Phi(N_i)} \leqq \sum_{i=1}^{j} \frac{\varepsilon_{N_i}\cdot N_i}{2^{2k_i}\Phi(N_i)} < \frac{2\varepsilon_{N_j}\cdot N_j}{2^{2k_j}\Phi(N_j)} < N_j$$

$$(x \in B_j^{(n)};\quad j = 1, 2, \ldots n).$$

Daraus und aus (2.14) und (2.18) folgt

$$\int_0^1 |S_{N_{n+1}}(x)|\,\Phi(|S_{N_{n+1}}(x)|)\,dx = \sum_{j=1}^{n} \int_{B_j^{(n)}} |S_{N_{n+1}}(x)|\,\Phi(|S_{N_{n+1}}(x)|)\,dx \leqq$$

$$\leqq \sum_{j=1}^{n} 2 \int_{B_j^{(n)}} \frac{\varepsilon_{N_j}\cdot N_j}{2^{2k_j}\Phi(N_j)}\,\Phi(N_j)\,dx = \sum_{j=1}^{n} \varepsilon_{N_j} < 2\sum_{j=1}^{\infty} \varepsilon_{N_j} < \infty \qquad (n = 1, 2, \ldots),$$

und so ist auf Grund des Satzes von Fatou die Behauptung (11) richtig.

Es sei

$$T = \bigcap_{j=1}^{\infty} \bigcup_{i=j}^{\infty} A_i.$$

Offensichtlich ist $|T|=0$. Wir zeigen, daß (12) für die Punkten von $R=[0,1]-T$, d.h. fast überall in $[0,1]$ besteht.

Es sei $x\in R$. Dann gibt es einen Index $i_0=i_0(x)$ derart, daß $x\notin A_i$ $(i>i_0)$ gilt, und so ist

$$S_{N_i}(t)=S_{N_{i_0}}(t) \qquad (i>i_0).$$

Auf Grund der Eigenschaften (6) *a)* und *d)* kann man eine Indexfolge $\mu_i=\mu_i(x)$ angeben, für welche

$$|S_{\mu_i}(P_{k_i};x)|>\frac{k_i}{3}-1>\frac{1}{12}\log\log N_i$$

gilt. Daraus folgt für genügend große i

$$\frac{|S_{N_i+\mu_i}(x)|}{\lambda_{N_i+\mu_i}}=\frac{\left|S_{N_i}(x)+\frac{\varepsilon_{N_i}}{\Phi(N_i)}\psi_{N_i}(x)S_{\mu_i}(P_{k_i};x)\right|}{\lambda_{N_i+\mu_i}}\geqq$$

$$\geqq\frac{\varepsilon_{N_i}\log\log N_i}{12\Phi(N_i)\lambda_{N_i}}-\frac{S_{N_i}(x)}{\lambda_{N_i+\mu_i}}=\frac{1}{12}+o(1)>\frac{1}{24}.$$

Damit ist Satz 6 bewiesen.

Literaturverzeichnis

[1] N. J. Fine, On the Walsh functions, *Trans. Amer. Math. Soc.*, **65** (1949), 372–414.
[2] F. Schipp, Über die Größenordnung der Partialsummen der Entwicklung integrierbarer Funktionen nach W-Systemen, *Acta Sci. Math.*, **28** (1967), 123–134.
[3] A. Zygmund, *Trigonometric series*, Vol. II. (Cambridge, 1959).
[4] В. Н. Прохоренко, О расходящихся рядах Фурье, *Мат. Сборник*, **75** (1968), 185–196.
[5] J. Marcinkiewicz, Sur les séries de Fourier, *Fundamenta Math.*, **27** (1963), 38–69.
[6] K. Tandori, Ein Divergenzsatz für Fourierreihen, *Acta Sci. Math.*, (Im Druck).
[7] L. G. Pál, On the rule of the structural properties of functions in the theory of their Walsh–Fourier expansions, *Annales Univ. Sci. Budapest*, Sectio Mathematica, **10** (1967), 155–166.

A NOTE ON KUROSH – AMITSUR RADICAL PROPERTIES

By

R. WIEGANDT

Mathematical Institute of the Hungarian Academy of Sciences, Budapest

(Received November 18, 1968)

Some decades ago in the theory of associative rings there were introduced many types of concrete radical properties (e.g. BROWN – MCCOY, JACOBSON, LEVITZKI, BAER and other radicals, see [1]). The aim was to get a good survey about rings having zero radical (such rings are called usually semi-simple rings). A good description of semi-simple rings would be a decomposition in a (discrete or complete) direct sum of simple rings. But generally, a semi-simple ring with respect to a concrete radical property, has not such a decomposition.

A general theory of radicals were developed by KUROSH and AMITSUR. We recite the definition of a KUROSH – AMITSUR radical property (cf. DIVINSKY [1]). Let $\mathcal{R}$ be an abstract property of rings. A ring A (an ideal I of A) possessing property $\mathcal{R}$ will be called an $\mathcal{R}$-ring (an $\mathcal{R}$-ideal). $\mathcal{R}$ is a *radical property* (in the sense of KUROSH and AMITSUR), if the following three conditions hold:

(A) *A homomorphic image of an $\mathcal{R}$-ring is an $\mathcal{R}$-ring.*

(B) *Every ring A contains an $\mathcal{R}$-ideal R which contains every other $\mathcal{R}$-ideal of the ring. R is called the $\mathcal{R}$-radical of A.*

(C) *The factor ring A/R is $\mathcal{R}$-semi-simple (i.e. its only $\mathcal{R}$-ideal is the ideal* 0).

In a personal discussion DR. F. SZÁSZ asked: does there exist a (non trivial) radical property satisfying the additional condition:

(X) *Every $\mathcal{R}$-semi-simple ring is a discrete direct sum of simple rings.*

It is the purpose of this note to prove the following

THEOREM. *A radical property $\mathcal{R}$ satisfies condition* (X) *if and only if every ring is an $\mathcal{R}$-ring.*

PROOF. If every ring has property $\mathcal{R}$, then the $\mathcal{R}$-semi-simple rings are just the rings of one element, and so (X) is trivially satisfied.

Suppose that the radical property $\mathcal{R}$ satisfies condition (X). $\mathcal{R}$ determines a class $\mathcal{S}$ consisting of all $\mathcal{R}$-semi-simple rings. According to DIVINSKY [1] p. 5. the class $\mathcal{S}$ satisfies condition

(D) If every non-zero ideal of a ring A can be mapped homomorphically onto some non-zero ring of $\mathcal{S}$, then the ring A belongs to $\mathcal{S}$.

By the assumption every $\mathcal{R}$-semi-simple ring A has a decomposition $A = \sum_{i \in I} A_i$, where all the components A_i are simple rings, and in the view of (B) $A_i \in \mathcal{S}$ holds for each $i \in I$. Hence it is sufficient to prove that $\mathcal{S}$ consists of rings having one element.

A simple ring $A \neq 0$ is either a zero ring of prime order, or $A^2 = A$ holds.

1. If $0 \neq A \in \mathcal{S}$ is a zero ring of prime order p, then by condition (D) also the zero ring A_2 over the cyclic group $C(p^2)$ belongs to $\mathcal{S}$, but obviously A_2 is not a direct sum of simple rings. Thus $\mathcal{S}$ does not contain zero rings of prime order.

2. If $A \neq 0$ is an idempotent simple ring of $\mathcal{S}$, then consider the complete direct sum

$$(*) \qquad B = \sum_{\alpha \in J}^{*} A_\alpha \qquad (A_\alpha \cong A,\ \alpha \in J).$$

Clearly, $M_\alpha = \sum_{\alpha \neq i \in J}^{*} A_i$ is a maximal ideal of B for each $\alpha \in I$. Denote the $\mathcal{R}$-radical of B by R, now $R \subseteq M_\alpha$ holds, otherwise, namely, the Second Isomorphism Theorem would imply

$$0 \neq R/R \cap M_\alpha \cong (R, M_\alpha)/M_\alpha = B/M_\alpha \cong A_\alpha \in \mathcal{S}$$

which is impossible, for an $\mathcal{R}$-radical ring cannot be mapped homomorphically on a non-zero ring of $\mathcal{S}$. Hence we obtain $R \subseteq \bigcap_{\alpha \in J} M_\alpha = 0$, and so B is $\mathcal{R}$-semi simple. By the assumption B can be decomposed in a discrete direct sum $\sum_{\gamma \in K} B_\gamma$, where every $B_\gamma \in \mathcal{S}$ is a simple ring. Consider an element $b \neq 0$ of B. According to (*) b has the form $(\ldots, a_\gamma, \ldots)$ $(\alpha_\gamma \in A_\gamma)$ where at least one component a_{γ_0} differs from 0. Thus $A_{\gamma_0} = A_{\gamma_0} b A_{\gamma_0} \subseteq B_{\gamma_0}$ is valid which implies $A_{\gamma_0} = B_{\gamma_0}$, and so the cardinal numbers of J and K are the same. If the cardinal number of J is infinite and graeter than that of A, then $\sum_{\alpha \in J} A_\alpha = \sum_{\gamma \in J}^{*} A_\alpha$ is obviously a contradiction. Hence $\mathcal{S}$ does not contain simple rings differing from 0, and to the theorem is proved.

REMARK. Observe that this theorem is valid not only for the class of all rings, but *for any primitive class* (i.e. variety) *of rings* (assuming that in this class there is at least one semi-simple idempotent[1] simple ring with respect to the radical property $\mathcal{R}$).

Instead of condition (X) one can consider condition

(Y) *Every $\mathcal{R}$-semi-simple ring is a complete direct sum of simple rings.*

Similarly (but somewhat easier) one can prove the following statement

A radical property $\mathcal{R}$ satisfies condition (Y) *if and only if every ring is an $\mathcal{R}$-ring.*

[1] The class of zero rings over elementary p-groups is a primitive class and every ring of this class is a direct sum of simple rings.

A corresponding theorem for generalized BROWN–McCOY radical properties was obtained in [2]. (Let us remark that the generalized BROWN–McCOY radicals, the so called $\mathcal{M}$-radicals in [2], need not be radicals in the sense of KUROSH and AMITSUR.)

References

[1] N. J. DIVINSKY, *Rings and radicals*, London, 1965.

[2] R. WIEGANDT, Radical and semi-simplicity in categories, *Acta Math. Acad. Sci. Hung.*, **19** (1968), 345–364.

NOTE ON THE PAPER OF W. M. SCHMIDT "SOME DIOPHANTINE EQUATIONS IN THREE VARIABLES WITH ONLY FINITELY MANY SOLUTIONS"

By

K. GYŐRY

(Debrecen)

(Received December 8, 1968)

W. M. SCHMIDT [3] obtained some results concerning diophantine equations and inequalities in three variables x, y, z. In this paper we prove a slightly improved form of Schmidt's Theorem 1, and we show that this is already best possible.

We shall apply Schmidt's notations throughout this paper. Write

$$\mathbf{x} = (x, y, z) \text{ and } |\mathbf{x}| = \max(|x|, |y|, |z|).$$

Given an algebraic number field K of degree n and $\xi \in K$, denote the conjugates of ξ by $\xi^{(1)} = \xi, \xi^{(2)}, \ldots, \xi^{(n)}$, its norm $\xi^{(1)} \ldots \xi^{(n)}$ by $N(\xi)$ and the real euclidean 3-space by E_3. Then the following proposition is true.

THEOREM. *Let K be an algebraic number field of degree $n \geq 4$ over the rationals Q. Let α, β, γ be three elements of K, linearly independent over Q and with the property that $K = Q(\alpha/\gamma, \beta/\gamma)$. Let*

$$L(\mathbf{x}) = \alpha x + \beta y + \gamma z$$

and

$$L^{(i)}(\mathbf{x}) = \alpha^{(i)} x + \beta^{(i)} y + \gamma^{(i)} z \qquad (i = 1, \ldots, n).$$

Suppose r is the maximal number of forms $L^{(i_1)}, \ldots, L^{(i_r)}$ for which there exist an $0 \neq \mathbf{a} \in E_3$ satisfying

$$L^{(i_1)}(\mathbf{a}) = 0, \ldots, L^{(i_r)}(\mathbf{a}) = 0,$$

and m is the maximal number of those forms $L^{(i)}$, which can be written simultaneously as linear combinations with complex coefficients of a rational linear form R and a real linear form S.

Then there are infinitely many triples of rational integers x, y, z having the property

$$|N(L(\mathbf{x}))| \leq c|\mathbf{x}|^{\min(n-(3/2)r,\, n-2m)} \tag{1}$$

with a suitable constant $c>0$, but for every $\varepsilon>0$ there are only finitely many triples of rational integers x, y, z satisfying[1]

$$|N(L(\mathbf{x}))| \leq |\mathbf{x}|^{\min(n-(3/2)r,\, n-2m)-\varepsilon} \tag{2}$$

If l is the maximal number of the forms $L^{(i)}$, which are linear combinations of two given linear forms (see [3]), then obviously $2 \leq r \leq l \leq n$. Moreover it is easy to prove, that $m \leq r$. Inded, if we set $L^{(i_1)}, \ldots, L^{(i_m)}$ as a maximal system of the forms $L^{(i)}$, which are linear combinations of a rational linear form R and a real linear form S, then $R(\mathbf{a}) = S(\mathbf{a}) = 0$ and consequently $L^{(i_s)}(\mathbf{a}) = 0$ $(s = 1, \ldots, m)$ at a suitable point $0 \neq \mathbf{a} \in E_3$. Then, according to Schmidt's lemmas 4 and 5

$$r \leq n/2 \text{ and } m \mid n. \tag{3}$$

Moreover the module $\{\alpha, \beta, \gamma\}$ is degenerated (see [1], p. 322.) for $n = 2m$, as it was shown by Schmidt. Otherwise one always has

$$n/4 \leq \min(n-(3/2)r,\, n-2m) \leq n-3.$$

Finally we note, that r is not necessarily equal to l, only $r \leq l$ holds. For showing this let α be a complex algebraic number of degree 2 and K an algebraic number field of degree $n>4$ containing α. Let β be a primitive element of K, and let

$$L(\mathbf{x}) = \alpha x + \beta y + z$$

be a form satisfying the conditions of the theorem. It is easy to see, that for $N(L(\mathbf{x}))$ we get $l = n/2$, but $r = 2$. So in this case we have $r < l$ and

$$\min(n-(3/2)l,\, n-2m) < \min(n-(3/2)r,\, n-2m).$$

Proof of (1). We suppose, that $L^{(i_1)}, \ldots, L^{(i_r)}$ form a maximal system, for which

$$L^{(i_1)}(\mathbf{a}) = 0, \ldots, L^{(i_r)}(\mathbf{a}) = 0 \tag{4}$$

at a certain point $0 \neq \mathbf{a} \in E_3$. It is obvious, that this system does not contain three linearly independent forms, but each of these forms can be expressed as a linear combination of two forms of the system.

If this system contains two real forms $L^{(i)}, L^{(j)}$, then

$$|L^{(i)}(\mathbf{x})| < c_1 |\mathbf{x}|^{-\frac{1}{2}}, \qquad |L^{(j)}(\mathbf{x})| < c_1 |\mathbf{x}|^{-\frac{1}{2}}$$

simultaneously, for infinitely many triples of integers $\mathbf{x} = (x, y, z)$ ($c_1>0$ is an appropriate constant). Then

$$|L^{(i_s)}(\mathbf{x})| < c_2 |\mathbf{x}|^{-\frac{1}{2}} \qquad (s = 1, \ldots, r) \tag{5}$$

for each of these $\mathbf{x}$, and for all other forms, since these forms are linear combinations of $L^{(i)}$ and $L^{(j)}$. From this we obtain

$$|N(L(\mathbf{x}))| < c_3 |\mathbf{x}|^{-\frac{1}{2}r+n-r} = c_3 |\mathbf{x}|^{n-\frac{3}{2}r} \tag{6}$$

for infinitely many triples of integers, with an appropriate constant $c_3>0$.

[1] In (1) of [3], corresponding to our (2), there is a misprint, namely "max" instead of "min".

If we do not have two real forms in system (4), and if $L^{(i)}$ is a complex form in (4), then also the complex conjugate form $\bar{L}^{(i)}$ belongs to (4), since $L^{(i)}(\mathbf{a}) = \bar{L}^{(i)}(\mathbf{a}) = 0$. For an appropriate constant $c_1 > 0$

$$|L^{(i)}(\mathbf{x})| < c_1 |\mathbf{x}|^{-\frac{1}{2}}$$

has infinitely many integral solutions $\mathbf{x}$, each of them satisfying also the inequality

$$|\bar{L}^{(i)}(\mathbf{x})| < c_1 |\mathbf{x}|^{-\frac{1}{2}}.$$

Since the other forms are linear combinations of $L^{(i)}$ and $\bar{L}^{(i)}$, we get (5) and (6) in a similar way for all of these $\mathbf{x}$.

Now let $m \geq 2$, and suppose that $L^{(i_1)}, \ldots, L^{(i_m)}$ is a maximal system such that each of these forms is a linear combination of a rational linear form R and a real linear form S. Therefore

$$L^{i_s}(\mathbf{x}) = \sigma_{1,i_s} R(\mathbf{x}) + \sigma_{2,i_s} S(\mathbf{x}) \qquad (s = 1, \ldots, m) \tag{7}$$

where

$$R(\mathbf{x}) = ax + by + cz$$

and a, b, c may be choosen so that a, b, c are integers with $(a, b, c) = 1$ ($a = b = c = 0$ is impossible, since then $L^{(i_1)}, \ldots, L^{(i_m)}$ would be proportional). Then there exist integers a', b', c' and a'', b'', c'' (see for example [2]), such that

$$\begin{vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{vmatrix} = 1.$$

Now if we apply the transformation

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{8}$$

on the forms (7), then evidently $R(\mathbf{x}) = x'$ and

$$L^{(i_s)}(\mathbf{x}) = L'^{(i_s)}(\mathbf{x}') = \sigma_{1,i_s} x' + \sigma_{2,i_s} S'(\mathbf{x}') = \sigma^*_{1,i_s} x' + \sigma_{2,i_s}(\mu y' + \nu z')$$
$$(s = 1, \ldots, m).$$

Here the real numbers μ, ν are linearly independent over Q, for the unimodular transformation (8) preserves this property of the coefficients of the forms $L^{(i)}$. Now

$$|\mu y' + \nu z'| < c_5 |\mathbf{x}'|^{-1} \qquad |\mathbf{x}'| = \max(|x'|, |y'|, |z'|)$$

has infinitely many integral solutions $\mathbf{x}' = (0, y', z')$, and consequently

$$|L'^{(i_s)}(\mathbf{x}')| < c_6 |\mathbf{x}'|^{-1} \qquad (s = 1, \ldots, m)$$

has infinitely many common integral solutions too. Finally applying the inverse of (8) and using $|\mathbf{x}'| \geq c_7|\mathbf{x}|$, we have

$$|L^{(i_s)}(\mathbf{x})| < c_8|\mathbf{x}|^{-1} \qquad (s = 1, \ldots, m)$$

also with infinitely many common integral solutions $\mathbf{x}$. Thus we have

$$|N(L(\mathbf{x}))| < c_9|\mathbf{x}|^{m+n-m} = c_9|\mathbf{x}|^{n+2m}$$

for all of these $\mathbf{x}$.

Proof of (2). Let us suppose, on the contrary, that for a certain $\varepsilon > 0$ the inequality (2) has infinitely many integral solutions $\mathbf{x}$. Then there exist also infinitely many solutions $\mathbf{x} = (x, y, z)$ such that e.g. $|\mathbf{x}| = \max(|x|, |y|, |z|) = |x|$. The points $(1, y/x, z/x)$ of E_3, obtained from these solutions, form an infinit bounded set, having an accumulation point $0 \neq \mathbf{a} \in E_3$. Let us consider only those solutions, whose corresponding points tend to $\mathbf{a}$. Since

$$|N(\alpha + \beta y/x + \gamma z/x)| \leq |\mathbf{x}|^{\min(n-(3/2)r,\, n-2m)-n-\varepsilon} \to 0$$

for all of these solutions, we have

$$N(L(\mathbf{a})) = L^{(1)}(\mathbf{a}) \ldots L^{(n)}(\mathbf{a}) = 0$$

by the continuity of the form $N(L(\mathbf{x}))$. If

$$L^{(i_1)}(\mathbf{a}) = 0, \ldots, L^{(i_s)}(\mathbf{a}) = 0, \tag{9}$$

then

$$|L^{(i)}(\mathbf{x})| \geq c_{10}|\mathbf{x}|$$

for all other forms and for each $\mathbf{x}$ above, with an appropriate $c_{10} > 0$.

If $s = 1$, then one has by Schmidt $|L^{(i_1)}(\mathbf{x})| \gg |\mathbf{x}|^{-2-\varepsilon'}$ for every $\varepsilon' > 0$, and so

$$|N(L(\mathbf{x}))| \geq c_{11}|\mathbf{x}|^{-2-\varepsilon'+n-1} \geq c_{11}|\mathbf{x}|^{n-(3/2)r-\varepsilon'}$$

for each $\mathbf{x}$ above, in contrary of our hypothesis.

Suppose now, that $2 \leq s \leq r$ and that the forms (9) can not be written simultaneously as linear combinations of a rational linear form and a real linear form. In this case

$$|L^{(i_1)}(\mathbf{x}) \ldots L^{(i_s)}(\mathbf{x})| \leq |\mathbf{x}|^{-\frac{1}{2}s-\varepsilon'}$$

has only finitely many integral solutions for every $\varepsilon' > 0$, as it is shown in Schmidt's paper. Thus, for each $\mathbf{x}$ above

$$|N(L(\mathbf{x}))| \geq c_{12}|\mathbf{x}|^{-\frac{1}{2}s-\varepsilon'+n-s} \geq c_{12}|\mathbf{x}|^{n-(3/2)r-\varepsilon'}$$

with an appropriate $c_{12} > 0$, and this is a contradiction again.

Suppose finally, that $s \geq 2$ and that the forms (9) are linear combinations of a given rational linear form and a given real linear form. Then, for these forms, the inequality

$$|L^{(i_1)}(\mathbf{x}) \ldots L^{(i_s)}(\mathbf{x})| < |\mathbf{x}|^{-s-\varepsilon'}$$

has only finitely many integral solutions for every $\varepsilon' > 0$, as this was shown by Schmidt. Thus we have

$$N(L(\mathbf{x})) \geq c_{13} |\mathbf{x}|^{-s-\varepsilon'+n-s} \geq c_{13} |\mathbf{x}|^{n-2m-\varepsilon'}$$

for all of the above $\mathbf{x}$, yielding a contradiction again.

References

[1] S. I. Borewicz – I. R. Šafarević, *Zahlentheorie*, Birkhäuser Verlag, 1966.
[2] T. Nagell, Contributions à la théorie des modules et des anneaux algébriques, *Arkiv för Mat.*, 6 (1965), 161 – 173.
[3] W. M. Schmidt, Some diophantine equations in three variables with only finitely many solutions, *Mathematika*, 14 (1967), 113 – 120.

EIN RADIKALTHEORETISCHER VEREINIGUNGSENDOMORPHISMUS DES IDEALVERBANDES DER RINGE

Von

F. SZÁSZ

Mathematisches Forschungsinstitut der Ungarischen Akademie der Wissenschaften

(Eingegangen am 20. Dezember 1968)

Unter einem Ring wird in dieser Note ein assoziativer Ring bzw. ein alternativer Ring, unter einem Radikal stets ein Amitsur—Kurosches Radikal verstanden [1], [6]. Bezüglich der nötigen Grundbegriffe verweisen wir noch auf ANDRUNAKIEWITSCH [3], BIRKHOFF [4], DIVINSKY [5] und RÉDEI [7].

Für die Abfassung des Resultates dieser Note machen wir eine Vorbereitung. Ist R ein Radikal, so wird ein R-halbeinfacher Ring A streng R-halbeinfach genannt [3], wenn jedes homomorphe Bild von A ebenfalls R-halbeinfach ist. Offenbar ist nicht jeder R-halbeinfache Ring streng R-halbeinfach. Weiterhin gibt es Radikale R, für die jeder R-halbeinfache Ring auch streng R-halbeinfach ist. Sind nun I ein Ideal eines Ringes A, und R ein beliebiges Radikal, so ist

$$\varphi : I \to R(I)$$

eine Abbildung des Idealverbandes des Ringes A in sich, denn das Radikal $R(I)$ des Ideals I ist nach Theorem 47 von DIVINSKY [5] ebenfalls ein Ideal des Ringes A. In dieser Note wird auch die Modularität des Idealverbandes eines Ringes benützt, die folgendes bedeutet:

Sind I_1 und I_2 Ideale von A mit der Bedingung $I_1 \supseteq I_2$, so gilt $I_1 \cap (I_2 + I_3) = I_2 + (I_1 \cap I_3)$ für jedes Ideal I_3 des Ringes A.

Als gewisse Dualisierung eines Satzes von AMITSUR [1] (Theorem 4.1, S. 783) kann folgendes Resultat bestätigt werden:

SATZ. *Sind A ein (assoziativer bzw. alternativer) Ring, I ein Ideal von A und R ein solches Radikal, für das jeder R-halbeinfache Ring auch streng R-halbeinfach ist, so ist die Abbildung*

$$\varphi : I \to \bar{I} = R(I)$$

ein Vereinigungsendomorphismus des Idealverbandes V von A; es gilt also $\overline{I_1 + I_2} = \bar{I}_1 + \bar{I}_2$ für beliebige Ideale I_1 und I_2 von A.

BEMERKUNG 1. In der Arbeit von AMITSUR [1] wurde ein Durchschnitthomomorphismus für den Idealverband V des Ringes A mit der Hilfe sogenannter erblicher Radikale [1], [3] und einer wesentlich anderen, wohlbestimmten Abbildung φ angegeben.

BEWEIS. Es seien I_1 und I_2 Ideale des Ringes A mit $I_1 \subseteq I_2$. Dann erhält man $\bar{I}_1 \subseteq \bar{I}_2$, und somit steht an der linken Seite der Isomorphie

$$(\bar{I}_1 + \bar{I}_2)/\bar{I}_2 \cong \bar{I}_1/\bar{I}_1 \cap \bar{I}_2$$

ein Ideal des R-halbeinfachen Ringes $I_2/\bar{I}_2$, und daher ist $(\bar{I}_1 + \bar{I}_2)/\bar{I}_2$ R-halbeinfach nach dem Theorem 47 von bzw. nach Theorem 2 von [2]. An der rechten Seite der Isomorphie kommt aber ein R-Radikalring, als ein homomorphes Bild eines R-Radikalringes, hervor. Hiernach ergibt sich $\bar{I}_1/\bar{I}_1 \cap \bar{I}_2 = 0$, folglich $I_1 = \bar{I}_1 \cap \bar{I}_2 \subseteq \bar{I}_2$.

Die Abbildung $\varphi : I \to \bar{I}$ ist also monoton.

Sind nun die Ringe B/C und C beide R-halbeinfach für ein Ideal C von B und für ein Radikal R, so ist B selbst R-halbeinfach. Es sei nämlich $R(B)$ das R-Radikal des Ringes B. Da $(R(B) + C)/C$ ein R-Radikalideal und B/C R-halbeinfach sind, ergibt sich $R(B) \subseteq C$, woraus man wegen der R-Halbeinfachheit von C wirklich $R(B) = 0$, also die R-Halbeinfachheit von B erhält.

Hiernach ist jede Everettsche Erweiterung eines R-halbeinfachen Ringes mit der Hilfe eines R-halbeinfachen Ringes ebenfalls R-halbeinfach.

Bisher haben wir die strenge R-Halbeinfachheit der R-halbeinfachen Ringe noch nicht benützt. Diese letztere Voraussetzung wird nur jetzt benötigt.

Wegen der Modularität des Idealverbandes V des Ringes A und wegen $I_2 \supseteq \bar{I}_2$ ergibt sich $I_2 \cap (\bar{I}_1 + \bar{I}_2) = \bar{I}_2 + (\bar{I}_1 \cap I_2)$ für beliebige Ideale I_1 und I_2, und somit ist der Faktorring $I_2/\bar{I}_2 \cap (\bar{I}_1 + \bar{I}_2)$ ein homomorphes Bild des R-halbeinfachen Ringes $I_2/\bar{I}_2$. Also ist auch $I_2/\bar{I}_2 \cap (\bar{I}_1 + \bar{I}_2)$ R-halbeinfach nach der vorausgesetzten strengen R-Halbeinfachkeit von $I_2/\bar{I}_2$. Nach dem Isomorphiesatz erhält man aber

$$\bar{I}_1 + I_2/\bar{I}_1 + \bar{I}_2 = (\bar{I}_1 + \bar{I}_2) + I_2/\bar{I}_1 + \bar{I}_2 \cong I_2/\bar{I}_2 \cap (\bar{I}_1 + \bar{I}_2)$$

und daher ist der Faktorring $\bar{I}_1 + I_2/\bar{I}_1 + \bar{I}_2$ R-halbeinfach.

Wegen der Modularität des Idealverbandes V von A und wegen $I_1 \supseteq \bar{I}_1$ erhält man andererseits $I_1 \cap (\bar{I}_1 + \bar{I}_2) = \bar{I}_1 + (I_1 \cap \bar{I}_2)$ und somit ist der Faktorring $I_1/\bar{I}_1 \cap (\bar{I}_1 + \bar{I}_2)$ ein homomorphes Bild des strengen R-halbeinfachen Ringes $I_1/\bar{I}_1$. Also ist auch $I_1/\bar{I}_1 \cap (\bar{I}_1 + \bar{I}_2)$ ein R-halbeinfacher Ring. Nach der Isomorphie

$$(\bar{I}_1 + \bar{I}_2)/\bar{I}_1 + \bar{I}_2 = (\bar{I}_1 + \bar{I}_2) + \bar{I}_1/\bar{I}_1 + \bar{I}_2 \cong \bar{I}_1/\bar{I}_1 \cap (\bar{I}_1 + \bar{I}_2)$$

ergibt sich die R-Halbeinfachheit von $\bar{I}_1 + \bar{I}_2/\bar{I}_1 + \bar{I}_2$.

Da jetzt der Faktorring $B/C = (\bar{I}_1 + \bar{I}_2)/\bar{I}_1 + \bar{I}_2$ und das Ideal $C = (\bar{I}_1 + \bar{I}_2)/(\bar{I}_1 + \bar{I}_2)$ nach dem vorigen beide R-halbeinfache Ringe sind, ist auch der Faktorring $B = (\bar{I}_1 + \bar{I}_2)/(\bar{I}_1 + \bar{I}_2)$ nach dem vorigen R-halbeinfach, denn $B = (\bar{I}_1 + \bar{I}_2)/\bar{I}_1 + \bar{I}_2)$ ist eine Everettsche Ringerweiterung von $C = (\bar{I}_1 + \bar{I}_2)/(\bar{I}_1 + \bar{I}_2)$

mit der Hilfe von $B/C \cong (I_1+I_2)/(I_1+I_2)$. Wegen $R(I_1+I_2) = I_1+I_2$ erhält man also $I_1+I_2 \subseteq \overline{I_1+I_2}$ denn I_1+I_2 ist ein R-Radikalring, und $I_1+I_2/\overline{I_1+I_2}$ ist R-halbeinfach.

Nach der bewiesenen Monotonität von $I \to \overline{I}$ ergibt sich aus $I_j \subseteq I_1+I_2$ $(j = 1, 2)$ offenbar $\overline{I_j} \subseteq \overline{I_1+I_2}$, folglich auch $\overline{I_1}+\overline{I_2} \subseteq \overline{I_1+I_2}$. Wegen der bewiesenen Relation $I_1+I_2 \subseteq \overline{I_1}+\overline{I_2}$ folgt $\overline{I_1+I_2} = \overline{I_1}+\overline{I_2}$ Daher ist $I \to \overline{I}$ wirklich ein Vereinigungsendomorphismus, w.z.b.w.

Bemerkung 2. Auch eine kategorientheoretische Verallgemeinerung des Satzes und seines dualen Satzes kann in gewissen Kategorien abgefaßt und bewiesen werden. Für solche Kategorien siehe z. B. [8] und [9].

Bemerkung 3. Folgendes Beispiel zeigt, daß der obige Satz nicht für jedes Radikal R gilt. Bestehe nämlich die Klasse aller R-Radikalringe aus sämtlichen idempotenten Ringen, und seien weiterhin I der Ring der ganzen rationalen Zahlen, p und q Primzahlen mit der Bedingung $(p, q) = 1$. Für die Ideale (p) und (q) von I ergibt sich dann $R((p)) = R((q)) = 0$ und $R((p)+(q)) = R(I) = I$, und somit $\overline{(p)}+\overline{(q)} \neq \overline{(p)+(q)}$.

Literaturverzeichnis

[1] S. A. Amitsur, A general theory of radicals, I., *Amer. J. Math*, **74** (1952), 774–786; II., *Amer. J. Math.*, **76** (1954), 100–125; III., *Amer. J. Math.*, **76** (1954), 126–136.

[2] T. Anderson – N. Divinsky – A. Sulinski, Hereditary radicals in associative and alternative rings, *Canadian J. Math.*, **17** (1965), 594–603.

[3] W. A. Andrunakiewitsch, Radikale assoziativer Ringe, I, *Mat. Sbor.* **44** (1958), 179–212; II, *Mat. Sbor.* **55** (1961), 329–346 (Russisch).

[4] G. Birkhoff, *Lattice Theory*, New-York (1948).

[5] N. Divinsky, *Rings and Radicals*, London (1965).

[6] A. G. Kurosch, Radikale der Ringe und Algebren, Mat. Sbor., **33** (1953), 13–26 (Russisch)

[7] L. Rédei, *Algebra*, I. Leipzig (1959).

[8] F. Szász – R. Wiegandt, On the dualization of subdirect embeddings, *Acta Math. Acad. Sci. Hung.* (im Erscheinen).

[9] F. Szász – R. Wiegandt, On radicals and semi-simplicities in categories, *Acta Math. Acad. Sci Hung.* (im Erscheinen).

RANDOM MODELS OF SOME QUASI-INTUITIONISTIC LOGICS

By

I. RUZSA

I. Department for Analysis of the Eötvös Loránd University, Budapest

(Received January 4, 1969)

In my earlier paper [3] I have presented a method to construct certain models for some logical systems in the probability calculus. In the present paper I shall give a report about my attempts to extend the indicated modelizing method to the intuitionistic logic.

The basic idea of the mentioned method is as follows: The logical variables are represented by random variables, and the logical operators by function operators ranging over random variables (viz. over n-tuples of random variables) and having random variables as their values. Hencefort the models thus generated will be called *random models*.

In the present paper I am going to use the notions and notation introduced in [3], and, sometimes, I shall also refer to the results of [3]. However, the greater part of the present article is self-contained.

As far as my results are concerned, I failed to find a random model structure being adequate representation of the intuitionistic logic (in the sense of *Definitions 3, 4, 6, 7* in [3], see Part I, **§.1** and **§.2**). I succeeded only in finding a random model structure which represents a system lying between intuitionistic and classical logic, and another one which represents a logical system having some features characteristic of the intuitionistic logic.

§.1. Preliminaries. Notation and basic notions

We shall denote the empty set by $\emptyset$, the union, the intersection and the difference of the sets A, B by $A \cup B$, $A \cap B$, and $A \setminus B$, respectively. $A \subseteq B$ denotes that the set B includes the set A. If A is a set then A^k denotes the set of the ordered k-tuples of the form $(a_1, \ldots, a_k)$, where $a_1 \in A, \ldots, a_k \in A$ $(k = 1, 2, \ldots)$. The symbol $\langle a_1, \ldots, a_k \rangle$ denotes an ordered k-tuple of the elements $a_1, \ldots, a_k$ provided it holds that for $i \neq j$, $a_i \neq a_j$.

DEFINITION 1. The formal system of the (quantified) intuitionistic logic (briefly: *System H)* is a quintuple

$$H = (J, V, O, F, T)$$

where the meaning of J, V, O, F and T is the following.[1]

J is a denumerably infinite set called *the set of individual variables*.

V is a denumerably infinite union of pairwise disjoint denumerable sets $V_0, V_1, \ldots, V_n, \ldots$ (i.e. $V = \bigcup_{n=0}^{\infty} V_n$), where V_0 is *the set of sentence variables*, and for $n \geqq 1$, V_n is *the set of the n-placed predicate variables*; V is called *the set of predicate variables*.

$O = \{\forall, \exists, \neg, \wedge, \vee, \rightarrow\}$, where $\forall$ and $\exists$ is the universal and the existential quantifier, respectively, $\neg$, $\wedge$, $\vee$, and $\rightarrow$ is the negation, conjunction, disjunction and implication operator, respectively.

J, V and O are pairwise disjoint.

F is the smallest set satisfying the following conditions: (a) $V_0 \subseteq F$; (b) if $q \in V_n$ $(n \geqq 1)$, $x_1 \in J, \ldots, x_n \in J$, then $qx_1 \ldots x_n \in F$; (c) if $x \in J$, and $\alpha \in F$ then $\forall x\alpha \in F$, and $\exists x\alpha \in F$; (d) if $\alpha \in F$ then $\neg\alpha \in F$; (e) if $\alpha \in F$, and $\beta \in F$ then $\wedge\alpha\beta \in F$, $\vee\alpha\beta \in F$, $\rightarrow\alpha\beta \in F$. — F is called *the set of the formulas of H*.

T is a subset of F called the *set of the theorems of H* and defined below.

To have a transparent notation we shall write "$\alpha \wedge \beta$", "$\alpha \vee \beta$" and "$\alpha \rightarrow \beta$" instead of "$\wedge\alpha\beta$", "$\vee\alpha\beta$" and "$\rightarrow\alpha\beta$", respectively, and so we shall also use brackets, in the usual way.

We shall use the notions of *free and bound occurrences of individual variables, closed and open formulas* in the usual sense.

We say that the individual variable y is *free from* the individual variable x in a formula α if no free occurrence of x in α is in a subformula of α of the form $\forall y\beta$ or $\exists y\beta$ $(\beta \in F)$.

The definition of the set T. T is the smallest subset of F satisfying the following conditions: (a) If $\alpha \in F$, $\beta \in F$, $\gamma \in F$ then the formulas (h1) to (h11) below are elements of T.[2]

(h1) $\alpha \rightarrow (\alpha \wedge \alpha)$
(h2) $(\alpha \wedge \beta) \rightarrow (\beta \wedge \alpha)$
(h3) $(\alpha \rightarrow \beta) \rightarrow ((\alpha \wedge \gamma) \rightarrow (\beta \wedge \gamma))$
(h4) $((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma)$
(h5) $\beta \rightarrow (\alpha \rightarrow \beta)$
(h6) $(\alpha \wedge (\alpha \rightarrow \beta)) \rightarrow \beta$
(h7) $\alpha \rightarrow (\alpha \vee \beta)$
(h8) $(\alpha \vee \beta) \rightarrow (\beta \vee \alpha)$
(h9) $((\alpha \rightarrow \gamma) \wedge (\beta \rightarrow \gamma)) \rightarrow ((\alpha \vee \beta) \rightarrow \gamma)$
(h10) $\neg\alpha \rightarrow (\alpha \rightarrow \beta)$
(h11) $((\alpha \rightarrow \beta) \wedge (\alpha \rightarrow \neg\beta)) \rightarrow \neg\alpha$

(b) If $\alpha \in F$, $x \in J$, $y \in J$ and y is *free from* x in α then the formulas (h12) and (h13) below are elements of T.[3]

[1] This definition is a special case of the more general *Definition* 16 given in [3], Part III, §. 8.

[2] These are the axiom-schemata of the intuitionistic propositional calculus. See HEYTING [1].

[3] These are the additional axiom-schemata for the quantified intuitionistic logic. See e.g. KLEENE [2], Ch. IV., §. 19.

(h12) $\forall x\alpha \to \alpha(x/y)$
(h13) $\alpha(x/y) \to \exists x\alpha$

(Here "$\alpha(x/y)$" denotes the formula arising from α by substituting y for all free occurrences of x.) (c) If $\alpha \in T$, $\beta \in F$, and $\alpha \to \beta \in T$ then $\beta \in T$. *(Detachment.)* (d) If $\alpha \in T$, and $\beta \in T$ then $\alpha \wedge \beta \in T$. (e) If $\alpha \in F$, $\beta \in F$, $x \in J$, and x has no free occurrence in α, then

(e1) if $\alpha \to \beta \in T$ then $\alpha \to \forall x\beta \in T$, and
(e2) if $\beta \to \alpha \in T$ then $\exists x\beta \to \alpha \in T$.

The quadruple

$$H' = (J, V, O, F)$$

will be called *the language* of the system H.

We shall use the symbol $J(\alpha)$ for denoting the sequence $\langle x_1, \ldots, x_k \rangle$ of the distinct individual variables having free occurrences in the formula α, arranged according to the order of their first occurrences in α.

We say that α is *a prime formula* if $\alpha \in F$ according to (a) or (b) in the definition of F above.

DEFINITION 2. We shall call a triple $\Sigma = (I, \mathcal{A}, P)$ a *probability space*, if I is a non-empty set, $\mathcal{A}$ is a σ-algebra of certain subsets of I, and P is a probability measure defined on the measurable space $(I, \mathcal{A})$ satisfying the condition $P(I) = 1$. — The elements of $\mathcal{A}$ will be called *events*. The event $I \setminus B$ will be called the complement of B ($B \in \mathcal{A}$) and denoted by $\overline{B}$.

A measurable function w defined on I will be called a *random variable on* Σ. — If w is a random variable on Σ, and z is a real number, then we denote by $[w < z]$ the event which contains an element E of I if and only if $w(E) < z$. Similarly, $[w \leq z]$, $[w = z]$, $[w > z]$, and $[w \geq z]$ have a self-explanatory meaning.

DEFINITION 3. The triple

$$Z = (a, b, \Theta)$$

will be called a *random model structure* (briefly: *rms*) of the language H' if a and b are real numbers such that $a < b$ holds, and Θ is a function defined on O such that the following conditions are fulfilled:[4]

(a) $\Theta(\forall) = \forall^*$ and $\Theta(\exists) = \exists^*$ are generalized function operators such that if B is a non-empty set of random variables defined on a probability space Σ, and the values of the elements of B belong to the real interval $[a, b]$, then $\forall^*(B)$ and $\exists^*(B)$ are random variables on Σ, and $[a, b]$ contains all their values.

(b) $\Theta(\neg) = \neg^*$ is a function operator in one variable such that if w is a random variable on a probability space Σ, and the values of w belong to $[a, b]$, then $\neg^*(w)$ is a random variable on Σ, and its values belong to $[a, b]$.

(c) $\Theta(\wedge) = \wedge^*$, $\Theta(\vee) = \vee^*$ and $\Theta(\to) = \to^*$ are function operators in two variables such that if w_1 and w_2 are random variables on a probability space Σ, and their values belong to $[a, b]$, then $\wedge^*(w_1, w_2)$, $\vee^*(w_1, w_2)$ and $\to^*(w_1, w_2)$ are random variables on Σ, and their values belong to $[a, b]$.

[4] This definition is a special case of the more general DEFINITION 17 given in [3], Part III, §. 8.

DEFINITION 4. The quintuple

$$\Gamma = (U, f, \Sigma, \Omega, W)$$

will be called *a random model* belonging to the *rms* $Z = (a, b, \Theta)$ of the language H', if the following conditions are fulfilled:[5]

U is a non-empty but at most denumerable set called *the universe of* Γ.

f is a function on J, the values of f are elements of U.

Σ is a probability space.

Ω is a function defined on F such that if $\alpha \in F$, and $J(\alpha) = \langle x_1, \ldots, x_k \rangle$ $(k \geqq 0)$, then $\Omega(\alpha) = \alpha^*$ is a function on U^k defined inductively as follows:

(a) If $\alpha \in V_0$ (in which case $k = 0$), then $\Omega(\alpha) = \alpha^*$ is a random variable on Σ, and the values of α^* belong to $[a, b]$.

(b) If $q \in V_k$ $(k \geqq 1)$, and $x_1, \ldots, x_k$ are *distinct* elements of J, then $\Omega(qx_1 \ldots x_k) = q^*$ is a function such that, for any $(u_1, \ldots, u_k) \in U^k$, $q^*(u_1, \ldots, u_k)$ is a random variable on Σ, and the values of this random variable belong to $[a, b]$.

(c) If $\alpha \in F$, $J(\alpha) = \langle x_1, \ldots, x_k \rangle$ $(k \geqq 1)$, $\{y_1, \ldots, y_m\} \subseteq J$, $1 \leqq m \leqq k$, g is a mapping of $\{x_1, \ldots, x_k\}$ onto $\{y_1, \ldots, y_m\}$, $g(x_i)$ is free from x_i in α (for $i = 1, \ldots, k$), $\Omega(\alpha) = \alpha^*$, and β is $\alpha(x_1/g(x_1)) \ldots (x_k/g(x_k))$, then $\Omega(\beta) = \beta^*$ is a function on U^m such that, for any $(v_1, \ldots, v_m) \in U^m$, $\beta^*(v_1, \ldots, v_m) = \alpha^*(u_1, \ldots, u_k)$, where $u_i = v_j$ if and only if $g(x_i) = y_j$ (for $i = 1, \ldots, k$).

(d) If $\alpha \in F$, and $\Omega(\alpha) = \alpha^*$, then $\Omega(\neg \alpha) = \neg^*(\alpha^*)$,

(e) If $\alpha \in F$, $\beta \in F$, $\Omega(\alpha) = \alpha^*$, $\Omega(\beta) = \beta^*$, $J(\alpha) = \langle x_1, \ldots, x_k \rangle$, $J(\beta) = \langle y_1, \ldots, y_m \rangle$, γ is one of $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha \rightarrow \beta$, and $J(\gamma) = \langle t_1, \ldots, t_n \rangle$, then $\Omega(\gamma) = \gamma^*$ is a function on U^n such that, for any $(s_1, \ldots, s_n) \in U^n$, $\gamma^*(s_1, \ldots, s_n) = Q(\alpha^*(u_1, \ldots, u_k), \beta^*(v_1, \ldots, v_m))$, where Q is $\wedge^*$, $\vee^*$ or $\rightarrow^*$ (according as γ is $\alpha \wedge \beta$, $\alpha \vee \beta$ or $\alpha \rightarrow \beta$), $u_i = s_j$ if and only if $x_i = t_j$ (for $i = 1, \ldots, k$), and $v_i = s_j$ if and only if $y_i = t_j$ (for $i = 1, \ldots, m$).

(f) If $\alpha \in F$, $x \subset J$, but $x \not\subset J(\alpha)$, then $\Omega(\forall x \alpha) = \Omega(\exists x \alpha) = \Omega(\alpha)$.

(g) If $\alpha \in F$, $J(\alpha) = \langle x_1, \ldots, x_k \rangle$ $(k \geqq 1)$, $1 \leqq i \leqq k$, and $\Omega(\alpha) = \alpha^*$, then $\Omega(\forall x_i \alpha) = \forall x_i \alpha^*$ and $\Omega(\exists x_i \alpha) = \exists x_i \alpha^*$ is a function on U^{k-1} such that, for any $(u_1, \ldots, u_{k-1}) \in U^{k-1}$,

$$\forall x_i \alpha^*(u_1, \ldots, u_{k-1}) = \forall^*(\{\alpha^*(u_1, \ldots, u_{i-1}, u, u_i, \ldots, u_{k-1}) | u \in U\}),$$

$$\exists x_i \alpha^*(u_1, \ldots, u_{k-1}) = \exists^*(\{\alpha^*(u_1, \ldots, u_{i-1}, u, u_i, \ldots, u_{k-1}) | u \in U\}),$$

where $\{\alpha^*(u_1, \ldots, u_{i-1}, u, u_i, \ldots, u_{k-1}) | u \in U\}$ denotes the set of all values of the function $\alpha^*(u_1, \ldots, u_{i-1}, u, u_i, \ldots, u_{k-1})$ for $u \in U$.

Finally, W is a function on F such that, if $\alpha \in F$, $J(\alpha) = \langle x_1, \ldots, x_k \rangle$, and $\Omega(\alpha) = \alpha^*$, then $W(\alpha) = \alpha^*(f(x_1), \ldots, f(x_k))$.

§. 2. The random model structure Z_{h1}

We define the *rms* $Z_{h1} = (0, 1, \Theta)$ of the language H' by giving the definition of the function operators $\forall^*$, $\exists^*$, $\neg^*$, $\wedge^*$, $\vee^*$, and $\rightarrow^*$ as follows (cf. Def. 3).

[5] Our definition is a special case of the more general DEFINITION 18 given in [3], Part III, §. 8.

If B is a (non-void) set of random variables, then

$$(1) \qquad \forall^{\cdot}(B) = \inf_{\mathfrak{w} \in B} \mathfrak{w}; \quad \exists^{\cdot}(B) = \sup_{\mathfrak{w} \in B} \mathfrak{w}.$$

If $\mathfrak{w}_1$ and $\mathfrak{w}_2$ are random variables, then

$$(2) \qquad \begin{cases} \wedge^{\cdot}(\mathfrak{w}_1, \mathfrak{w}_2) = \min(\mathfrak{w}_1, \mathfrak{w}_2), \\ \vee^{\cdot}(\mathfrak{w}_1, \mathfrak{w}_2) = \max(\mathfrak{w}_1, \mathfrak{w}_2), \end{cases}$$

$$(3) \qquad \rightarrow^{\cdot}(\mathfrak{w}_1, \mathfrak{w}_2)(E) = \begin{cases} 1 \text{ if } \mathfrak{w}_1(E) \leqq \mathfrak{w}_2(E), \\ \mathfrak{w}_2(E) \text{ otherwise} \end{cases}$$

for any $E \in I$, where I is the (common) domain of $\mathfrak{w}_1$ and $\mathfrak{w}_2$. — Finally, if $\mathfrak{w}$ is a random variable, then

$$\neg^{\cdot}(\mathfrak{w}) = \rightarrow^{\cdot}(\mathfrak{w}, 0),$$

where "0" is the "degenerated" random variable having the sole value 0.

We shall write "$\neg^{\cdot}\mathfrak{w}$", "$\mathfrak{w}_1 \wedge^{\cdot} \mathfrak{w}_2$", "$\mathfrak{w}_1 \vee^{\cdot} \mathfrak{w}_2$" and "$\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2$" instead of "$\neg^{\cdot}(\mathfrak{w})$", "$\wedge^{\cdot}(\mathfrak{w}_1, \mathfrak{w}_2)$", "$\vee^{\cdot}(\mathfrak{w}_1, \mathfrak{w}_2)$" and "$\rightarrow^{\cdot}(\mathfrak{w}_1, \mathfrak{w}_2)$" respectively.

One can see easily that $\forall^{\cdot}$, $\exists^{\cdot}$, $\wedge^{\cdot}$ and $\vee^{\cdot}$ defined above fulfil the requirements of Def. 3. As far as $\rightarrow^{\cdot}$ and $\neg^{\cdot}$ are concerned, the problem is somewhat more difficult. The following lemmas will be useful to clear up the question.

LEMMA 1. Let $\mathfrak{w}_1$ and $\mathfrak{w}_2$ be random variables on a probability space $\Sigma = (I, \mathcal{A}, P)$, and let us denote by "$[\mathfrak{w}_2 < \mathfrak{w}_1]$" the subset of I that contains $E (E \in I)$ if and only if $\mathfrak{w}_2(E) < \mathfrak{w}_1(E)$. Then:

$$(4) \qquad [\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2 < z] = [\mathfrak{w}_2 < z] \cap [\mathfrak{w}_2 < \mathfrak{w}_1] \qquad \text{for } z \leqq 1.$$

PROOF. If $E \in [\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2 < z]$, then, according to (3) (taking into account that $z \leqq 1$), $(\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2)(E) = \mathfrak{w}_2(E)$, and $\mathfrak{w}_2(E) < \mathfrak{w}_1(E)$, hence $E \in [\mathfrak{w}_2 < z]$, and $E \in [\mathfrak{w}_2 < \mathfrak{w}_1]$. — Conversely, if $E \in [\mathfrak{w}_2 < z]$, and $E \in [\mathfrak{w}_2 < \mathfrak{w}_1]$, then, according to (3), $(\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2)(E) = \mathfrak{w}_2(E)$, hence $E \in [\mathfrak{w}_1 \rightarrow \mathfrak{w}_2 < z]$.

LEMMA 2. Let $\mathfrak{w}_1$, $\mathfrak{w}_2$ and Σ be as in Lemma 1. (a) For $z \leqq 1$, the set $[\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2 < z]$ is measurable. (b) If $\mathfrak{w}_1 \leqq 1$ and $\mathfrak{w}_2 \leqq 1$ then $\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2$ is a measurable function.

PROOF. (a) Since $\mathfrak{w}_1$ and $\mathfrak{w}_2$ are measurable functions, it follows that $\mathfrak{w}_1 - \mathfrak{w}_2$ is a measurable function. Hence the sets $[\mathfrak{w}_2 < z]$ and $[\mathfrak{w}_2 < \mathfrak{w}_1] = [\mathfrak{w}_1 - \mathfrak{w}_2 > 0]$ are measurable (for *any* z). If $z \leqq 1$, then — according to Lemma 1 — (4) holds; henceforth $[\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2 < z]$ is measurable. — (b) From the assumption and (3) it follows that $\mathfrak{w}_1 \rightarrow \mathfrak{w}_2 \leqq 1$. Having proved (a), what remains to prove is that $[\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2 = 1]$ is measurable. But this follows from the fact that $[\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2 = 1] = \overline{[\mathfrak{w}_1 \rightarrow^{\cdot} \mathfrak{w}_2 < 1]}$.

From these lemmas it follows immediately that also $\rightarrow^{\cdot}$ and $\neg^{\cdot}$ fulfil the requirements of Def. 3.

We list some simple consequences of the definitions of our function operators. (For the proof of the following identities (5) to (10) see [3], Part I, **§. 2.** and Part III, **§. 9.**)

(5) (a) $w \wedge^{\cdot} w \equiv w$, (b) $w \vee^{\cdot} w \equiv w$

(6) (a) $w_1 \wedge^{\cdot} w_2 \equiv w_2 \wedge^{\cdot} w_1$, (b) $w_1 \vee^{\cdot} w_2 \equiv w_2 \vee^{\cdot} w_1$

(7) $$[w_1 \wedge^{\cdot} w_2 < z] = [w_1 < z] \cup [w_2 < z]$$

(8) $$[w_1 \vee^{\cdot} w_2 < z] = [w_1 < z] \cap [w_2 < z]$$

(9) $$[\forall^{\cdot}(B) < z] = \bigcup_{w \in B} [w < z]$$

(10) $$[\exists^{\cdot}(B) < z] \subseteq \bigcap_{w \in B} [w < z], \quad [\exists^{\cdot}(B) \leqq z] = \bigcap_{w \in B} [w \leqq z]$$

(11) $$w \rightarrow^{\cdot} w \equiv 1$$

(12) $$\neg^{\cdot} w = w \rightarrow^{\cdot} 0 = \begin{cases} 1 & \text{if } w \leqq 0, \\ 0 & \text{if } w > 0. \end{cases}$$

(13) $$\neg^{\cdot}\neg^{\cdot} w = \neg^{\cdot} w \rightarrow^{\cdot} 0 = \begin{cases} 1 & \text{if } w > 0, \\ 0 & \text{if } w \leqq 0. \end{cases}$$

If $(w_1 \rightarrow^{\cdot} w_2)(E) = 1$, and $w_1(E) = 1$, then (according to (3)) $w_2(E) \geqq 1$. If we interpret 1 as "true", and assume that $w_2 \leq 1$, then we may give the following logical interpretation of the fact just mentioned: If $w_1 \rightarrow^{\cdot} w_2$ and w_1 are "true" then also w_2 must be "true". This gives a reason for our definition of $\rightarrow^{\cdot}$.

If we interpret 0 as "false" then the definition $\neg^{\cdot} w = w \rightarrow^{\cdot} 0$ will be in accordance with the definition $\neg p = p \rightarrow \downarrow$ (where "$\downarrow$" means "falsehood") used frequently in the intuitionistic logic.

LEMMA 3. If $w_1 \leqq 1$ and $w_2 \leqq 1$, then $w_1 \rightarrow^{\cdot} w_2 \equiv 1$ if and only if for all E $(E \in I)$, $w_1(E) \leqq w_2(E)$. — This statement follows immediately from (3) (and from the assumptions $w_1 \leqq 1$, $w_2 \leqq 1$).

THEOREM 1. *If the structure of a formula ω is one of* (h1) *to* (h13) (listed in the definition of T) *then in any random model Γ belonging to the rms Z_{h1}, $W(\omega) \equiv 1$ holds.*

PROOF. We shall use the abbreviation $\alpha^{\cdot}$ for $W(\alpha)$ (where $\alpha \in F$).

For (h1) and (h2) the statement of the theorem follows from (5a), (6a), and (11).

Ad (h3). (a) If $(\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot})(E) = 1$, then $\alpha^{\cdot}(E) \leqq \beta^{\cdot}(E)$. Consequently $\min(\alpha^{\cdot}(E), \gamma^{\cdot}(E)) \leqq \min(\beta^{\cdot}(E), \gamma^{\cdot}(E))$. Hence $((\alpha^{\cdot} \wedge^{\cdot} \gamma^{\cdot}) \rightarrow (\beta^{\cdot} \wedge^{\cdot} \gamma^{\cdot}))(E) = 1$. — (b) If $(\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot})(E) \neq 1$, then $(\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot})(E) = \beta^{\cdot}(E) < \alpha^{\cdot}(E)$. Consequently $\min(\alpha^{\cdot}(E), \beta^{\cdot}(E)) \geqq \min(\beta^{\cdot}(E), \gamma(E))$. In the case of equality $((\alpha^{\cdot} \wedge^{\cdot} \gamma^{\cdot}) \rightarrow^{\cdot} (\beta^{\cdot} \wedge^{\cdot} \gamma^{\cdot}))(E) = 1 > (\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot})(E)$. — In the case of inequality, $((\alpha^{\cdot} \wedge^{\cdot} \gamma^{\cdot}) \rightarrow^{\cdot} (\beta^{\cdot} \wedge^{\cdot} \gamma^{\cdot}))(E) = \beta^{\cdot}(E) = (\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot})(E)$. — We see that in all possible cases $(\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot})(E) \leqq ((\alpha^{\cdot} \wedge^{\cdot} \gamma^{\cdot}) \rightarrow^{\cdot} (\beta^{\cdot} \wedge^{\cdot} \gamma^{\cdot}))(E)$ holds. Henceforth, according to Lemma 3, $(\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot}) \rightarrow^{\cdot} ((\alpha^{\cdot} \wedge^{\cdot} \gamma^{\cdot}) \rightarrow^{\cdot} (\beta^{\cdot} \wedge^{\cdot} \gamma^{\cdot})) \equiv 1$.

Ad (h4). (a) If $\alpha^{\cdot}(E) \leqq \beta^{\cdot}(E) \leqq \gamma^{\cdot}(E)$ then

$((\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot}) \wedge^{\cdot} (\beta^{\cdot} \rightarrow^{\cdot} \gamma^{\cdot}))(E) = \min(1, 1) = 1$, and $(\alpha^{\cdot} \rightarrow^{\cdot} \gamma^{\cdot})(E) = 1$. — (b) If $(\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot})(E) \neq 1$ or $(\beta^{\cdot} \rightarrow^{\cdot} \gamma^{\cdot})(E) \neq 1$, then $((\alpha^{\cdot} \rightarrow^{\cdot} \beta^{\cdot}) \wedge^{\cdot} (\beta^{\cdot} \rightarrow^{\cdot} \gamma^{\cdot}))(E)$ equals to

$\beta^*(E)$ or to $\gamma^*(E)$. In the first case $\beta^*(E) \leqq \gamma^*(E) \leqq (\alpha^* \to^* \gamma^*)(E)$, in the second case $\gamma^*(E) \leqq (\alpha^* \to^* \gamma^*)(E)$. — Hence, in all cases, the antecedent of (h4) is $\leqq$ as the consequent of (h4), i.e. $((\alpha^* \to^* \beta^*) \wedge^* (\beta^* \to^* \gamma^*)) \to^* (\alpha^* \to^* \gamma^*) \equiv 1$.

Ad (h5). Since $\beta^*(E) \leqq (\alpha^* \to^* \beta^*)(E)$, it follows that $\beta^* \to^* (\alpha^* \to^* \beta^*) \equiv 1$.

Ad (h6). (a) If $\alpha^*(E) \leqq \beta^*(E)$ then $(\alpha^* \wedge^* (\alpha^* \to^* \beta^*))(E) = \min(\alpha^*(E), 1) = \alpha^*(E) \leqq \beta^*(E)$. — (b) If $\alpha^*(E) > \beta^*(E)$ then $(\alpha^* \wedge^* (\alpha^* \to^* \beta^*))(E) = \min(\alpha^*(E), \beta^*(E)) = \beta^*(E)$. — This means that in all cases $\alpha^* \wedge^* (\alpha^* \to^* \beta^*) \leqq \beta^*$. Hence $(\alpha^* \wedge^* (\alpha^* \to^* \beta^*)) \to^* \beta^* \equiv 1$.

Ad (h7). This case follows obviously from $\alpha^*(E) \leqq \max(\alpha^*(E), \beta^*(E)) = (\alpha^* \vee^* \beta^*)(E)$.

Ad (h8). This follows from (6b) and (11).

Ad (h9). (a) If $\alpha^*(E) \leqq \gamma^*(E)$, and $\beta^*(E) \leqq \gamma^*(E)$ then $((\alpha^* \to^* \gamma^*) \wedge^* (\beta^* \to^* \gamma^*))(E) = 1$, and $(\alpha^* \vee^* \beta^*)(E) = \max(\alpha^*(E), \beta^*(E)) \leqq \gamma^*(E)$, consequently $((\alpha^* \vee^* \beta^*) \to^* \gamma^*)(E) = 1$. — (b) If $\alpha^*(E) > \gamma^*(E)$, or $\beta^*(E) > \gamma^*(E)$, then $((\alpha^* \to^* \gamma^*) \wedge^* (\beta^* \to^* \gamma^*))(E) = \gamma^*(E)$, and $(\alpha^* \vee^* \beta^*)(E) = \max(\alpha^*(E), \beta^*(E)) > \gamma^*(E)$, hence $((\alpha^* \vee^* \beta^*) \to^* \gamma^*)(E) = \gamma^*(E)$. — In both cases the antecedent equals to the consequent, hence $((\alpha^* \to^* \gamma^*) \wedge^* (\beta^* \to^* \gamma^*)) \to^* ((\alpha^* \vee^* \beta^*) \to^* \gamma^*) \equiv 1$.

Ad (h10). (a) If $\alpha^*(E) = 0$ then $(\neg^* \alpha^*)(E) = 1$, and $\alpha^*(E) \leqq \beta^*(E)$, hence $(\alpha^* \to^* \beta^*)(E) = 1$. (b) If $\alpha^*(E) > 0$ then $(\neg^* \alpha^*)(E) = 0 \leqq (\alpha^* \to^* \beta^*)(E)$. — In both cases $\neg^* \alpha^* \leqq \alpha^* \to^* \beta^*$, henceforth $\neg^* \alpha^* \to^* (\alpha^* \to^* \beta^*) \equiv 1$.

Ad (h11). (a) If $\alpha^*(E) = 0$ then $((\alpha^* \to^* \beta^*) \wedge^* (\alpha^* \to^* \neg^* \beta^*))(E) \geqq 1 = (\neg^* \alpha^*)(E)$. (b) If $\alpha^*(E) > 0$ then — since $\beta^*(E)$ or $\neg^* \beta^*(E)$ equals to 0 — $((\alpha^* \to^* \beta^*) \wedge^* (\alpha^* \to^* \neg^* \beta^*))(E) = 0 = (\neg^* \alpha^*)(E)$. — In both cases the antecedent is $\leqq$ as the consequent; hence $((\alpha^* \to^* \beta^*) \wedge^* (\alpha^* \to^* \neg^* \beta^*)) \to^* \neg^* \alpha^* \equiv 1$.

Ad (h12) and (h13). If $x \notin J(\alpha)$ (see before Def. 2), then $W(\forall x \alpha) = W(\alpha) = W(\alpha(x/y))$ (see Def. 4, (f)). Henceforth, we may assume that $x \in J(\alpha)$. Assume that $J(\alpha) = \langle x_1, \ldots, x_n \rangle$, and x is x_i $(1 \leqq i \leqq n;\ n \geqq 1)$. Then (see Def. 4, (g)) $\Omega(\alpha) = \alpha^*$ is a function on U^n, and (see (1))

$$
(14) \quad \left\{
\begin{aligned}
&W(\forall x \alpha) = \inf_{u \in U} \alpha^*(f(x_1), \ldots, f(x_{i-1}), u, f(x_{i+1}), \ldots, f(x_n)),\\
&W(\exists x \alpha) = \sup_{u \in U} \alpha^*(f(x_1), \ldots, f(x_{i-1}), u, f(x_{i+1}), f(x_n)),\\
&W(\alpha(x/y)) = \alpha^*(f(x_1), \ldots, f(x_{i-1}), f(y), f(x_{i+1}), \ldots, f(x_n))
\end{aligned}
\right.
$$

(taking into account that y is free from x_i in α). Since $f(y) \in U$, it follows from these identities that

$$W(\forall x \alpha)(E) \leqq W(\alpha(x/y))(E) \leqq W(\exists x \alpha)(E)$$

for any $E \in I$. Hence $W(\forall x \alpha \to \alpha(x/y)) \equiv 1$ and $W(\alpha(x/y) \to \exists x \alpha) \equiv 1$.

THEOREM 2. *If $\alpha \in T$ then in any random model belonging to Z_{h1}, $W(\alpha) \equiv 1$ holds.*

REMARK. Using Def. 6 of [3] (see **§. 2**, Part 1) we can re-formulate our theorem as follows: The *rms* Z_{h1} is a total 1-representation of system H.

PROOF. We shall prove inductively that, if $\alpha \in T$ (according to (a) to (e) in the definition of T, see p. 78) then in any random model Γ belonging to Z_{h1}, $W(\alpha) \equiv 1$. Evidently, it is sufficient to prove that:

(a) and (b): If the structure of ω is the one of (h1) to (h13), then $W(\omega)\equiv 1$ holds in any Γ belonging to Z_{h1}.

(c) If $W(\alpha)\equiv 1$ and $W(\alpha\to\beta)\equiv 1$ hold in a Γ, then also $W(\beta)\equiv 1$ holds in this Γ.

(d) If $W(\alpha)\equiv 1$ and $W(\beta)\equiv 1$ hold in a Γ, then $W(\alpha\wedge\beta)\equiv 1$ holds in Γ, too.

(e) If in every Γ belonging to Z_{h1}, $W(\alpha\to\beta)\equiv 1$ $(W(\beta\to\alpha)\equiv 1)$ holds, then in any Γ belonging to Z_{h1}, $W(\alpha\to\forall x\beta)\equiv 1$ $(W(\exists x\beta\to\alpha)\equiv 1)$ holds, too, provided x has no free occurence in α.

(a) and (b) is proved in Th. 1. (c) and (d) follow easily from (3) and (2). We have to prove (e).

Assume that $W(\alpha\to\beta)\equiv 1$ holds in any random model belonging to Z_{h1}, and x has no free occurrence in α. Furthermore, assume, indirectly, that there is a random model Γ belonging to Z_{h1} in which $W(\alpha\to\forall x\beta)=1$ does not hold. If we use similar notation as in (14) in the proof of Th. 1, then our indirect assumption means that there is an $E\in I$ for which

$$\alpha^*(E)>\inf_{u\in U}\left(\beta^*(f(x_1),\ \ldots,f(x_{i-1}),u,f(x_{i+1}),\ \ldots,f(x_n))\,(E)\right).$$

The brief notation hereunder can lead to no misinterpretation:

$$\alpha^*(E)>\inf_{u\in U}\left(\beta^*(u)\,(E)\right).$$

From this it follows that there is an $u_1\in U$ for which

$$\alpha^*(E)>\beta^*(u_1)\,(E).$$

Let Γ_1 be a random model which differs from Γ only in $f(x)=u_1$. Since x has no free occurrence in α, it follows that in Γ_1, $W(\alpha)$ is the same as in Γ. Furthermore, in Γ_1, $W(\beta)\equiv\beta^*(u_1)$. Hence $W(\alpha)\,(E)>W(\beta)\,(E)$ in Γ_1. This implies that $W(\alpha\to\beta)\,(E)\neq 1$ in Γ_1, from which it follows that our indirect assumption contradicts to the assumption that $W(\alpha\to\beta)\equiv 1$ holds in any random model belonging to Z_{h1}.

The proof of the bracketed subcase of (e) is dual-analogous, hence it will be omitted here. — Thus Th. 2 is proved.

The *rms* Z_{h1} is not an "adequate" representation of system H, in the sense that the converse of Th. 2 does not hold. In other words: it is not true that if $\alpha\in F$, and $W(\alpha)\equiv 1$ holds in any random model belonging to Z_{h1} then $\alpha\in T$. A counter-example is the formula $\neg\alpha\vee\neg\neg\alpha$ $(\alpha\in F)$. It is well-known that $\neg p\vee\neg\neg p$ is not a theorem of H $(p\in V_0)$. However, $W(\neg\alpha\vee\neg\neg\alpha)\equiv 1$ holds in any random model belonging to Z_{h1}. Indeed, one may see immediately from (12) and (13) that one of $(\neg^*\alpha^*)\,(E)$, $(\neg^*\neg^*\alpha^*)\,(E)$ always equals to 1, consequently $W(\neg\alpha\vee\neg\neg\alpha)\equiv\max\left(W(\neg\alpha),W(\neg\neg\alpha)\right)\equiv 1$.

Let us consider the system $H_1=(J,V,O,F,T_1)$, where J, V, O and F are the same as in H (i.e. $H_1'=H'$), and T_1 is determined as follows: $\alpha\in T_1$ if and only if $\alpha\in F$, and for any random model belonging to Z_{h1}, $W(\alpha)\equiv 1$ holds.

THEOREM 3. (a) *If α is one of the formulas* (15) *to* (25) *below then* $\alpha\notin T_1$. (b) *If $\alpha\in F$, and α is not a valid formula of the two-valued predicate calculus* (of the first order), *then* $\alpha\notin T_1$.

(15) $p \vee \neg p$

(16) $\neg\neg p \to p$

(17) $(p \vee \neg p) \to (q \vee \neg q)$

(18) $\neg(\neg p \wedge \neg q) \to (p \vee q)$

(19) $\neg(\neg p \vee \neg q) \to (p \wedge q)$

(20) $\neg(p \to q) \to (p \wedge \neg q)$

(21) $(\neg p \to q) \to (\neg q \to p)$

(22) $(\neg p \to \neg q) \to (q \to p)$

(23) $(p \to q) \to (\neg p \vee q)$

(24) $\neg \forall x \neg qx \to \exists x qx$

(25) $\neg \exists x \neg qx \to \forall x qx$

(Here $p \in V_0$, $q \in V_0$, $q \in V_1$, $x \in J$.)

Proof. (a) Let us construct the random model $\Gamma = (U, f, \Sigma, \Omega, W)$ as follows. In $\Sigma = (I, \mathcal{A}, P)$ take $I = \{A, B, C\}$, $P(\{A\}) = P(\{B\}) = P(\{C\}) = \frac{1}{3}$, and let $\mathcal{A}$ be the σ-algebra of all subsets of I. Furthermore, we give:

$$p^{\cdot}(A) = 1/2, \qquad p^{\cdot}(B) = 1/2, \qquad p^{\cdot}(C) = 1$$
$$q^{\cdot}(A) = 0, \qquad q^{\cdot}(B) = 1, \qquad q^{\cdot}(C) = 1/2$$

Thus $\Omega(p) = W(p)$ and $\Omega(q) = W(q)$ are defined ($p \in V$, $q \in V$). Except for this stipulations, Γ may be arbitrarily chosen.

An easy computation shows that Γ "refutes" the formulas (15) to (22); i.e. if α is one of these formulas, then $W(\alpha) = 1$ does not hold in Γ.

Let Γ_1 be the same as Γ except that in Γ_1, $U = \{a, b\}$, and for $\Omega(q) = q^*$, $q^*(a) \equiv \Omega(p)$, and $q^*(b) \equiv \Omega(q)$ hold. Then Γ_1 "refutes" (24) and (25).

Let Γ_2 be the same as Γ except that in Γ_2

$$p^{\cdot}(A) = 0 \qquad p^{\cdot}(B) = 1, \qquad p^{\cdot}(C) = 1/2;$$
$$q^{\cdot}(A) = q^{\cdot}(B) = 1/2, \qquad q^{\cdot}(C) = 1.$$

Then Γ_2 "refutes" (23).

(b) Assume that $\alpha \in F$ but α is not valid in the two-valued logic. In [3] I proved that there is a random model Γ belonging to the *rms* Z_1 which "refutes" Γ (see Th. 9.2 in Part III). The stipulations used in the definition of this Γ are sufficient to define a random model Γ_1 belonging to $Z_{\aleph_1}$. This Γ_1 then "refutes" α in the sense that in Γ_1, $W(\alpha) \equiv 0$ holds. This follows from the facts that (i) any random variable in Γ and in Γ_1 equals to 0 or to 1; (ii) the laws

$$(26)\quad \begin{cases} 0\wedge^{\cdot}0 = 0\wedge^{\cdot}1 = 1\wedge^{\cdot}0 = 0, & 1\wedge^{\cdot}1 = 1, \\ 1\vee^{\cdot}1 = 0\vee^{\cdot}1 = 1\vee^{\cdot}0 = 1, & 0\vee^{\cdot}0 = 0 \\ 0\to^{\cdot}1 = 0\to^{\cdot}0 = 1\to^{\cdot}1 = 1, & 1\to^{\cdot}0 = 0 \\ \neg^{\cdot}0 = 1, \quad \neg^{\cdot}1 = 0, & \\ \forall^{\cdot}(B) = \begin{cases} 0, \text{ if } 0\in B, \\ 1 \text{ otherwise.} \end{cases} & \exists^{\cdot}(B) = \begin{cases} 1 \text{ if } 1\in B, \\ 0 \text{ otherwise} \end{cases} \end{cases}$$

holds in Z_1 as far as in Z_{h1} (here B is a set of random variables such that if $w\in B$ then $w\equiv 0$ or $w\equiv 1$); (iii) if β is a subformula of α then $W(\beta)$ in Γ_1 is the same as in Γ; and (iv) in Γ, $W(\alpha)\equiv 0$ holds.

Thus Th. 3 is proved. The meaning of this theorem is that H_1 is an intermediate system between H and the two-valued logic. It seems me that if we add to H the axiom scheme

$$(\neg\alpha\to\beta)\to(((\beta\to\gamma)\to\beta)\to\beta)$$

then we get H_1. But so far I have not succeeded in proving this conjecture.

§. 3. The random model structure Z_{h2}

We define the *rms* $Z_{h2} = (0, 1, \Theta)$ of the language H' as follows. Let the function operators $\forall^{\cdot}$, $\exists^{\cdot}$, $\neg^{\cdot}$, $\wedge^{\cdot}$ and $\vee^{\cdot}$ be the same as in Z_{h1}. For the definition of the function operator $\to^{\cdot}$ assume that w_1 and w_2 are random variables (on the same probability space Σ) with values in $[0, 1]$. We shall define the level sets $[w_1\to^{\cdot}w_2<z]$ of $w_1\to^{\cdot}w_2$ for any real z as follows:

$$(27)\qquad [w_1\to^{\cdot}w_2<z] = \begin{cases} 0 \text{ if } z\leq 0 \\ [w_2<s(z)] \text{ if } 0<z\leq 1, \\ I \text{ if } z>1; \end{cases}$$

here

$$(28)\qquad s(z) = \begin{cases} \sup Y(z), \text{ if } Y(z) \neq 0, \\ 0 \text{ otherwise;} \end{cases}$$

where $Y(z)$ is a set of real numbers for which $y\in Y(z)$ if and only if $0<y<z$ and $[w_1<y]\not\supseteq[w_2<y]$ hold. Note that if $[w_1<z]\not\supseteq[w_2<z]$ then $s(z) = z$. Hence:

$$(27')\qquad [w_1\to^{\cdot}w_2<z] = [w_2<z], \quad \text{if} \quad [w_1<z]\supseteq[w_2<z].$$

— It is clear that the function $w_1\to^{\cdot}w_2$ is fully determined by giving its level sets for all z. Furthermore, one may see immediately that the level sets of $w_1\to^{\cdot}w_2$ are measurable for any z (taking into account that w_1 and w_2 are random variables i.e. measurable functions), hence $w_1\to^{\cdot}w_2$ is a random variable (on Σ) which fulfils the stipulation (c) in Def. 3. — Finally, we define $\neg^{\cdot}$ similarly as in Z_{h1}:

$$(29)\qquad \neg^{\cdot}w = w\to^{\cdot}0.$$

In what follows we assume throughout this § that the restriction $0 \leqq w \leqq 1$ holds for any random variable w.

We list some simple consequences of the definitions above. First, it is clear that the laws (5) to (10) hold also in Z_{h2}. Similarly, it is clear that

$$s(z) \leqq z \tag{30}$$

holds for $s(z)$ in (28). — Furthermore,

$$w \to^{\cdot} w \equiv 1. \tag{31}$$

PROOF. Since $[w<1] \supseteq [w<1]$, it follows from (27) that $[w \to^{\cdot} w<1] = [w<s(1)]$. Taking into account that for $0<y<1$, $[w<y] \supseteq [w<y]$, we get that the set $Y(1)$ in (28) is empty, henceforth $s(1)=0$. Consequently $[w \to^{\cdot} w<1] = [w<0] = \emptyset$. From this and the third line of (27) it follows (31).

A simple consequence of (31) and (29):

$$\neg^{\cdot} 0 = 0 \to^{\cdot} 0 \equiv 1 \tag{32}$$

If $[w>0] \neq \emptyset$ then $\neg^{\cdot} w \equiv 0$.

PROOF. From our assumption it follows that there is a number z_0 such that $0<z_0 \leqq 1$, and for $0<z<z_0$, $[w<z] \neq I$. But $z>0$ implies that $[0<z] = I$. Hence $[w<z] \not\supseteq [0<z]$, if $0<z<z_0$. Consequently (using (29) and (27')):

$$[\neg^{\cdot} w<z] = [w \to 0<z] = [0<z] = I \qquad \text{for } 0<z<z_0.$$

From this it follows that for *any* positive z, $[\neg^{\cdot} w<z] = I$. This means that $\neg^{\cdot} w \equiv 0$. — From this result and (32) we get that

$$\neg^{\cdot} w = \begin{cases} 1 & \text{if } w \equiv 0, \\ 0 & \text{otherwise}. \end{cases} \tag{33}$$

From (33) it follows immediately:

$$\neg^{\cdot}\neg^{\cdot} w = \begin{cases} 1 & \text{if } \neg^{\cdot} w \equiv 0, \text{ i.e. if } w \text{ is not identically } 0, \\ 0 & \text{if } \neg^{\cdot} w \text{ is not identically } 0, \text{ i.e. if } \neg^{\cdot} w \equiv 1, \text{ i.e. if } w \equiv 0. \end{cases}$$

In its final form:

$$\neg^{\cdot}\neg^{\cdot} w \equiv \begin{cases} 0 & \text{if } w \equiv 0, \\ 1 & \text{otherwise}. \end{cases} \tag{34}$$

A further simple law: for all z,

$$[w_1 \to^{\cdot} w_2<z] \subseteq [w_2<z]. \tag{35}$$

For $z \leq 0$ this follows from the first line of (27). For $0<z \leq 1$ our statement follows from the second line of (27), since

$$[w_1 \to w_2<z] = [w_2<s(z)] \subseteq [w_2<z]$$

(with respect to (30), too). — For $z>1$, (35) holds obviously, since $w_2 \leqq 1$.

LEMMA 4. $w_1 \to^{\cdot} w_2 \equiv 1$ if and only if $[w_1<z] \supseteq [w_2<z]$ holds for $0<z \leq 1$.

PROOF. Assume that $[w_1<z]\supseteq[w_2<z]$ for $0<z\leqq 1$. From this it follows that $Y(z)=0$ for $0<z\leqq 1$. Hence $s(z)=0$ for $0<z\leqq 1$. Consequently:

$$[w_1\to^{\cdot} w_2<z] = [w_2<s(z)] = [w_2<0] = 0 \text{ for } 0<z\leqq 1$$

(taking into account that $w_2\geqq 0$). From this and the last line of (27) we get that $w_1\to^{\cdot} w_2=1$.

Conversely, if $w_1\to^{\cdot} w_2\equiv 1$, then $[w_1\to^{\cdot} w_2<z]=0$ for $z\leqq 1$. If for a z $(0<z\leqq 1)$, $[w_1<z]\not\supseteq[w_2<z]$, then, according to (27'), $0=[w_1\to^{\cdot} w_2<z]=[w_2<z]$, but this contradicts to $[w_1<z]\not\supseteq[w_2<z]$. Hence $[w_1<z]\supseteq[w_2<z]$ holds for $0<z\leqq 1$.

REMARK. Lemma 4 remains true even if we put "$\leqq$" instead of "$<$".

THEOREM 4. *If the structure of a formula ω is one of* (h1) *to* (h13) *except* (h3) (see in the definition of T, p. 78), *then in any random model Γ belonging to the rms Z_{h2}, $W(\omega)=1$ holds.*

PROOF. The form of the mentioned formulas is always $\eta\to\lambda$. According to Lemma 4, to prove that $W(\eta\to\lambda)=1$, it is sufficient to prove that for $0<z\leqq 1$, $[\eta<z]\supseteq[\lambda<z]$ holds. (We write briefly $[\alpha<z]$ instead of $[W(\alpha)<z]$ for any $\alpha\in F$.) In what follows we shall exploit this fact without particular reference.

For (h1) and (h2) the statement of the theorem follows from (5a), (6a) and (31).

Ad (h4). Let η be $(\alpha\to\beta)\wedge(\beta\to\gamma)$. We shall distinguish four cases.

Case (i):

$$[\alpha<z]\not\supseteq[\beta<z] \quad\text{and}\quad [\beta>z]\not\supseteq[\gamma<z]. \tag{36}$$

From this, using (7), (27') and (35), we get:

$$[\eta<z] = [\alpha\to\beta<z]\cup[\beta\to\gamma<z] = [\beta<z]\cup[\gamma<z]\supseteq[\gamma<z]\supseteq[\alpha\to\gamma<z].$$

Case (ii):

$$[\alpha<z]\not\supseteq[\beta<z], \quad\text{but}\quad [\beta<z]\supseteq[\gamma<z]. \tag{37}$$

In this case we have:

$$[\eta<z]=[\alpha\to\beta<z]\cup[\beta\to\gamma<z]=[\beta<z]\cup[\beta\to\gamma<z]\supseteq[\beta<z]\supseteq[\gamma<z]\supseteq[\alpha\to\gamma<z]$$

(using (37) and (35)).

Case (iii):

$$[\alpha<z]\supseteq[\beta<z], \quad\text{but}\quad [\beta<z]\not\supseteq[\gamma<z].$$

Similarly as in the preceding cases we get:

$$[\eta<z] = [\alpha\to\beta<z]\cup[\beta\to\gamma<z]\supseteq[\gamma<z]\supseteq[\alpha\to\gamma<z].$$

Case (iv):

$$[\alpha<z]\supseteq[\beta<z], \quad\text{and}\quad [\beta<z]\supseteq[\gamma<z]. \tag{38}$$

From (38) it follows that $[\alpha<z]\supseteq[\gamma<z]$. Hence:

$$[\alpha\to\beta<z] = [\beta<s_1(z)],$$
$$[\beta\to\gamma<z] = [\gamma<s_2(z)],$$
$$[\alpha\to\gamma<z] = [\gamma<s_3(z)].$$

Take: $s=\max(s_1(z), s_2(z))$. It is clear that if $s<z_0<z$ then (38) is true for z_0 (instead of z), hence $[\alpha<z_0]\supseteq[\gamma<z_0]$ is true for any such z_0. (Take into account (30), too.) This means that $s_3(z)\leqq s$. We have to distinguish two subcases.

(a) $s_1(z)\leqq s_2(z)$. Then $s_3(z)\leqq s_2(z)$. Hence:

$$[\eta<z] = [\beta<s_1(z)]\cup[\gamma<s_2(z)]\supseteq[\gamma<s_2(z)]\supseteq[\gamma<s_3(z)] = [\alpha\to\gamma<z].$$

(b) $s_1(z)>s_2(z)$. Then $[\beta<s_1(z)]\supseteq[\gamma<s_1(z)]$, and $s_3(z)\leqq s_1(z)$. Hence

$$[\eta<z]=[\beta<s_1(z)]\cup[\gamma<s_2(z)]\supseteq[\beta<s_1(z)]\supseteq[\gamma<s_1(z)]\supseteq[\gamma<s_3(z)] = [\alpha\to\gamma<z].$$

In all cases (i) to (iv) we get that $[\eta<z]$(i.e. $[(\alpha\to\beta)\wedge(\beta\to\gamma)<z]$) includes $[\alpha\to\gamma<z]$.

Ad (h5). According to (35) we have that

$$[\beta<z]\supseteq[\alpha\to\beta<z].$$

Ad (h6). If $[\alpha<z]\supseteq[\beta<z]$ then

$$[\alpha\wedge(\alpha\to\beta)<z] = [\alpha<z]\cup[\alpha\to\beta<z]\supseteq[\alpha<z]\supseteq[\beta<z].$$

In other cases $[\alpha\to\beta<z] = [\beta<z]$ (see (27')), thus

$$[\alpha\wedge(\alpha\to\beta)<z]\supseteq[\alpha\to\beta<z] = [\beta<z].$$

Consequently, in all cases, $[\alpha\wedge(\alpha\to\beta)<z]\supseteq[\beta<z]$.

Ad (h7). Since $[\alpha\vee\beta<z] = [\alpha<z]\cap[\beta<z]\subseteq[\alpha<z]$ (see (8), too), this case is obvious.

Ad (h8). This case follows from (6b) and (31).

Ad (h9). We shall distinguish two cases.

First case: at least one of $[\alpha<z]\not\supseteq[\gamma<z]$ and $[\beta<z]\not\supseteq[\gamma<z]$ is true. Then one of $[\alpha\to\gamma<z]$, $[\beta\to\gamma<z]$ equals to $[\gamma<z]$. Hence (using (35)), too:

$$[(\alpha<\gamma)\wedge(\beta\to\gamma)<z] = [\alpha\to\gamma<z]\cup[\beta\to\gamma<z]\supseteq[\gamma<z]\supseteq[(\alpha\vee\beta)\to\gamma<z].$$

Second case: $[\alpha<z]\supseteq[\gamma<z]$, and $[\beta<z]\supseteq[\gamma<z]$. Then $[\alpha\vee\beta<z] = [\alpha<z]\cap[\beta<z]\supseteq[\gamma<z]$. Hence:

$$[\alpha\to\gamma<z] = [\gamma<s_1(z)],\ [\beta\to\gamma<z] = [\gamma<s_2(z)],[(\alpha\vee\beta)\to\gamma<z] = [\gamma<s_3(z)].$$

One may see easily that $s_3(z)\leqq\max(s_1(z), s_2(z))$ (similarly as in "Case (iv)" in "Ad (h4)"). Henceforth:

$$[(\alpha\to\gamma)\wedge(\beta\to\gamma)<z] = [\gamma<s_1(z)]\cup[\gamma<s_2(z)] =$$
$$= [\gamma<\max(s_1(z), s_2(z))]\supseteq[\gamma<s_3(z)] = [(\alpha\vee\beta)\to\gamma<z].$$

We see that in both cases $[(\alpha\to\gamma)\wedge(\beta\to\gamma)<z]$ includes $[\alpha\vee\beta)\to\gamma<z]$.

Ad (h10). *First case:* $W(\neg\alpha)=0$. Then, for $z>0$

$$[\neg\alpha<z] = [0<z] = I \supseteq [\alpha\to\beta<z].$$

Second case: $W(\neg\alpha)=1$. Then $W(\alpha)\equiv 0$ (see (33)), and for $z>0$

$$[\alpha<z] = [0<z] = I \supseteq [\beta<z],$$

hence $W(\alpha\to\beta)\equiv 1$. Consequently:

$$W(\neg\alpha\to(\alpha\to\beta)) = W(\neg\alpha)\to^{\cdot}W(\alpha\to\beta) = 1\to^{\cdot}1 = 1.$$

Ad (h11). *First case:* $W(\alpha)\equiv 0$. Then $W(\neg\alpha)\equiv 1$, hence:

$$[(\alpha\to\beta)\wedge(\alpha\to\neg\beta)<z]\supseteq 0=[1<z]=[\neg\alpha<z] \quad \text{for } z\geq 1.$$

Second case: $W(\neg\alpha)=0$. In this case there is a number z_0 such that $0<z_0\leq 1$, and for $0<z<z_0$, $[\alpha<z]\neq I$. Taking into account that $W(\beta)\equiv 0$ or $W(\neg\beta)\equiv 0$ we get that

$$[\beta<z] = I \text{ or } [\neg\beta<z] = I \tag{39}$$

holds for $z>0$. Consequently, for $0<z<z_0$,

$$[\alpha<z]\not\supseteq[\beta<z] \text{ or } [\alpha<z]\not\supseteq[\neg\beta<z]$$

holds. Hence

$$[\alpha\to\beta<z] = [\beta<z] \text{ or } [\alpha\to\neg\beta<z] = [\neg\beta<z]$$

for $0<z<z_0$. From this and (39) it follows that

$$[(\alpha\to\beta)\wedge(\alpha\to\neg\beta)<z] = I$$

for $0<z<z_0$, and for $z\geq z_0$ this is true *a fortiori*. Hence

$$[(\alpha\to\beta)\wedge(\alpha\to\neg\beta)<z] = I = [\neg\alpha<z]$$

holds for $z>0$.

Ad (h12) and (h13). Consider the identities given in (14). Let us introduce the abbreviations

$$W(\forall x\alpha) \equiv \inf_{u\in U}\alpha^*(u); \qquad W(\exists x\alpha) \equiv \sup_{u\in U}\alpha^*(u); \tag{40}$$

$$W(\alpha(x/y)) \equiv \alpha^*(f(y)).$$

Using the identities (9) and (10), and taking into account that $f(y)\in U$, we get

$$[\forall x\alpha<z] = \bigcup_{u\in U}[\alpha^*(u)<z]\supseteq[\alpha^*(f(y))<z] =$$

$$= [\alpha(x/y)<z]\supseteq\bigcup_{u\in U}[\alpha^*(u)<z]\supseteq[\exists x\alpha<z].$$

This means that

$$[\forall x\alpha<z]\supseteq[\alpha(x/y)<z] \quad \text{and} \quad [\alpha(x/y)<z]\supseteq[\exists x\alpha<z]$$

for all z. — Thus Th. 4 is proved.

The following counter-example shows that there is no possibility of extending Th. 4 to (h3).

Let I be $\{A, B, C\}$ let $\mathcal{A}$ be the σ-algebra of all subsets of I, and let $P(\{A\}) = P(\{B\}) = P(\{C\})$ be $1/3$. Then the probability space $\Sigma = (I, \mathcal{A}, P)$ is fully determined. Let p, q and r be elements of V_0 (i.e. let p, q and r be sentence variables), and let $\Omega(p)$, $\Omega(q)$ and $\Omega(r)$ be the characteristic random variables of $\{A\}$, $\{\bar{B}\}$ and $\{\bar{C}\}$ respectively; i.e. assume that the identities

$$[p = 1] = \{\bar{A}\},\ [q = 1] = \{\bar{B}\},\ [r = 1] = \{\bar{C}\},$$
$$[p = 0] = \{A\},\ [q = 0] = \{B\},\ [r = 0] = \{C\}$$

hold. Finally, let $\Gamma = (U, f, \Sigma, \Omega, W)$ be a random model belonging to Z_{h2}, where Σ is as given above, Ω fulfils the requirements just given for p, q and r, otherwise it may be arbitrary. U and f may be given arbitrarily as well.

We shall get that in Γ, $W((p \to q) \to ((p \wedge r) \to (q \wedge r))) = 1$ does not hold.

PROOF. If $0 < z \leqq 1$ then

$$[p < z] = [p = 0] = \{A\};\quad [q < z] = [q = 0] = \{B\};\quad [r < z] = [r = 0] = \{C\}.$$

We see that $[p < z] \not\supseteq [q < z]$, hence:

$$[p \to q < z] = [q < z] = \{B\} \qquad (0 < z \leqq 1). \tag{41}$$

Furthermore:

$$[p \wedge r < z] = [p < z] \cup [r < z] = \{A, C\}, \quad \text{and}$$
$$[q \wedge r < z] = [q < z] \cup [r < z] = \{B, C\}.$$

We see that $[p \wedge r < z] \not\supseteq [q \wedge r < z]$, hence

$$[(p \wedge r) \to (q \wedge r) < z] = [q \wedge r < z] = \{B, C\} \qquad (0 < z \leqq 1).$$

From this and (41) we get that

$$[p \to q < z] \not\supseteq [(p \wedge r) \to (q \wedge r) < z] \quad \text{for} \quad 0 < z \leqq 1.$$

From this it follows — according to Lemma 4 — that our statement is true.

Our counter-example shows that the *rms* Z_{h2} is not a total 1-representation of system H. However, it is a total 1-representation of a subsystem of H. This follows from the next theorem.

THEOREM 5. *In the rms Z_{h2} the following laws hold:*

(a) *If* $\mathfrak{w}_1 \to^* \mathfrak{w}_2 \equiv 1$ *and* $\mathfrak{w}_1 \equiv 1$ *then* $\mathfrak{w}_2 \equiv 1$.

(b) *If* $\mathfrak{w}_1 \equiv 1$ *and* $\mathfrak{w}_2 \equiv 1$, *then* $\mathfrak{w}_1 \wedge^* \mathfrak{w}_2 \equiv 1$.

(c) *If* $\mathfrak{w}_1 \to^* \mathfrak{w}_2 \equiv 1$ *then* $(\mathfrak{w}_1 \wedge^* \mathfrak{w}_3) \to^* (\mathfrak{w}_2 \wedge^* \mathfrak{w}_3) = 1$.

(d) *If* $\alpha \to \beta \in F$ (i.e. *if* $\alpha \to \beta$ *is a formula of* H), $x \in J$, *and* $W(\alpha \to \beta) \equiv 1$ *holds in any random model belonging to* Z_{h2}, *then:*

if x *has no free occurrence in* α, *then* $W(\alpha \to \forall x \beta) \equiv 1$.

if x *has no free occurrence in* β, *then* $W(\exists x \alpha \to \beta) \equiv 1$ *holds in any random model belonging to* Z_{h2}, *too.*

PROOF.

For (a). From $w_1 \equiv 1$ it follows that $[w_1 < 1] = 0$. From $w_1 \rightarrow^* w_2 \equiv 1$ and Lemma 4 it follows that $0 = [w_1 < 1] \supseteq [w_2 < 1]$, that is $[w_2 < 1] = 0$, too. This means that $w_2 \equiv 1$, indeed.

For (b). The statement follows immediately from the definition of $\wedge^*$, see in (2).

For (c). From $w_1 \rightarrow^* w_2 \equiv 1$ it follows (see Lemma 4) that $[w_1 < z] \supseteq [w_2 < z]$ for all z. Hence:

$$[w_1 \wedge^* w_3 < z] = [w_1 < z] \cup [w_3 < z] \supseteq [w_2 < z] \cup [w_3 < z] = [w_2 \wedge^* w_3 < z].$$

According to Lemma 4, from this result it follows that $(w_1 \wedge^* w_3) \rightarrow^* (w_2 \wedge^* w_3) \equiv 1$.

For (d). Assume that $W(\alpha \rightarrow \beta) \equiv 1$ holds in any random model belonging to Z_{h2}, and x has no free occurrence in α (in β). Furthermore, assume, indirectly, that there is a random model Γ belonging to Z_{h2} in which $W(\alpha \rightarrow \forall x \beta) \equiv 1$ $(W(\exists x \alpha \rightarrow \beta) \equiv 1)$ does not hold. Using similar notation as in (40), this means (according to (9), (10) and Lemma 4) that there is a number z $(0 < z \leq 1)$ for which

$$[\alpha < z] \not\supseteq \bigcup_{u \in U} [\beta^*(u) < z] \quad \left(\bigcap_{u \in U} [\alpha^*(u) \leq z] \not\supseteq [\beta \leq z]\right).$$

From this it follows that there is an $u_1 \in U$ such that

$$[\alpha < z] \not\supseteq [\beta^*(u_1) < z] \quad ([\alpha^*(u_1) \leq z] \not\supseteq [\beta \leq z]). \tag{42}$$

Let Γ_1 be a random model which differs from Γ only in $f(x) = u_1$. Since x has no free occurrence in α (in β), it follows that in Γ_1, $W(\alpha)$ $(W(\beta))$ is the same as in Γ. Furthermore, $W(\beta) \equiv \beta^*(u_1)$ $(W(\alpha) = \alpha^*(u_1))$ in Γ_1. Hence in Γ_1, $[\alpha < z] \not\supseteq [\beta < z]$ (see also (42)). But this contradicts to the assumption that in *any* random model belonging to Z_{h2} (consequently also in Γ_1), $W(\alpha \rightarrow \beta) \equiv 1$ holds (taking into consideration Lemma 4, too).

Let us consider the system $H_2 = (J, V, O, F, T_2)$, where J, V, O and F are the same as in H (i.e. $H_2' = H'$), and T_2 is determined as follows: $\alpha \in T_2$ if and only if $\alpha \in F$, and for any random model belonging to Z_{h2}, $W(\alpha) \equiv 1$ holds.

It follows immediately from Th. 4 and 5:

(a) If $\omega \in F$ and the structure of ω is one of (h1) to (h13) except (h3) then $\omega \in T_2$. (b) If $\alpha \in T_2$, $\beta \in F$, and $\alpha \rightarrow \beta \in T_2$, then $\beta \in T_2$. (c) If $\alpha \in T_2$, and $\beta \in T_2$ then $\alpha \wedge \beta \in T_2$. (d) If $\alpha \in F$, $\beta \in F$, $\gamma \in F$, and $\alpha \rightarrow \beta \in T_2$, then $(\alpha \wedge \gamma) \rightarrow (\beta \wedge \gamma) \in T_2$. (e) If $\alpha \in F$, $\beta \in F$, $x \in J$, and x has no free occurrence in α then:

(e1) if $\alpha \rightarrow \beta \in T_2$ then $\alpha \rightarrow \forall x \beta \in T_2$.
(e2) if $\beta \rightarrow \alpha \in T_2$ then $\exists x \beta \rightarrow \alpha \in T_2$.

Some properties of the system H_2:

(i) H_2 is a proper part of the two-valued logic. Namely, on the one hand, if $\alpha \in F$, but α is not valid in the two-valued logic, then $\alpha \notin T_2$. The proof of this statement is the same as the proof of Th.3 (b), taking into account that the laws listed in (26) hold also in Z_{h2}. On the other hand, there are formulas which are valid in the two-valued logic, but are not theorems of H_2. Such a formula is e.g. (h3).

(ii) H_2 is not a proper subsystem of H. This means that there are such formulas α for which $\alpha \notin T$ but $\alpha \in T_2$. Such an α is e.g. $\neg p \vee \neg\neg p$. It follows easily from (33) and (34) that $\neg p \vee \neg\neg p \in T_2$.

(iii) Probably, H_2 is a proper subsystem of H_1, i.e. probably $T_2 \subset T_1$.

System H_2 is, like H_1, a kind of quasi-intuitionistic logic.

References

[1] A. Heyting, Die formalen Regeln der intuitionistischen Logik, *Sitzungsberichte der Berliner Akademie der Wiss., Phys.-math. Klasse*, 1930, 42–56.

[2] S. C. Kleene, *Introduction to Metamathematics*, North-Holland Pub. Co., Amsterdam, 1952.

[3] I. Ruzsa, Random models of logical systems, Part I. *Studia Sci. Math. Hung.*, 4 (1969), 289–300. – Part II and III are in print (int the next number of the same periodical).

ÜBER DIE TEILWEISE GEORDNETE MENGE DER KONJUGIERTEN UNTERGRUPPEN

Von

E. FRIED

Lehrstuhl für Algebra und Zahlentheorie der Eötvös Loránd Universität, Budapest

(Eingegangen am 26. Jänner 1969)

1. Einleitung

Es sei H eine beliebige Untergruppe der Gruppe G. Die Menge $\Sigma(G; H)$ aller konjugierten Untergruppen vom H bildet bezüglich des mengentheoretischen Erhaltenseins eine teilweise geordnete Menge. Ist G endlich, so muss $\Sigma(G; H)$ triwialerweise ungeordnet sein. Es sind aber Gruppen bekannt, wo $\Sigma(G; H)$ für eine geeignete Untergruppe eine Kette bildet. (Siehe [1] Seite 61 und [2]).

Es sei $\mathcal{S}$ eine teilweise geordnete Menge. Wenn eine Gruppe G mit einer Untergruppe H derart existiert, daß $\Sigma(G; H) \cong \mathcal{S}$ ist, dann sprechen wir über eine Darstellung der teilweisen geordneten Menge $\mathcal{S}$ in der Form $\Sigma(G; H)$.

Wir wollen in dieser Note diejenige teilweise geordnete Mengen $\mathcal{S}$ charakterisieren die sich in der Form $\Sigma(G; H)$ darstellen lassen.

Ist $\mathcal{S}$ eine Kette, so werden wir für das Paar $(G; H)$ mit $\mathcal{S} \cong \Sigma(G; H)$ noch eine andere Konstruktion angeben.

2. Zwei wichtige Beispiele

Daß die eben erwähnte Konstruktione tatsächlich verschieden Charaktere haben, werden wir in den nachstehenden Beispielen mit Hilfe der Normalisatoren der konjugierten Untergruppe zeigen.

Beispiel I. Als erstes Beispiel geben wir eine Gruppe an, die mit der in [1] gegebene Gruppe isomorph ist.

Es sei N die Gruppe aller diadischen rationalen Zahlen (d.h. deren Nenner eine Potenz von 2 ist), und betrachten wir die Menge aller Paaren (a, b), wo a in N liegt und b eine natürliche Zahl ist.

Diese Paare bilden dann eine Gruppe G, wenn die Multiplikation folgendermaße definiert wird:

$$(a, b)\cdot(a_1, b_1) = (a+2^b a_1, b+b_1).$$

Die Untergruppe H sei wie folgt erklärt:

$(a, b)\in H$ dann und nur dann, wenn a eine ganze Zahl und $b = 0$ ist. (H ist offenbar eine Untergruppe der Gruppe G.)

Man läßt sich leicht zeigen, daß $\Sigma(G; H)$ mit der geordneten Menge der ganzen Zahlen isomorph ist.

Der Normalisator $N(H)$ der Untergruppe H besteht aus den Elementen $(a, 0)$. Beobachten wir, daß der Normalisator $N(H')$ einer beliebigen zu H konjugierten Untregruppe H' ebenfalls mit N übereinstimmt.

Beispiel II. Betrachten wir jetzt die monoton-wachsenden reellen Funktionen, die zugleich Permutationen der Menge der reellen Zahlen sind. Solche Funktionen wollen wir monotone Permutationen nennen. Diese monotone Permutationen bilden eine Untergruppe aller Permutationen der reellen Zahlen. Wir definieren die Untergruppe H von G wie folgt:

$f(x)\in H$ genau dann, wenn für jedes $\alpha\geqq 0$ $f(\alpha)=\alpha$ ist.

Man kann leicht beweisen, daß $\Sigma(G; H)$ isomorph mit der geordneten Menge der reellen Zahlen ist.

Der Normalisator $N(H)$ besteht aus den Funktionen für die $f(0) = 0$ gilt.

Es sei $g\in G$ eine beliebige Funktion, so ist $h\in g^{-1}Hg$ genau dann, wenn für $\alpha\geqq g(0)$, $h(\alpha) = \alpha$ ist, und $h\in N(g^{-1}Hg)$ genau dann, wenn $h(g(0)) = g(0)$ ist. Das bedeutet, daß die Normalisatoren zwei verschiedener konjugierten Untergruppen der Gruppe H ebenso verschieden sind.

3. Die Bestimmung der teilweise geordnete Menge $\Sigma(G; H)$

Es ist bekannt, daß die Abbildung

$$\Phi : a^{-1}Ha \to Na \qquad (N = N(H) \text{ und } a\in G)$$

eine ein-eindeutige Abbildung ist. Wir können dann die rechtseitige Nebenklassen folgendermaße ordnen:

$Na\leqq Nb$ genau dann, wenn $a^{-1}Ha$ in $b^{-1}Hb$ liegt.

Wir werden diese teilweise geordnete Menge mit $\mathcal{S}(G; H)$ bezeichnen. (Nach der Definition $\Sigma(G; H)\cong\mathcal{S}(G; H)$ ist.)

Es sei $\mathcal{S}$ eine beliebige teilweise geordnete Menge und σ eine Permutation von $\mathcal{S}$. Das Bild eines $A\in\mathcal{S}$ wollen wir mit A^σ bezeichnen. Die Permutation σ wird eine Ordnungspermutation genannt, falls aus $A\leqq B$ stets $A^\sigma\leqq B^\sigma$ folgt ($A, B\in\mathcal{S}$). Sind σ und σ^{-1} beide Ordnungspermutationen, so heiße σ monoton.

(i) Man kann die monotone Permutationen, wie Permutationen schlechthin, multiplizieren.

(ii) Man kann zwischen Permutationen die folgende Relation einführen:

$\sigma\leqq\tau$ genau dann, wenn aus $A\in\mathcal{S}$ stets $A^\sigma\leqq A^\tau$ folgt.

Es bezeichne $M(\mathcal{S})$ die Menge aller monotonen Permutationen der teilweisen geordneten Menge $\mathcal{S}$, mit der Operation und mit der Relation definiert in (i) bzw. (ii).

SATZ 1. *$M(\mathcal{S})$ ist eine teilweise geordnete Gruppe.*

BEWEIS. Die Ordnungspermutationen bilden offenbar eine Halbgruppe mit Einselement. Daraus folgt, daß $M(\mathcal{S})$ eine Gruppe ist. Die, in (ii) definierte Relation ist offenbar reflexiv, solange die Transitivität bzw. die Symmetrie folgt aus der Transitivität bzw. aus der Symmetrie der Ordnungsrelation der teilweise geordnete Menge $\mathcal{S}$. Es seien weiter σ, τ, ϱ mit $\sigma \leqq \tau$ beliebige Elemente aus $M(\mathcal{S})$. Für jedes $U \in \mathcal{S}$ aus $\sigma \leqq \tau$ folgt $U^\sigma \leqq U^\tau$ und so auch $(U^\sigma)^\varrho \leqq (U^\tau)^\varrho$. Anderseits, aus $\sigma \leqq \tau$ erhalten wir, daß $(U^\varrho)^\sigma \leqq (U^\varrho)^\tau$ ist. So ist sowohl $\sigma\varrho \leqq \tau\varrho$ wie $\varrho\sigma \leqq \varrho\tau$ gültig, d.h. die Monotonität ist erfüllt.

Wir definieren, für jedes a aus G, die Abbildungen

$$\sigma_a : Nx \to (Nx)^{\sigma_a} = Nxa$$

(G und H sind gegeben; $N = N(H)$).

SATZ 2. *Es gilt $\sigma_a \in M(\mathcal{S}(G; H))$. Die Abbildung $\sigma : a \to \sigma_a$ ist ein Homomorphismus von G in $M(\mathcal{S}(G; H))$, deren Kern, $\operatorname{Ker}\sigma = N^* = \bigcap_{x \in G} x^{-1}Nx$ ist.*

BEWEIS. Bekanntlich ist σ_a eine Permutation der Menge aller rechtseitigen Nebenklassen. $Nx \leqq Ny$ bedeutet $x^{-1}Hx \subseteq y^{-1}Hy$, woraus $a^{-1}x^{-1}Hxa \subseteq$ $\subseteq a^{-1}y^{-1}Hya$, ferner $Nxa \leqq Nya$ folgt. So ist σ_a eine Ordnungspermutation. Aus $(\sigma_a)^{-1} = \sigma_{a^{-1}}$ folgt nach Satz 1. $\sigma_a \in M(\mathcal{S}(G; H))$.

Wegen $(Nx)^{\sigma_a \sigma_b} = (Nxa)^{\sigma_b} = Nxab = (Nx)^{\sigma_{ab}}$ folgt, daß σ wirklich ein Homomorphismus ist. Zuletzt, liegt a in $\operatorname{Ker}\sigma$ genau dann, wenn $Nxa = Nx$ d.h. $xax^{-1} \in N$ gilt ($x \in G$). Das bedeutet aber, daß a ein Element der (normalen) Untergruppe N^* $(= \bigcap_{x \in G} x^{-1}Nx)$ ist.

Betrachten wir jetzt den Homomorphismus $\sigma : G \to M(\mathcal{S}(G; H))$. Bekanntlich, das vollinverse Bild des Bildes der Untergruppe $a^{-1}Ha$ stimmt mit $a^{-1}HN^*a$ überein. Aus $a^{-1}Ha \subseteq H$ folgt $a^{-1}HN^*a \subseteq HN^*$. So ist $\Sigma(G; HN^*)$ ein ordnungshomomorphes Bild der teilweisen geordneten Menge $\Sigma(G; H)$. Wegen des Ordnungisomorphismus $\Sigma(G; HN^*) \cong \Sigma(G/N^*; HN^*/N^*)$ haben wir gewonnen:

LEMMA 1. Die Abbildung $\sigma^* : a^{-1}Ha \to (aN^*)^{-1}(HN^*/N^*)(aN^*)$ ist ein Ordnungshomomorphismus von $\Sigma(G; H)$ in $\Sigma(G/N^*; HN^*/N^*)$.

Es sei $\Sigma(G; H)$ eine Darstellung der teilweisen geordneten Menge $\mathcal{S}$. Wir wollen diese Darstellung *separabel* bzw. *vollständig inseparabel* nennen, wenn σ^* ein Isomorphismus bzw. $\Sigma(G/N^*; HN^*/N^*)$ einelementig ist.

4. Die Darstellung einer teilweisen geordneten Menge als $\Sigma(G; H)$

Bevor wir eine notwendige und hinreichende Bedingung zur Darstellung angeben, werden wir das Kranzprodukt (s. : [1]) verallgemeinern.

Es sei eine Gruppe G, eine Menge $\mathcal{S}$ und eine Untergruppe Θ der Permutationsgruppe $H(\mathcal{S})$ der Menge $\mathcal{S}$ gegeben. Betrachten wir das diskreten direkten Produkt $G_{\mathcal{S}}$ der mit den Elementen der Menge $\mathcal{S}$ indizierten Exemplaren der Gruppe G. Wir können dann die Elemente von $G_{\mathcal{S}}$ als diejenige Abblidungen $f : \mathcal{S} \to G$ betrachten, für die $f(A)$ nur für endlich viele $A \in \mathcal{S}$ von dem Einselement der Gruppe G verschieden ist.

Das Produkt fg der Elementen f und g der Gruppe $G_{\mathcal{S}}$ ist durch $fg(A) = (f(A))\cdot(g(A))$ festgelegt.

Wir definieren das *Permutationsprodukt* $\Pi(G; \mathcal{S}; \Theta)$ als die zerfallende Erweiterung der Gruppe $G_{\mathcal{S}}$ durch Θ die der Bedingung

$$(\sigma^{-1}f\sigma)(A) = f(A^{\sigma}) \text{ für alle } A\in\mathcal{S},\ \sigma\in\Theta,\ f\in G_{\mathcal{S}}$$

genügt. Es kann durchaus paßieren, daß die Menge $\mathcal{S}$ aus den Elementen einer Gruppe H und Θ aus der rechtseitigen Multiplikation der Gruppe H besteht. In diesem Fall geht das Permutationsprodukt in das Kranzprodukt $G\ \ H$ über.

Wir werden nur das Permutationsprodukt $\Pi(Z; \mathcal{S}; \Theta)$ benutzen, wo Z die additive Gruppe der ganzen Zahlen bezeichnet.

Es sei $\mathcal{S}'$ eine beliebige Teilmenge der Menge $\mathcal{S}$. Wir betrachten die Menge $G(\mathcal{S}')$ derjenigen Elementen f aus $Z_{\mathcal{S}}$, für die aus $A\notin\mathcal{S}'$ $f(A) = 0$ folgt. $G(\mathcal{S}')$ ist, offenbar, eine Untergruppe der Gruppe $Z_{\mathcal{S}}$. Es sei definitionsgemäß, $G(\mathcal{S}) = Z_{\mathcal{S}}$. $(\mathcal{S}')^{\sigma}$ bezeichnet die Elemente in der Form A^{σ}, wo A die Elemente der Menge $\mathcal{S}'$ durchläuft.

Lemma 3. Die sämtliche konjugierte Untergruppen der Untergruppe $G(\mathcal{S}')$ vom Gruppe $\Pi(Z; \mathcal{S}; \Theta)$ kann in der Form $G((\mathcal{S}')^{\sigma})$ geschreiben werden.

Beweis. Da die Gruppe $G(\mathcal{S})$ kommutative ist, kann man die konjugierte Untergruppen einer Untergruppe H der Gruppe $G(\mathcal{S})$ in der Form $\sigma H\sigma^{-1}$ schreiben. Das Element f liegt in $\sigma G(\mathcal{S}')\sigma^{-1}$ dann und nur dann, wenn $\sigma^{-1}f\sigma$ in $G(\mathcal{S}')$ liegt. Das bedeutet aber, daß aus $A\notin\mathcal{S}'$ $(\sigma^{-1}f\sigma)(A) = 0$, und wegen der Definition des Permutationproduktes $f(A^{\sigma}) = 0$ folgt. Das ist gerade für die Elementen der Untergruppe $G((\mathcal{S}')^{\sigma})$ gültig.

Wir nennen eine teilweise geordnete Menge $\mathcal{S}$ *homogengeordnet*, wenn $M(\mathcal{S})$ eine transitive Untergruppe der Permutationsgruppe der Menge $\mathcal{S}$ ist. Es sei $\mathcal{S}(A)$ die Menge aller $X\in\mathcal{S}$ mit $X\leqq A$, wo $\mathcal{S}$ eine beliebige teilweise geordnete Menge ist.

Satz 3. *Wenn $\mathcal{S}$ eine homogen-geordnete Menge ist, so gilt:*

$$\Sigma(\Pi(Z; \mathcal{S}; M(\mathcal{S})); G(\mathcal{S}(A))) \cong \mathcal{S}.$$

Beweis. Da die Elemente der Gruppe $M(\mathcal{S})$ genau die monotone Permutationen sind, gilt $(\mathcal{S}(A))^{\sigma} = \mathcal{S}(A^{\sigma})$, für jedes $\sigma\in M(\mathcal{S})$. Nach Lemma 3. die sämtlichen konjugierten Untergruppen der Untergruppe $G(\mathcal{S}(A))$ sind die Untergruppen, die man in der Form $G(\mathcal{S}(A^{\sigma}))$ schreiben kann. Nach der Homogenität bringt die Abbildung $\Phi : B\to G(\mathcal{S}(B))$ die ganze Menge $\mathcal{S}$ in die Menge der konjugierten Untergruppen der Gruppe $G(\mathcal{S}(A))$ über. Jetzt werden wir die Untergruppe $G(\mathcal{S}(A))$ bestimmen.

$X\notin\mathcal{S}(A)$ bedeutet, daß $X\not\leqq A$ ist. Folglich gehört f dann und nur dann zur $G(\mathcal{S}(A))$, wenn aus $X\not\leqq A$ $f(X) = 0$ folgt.

Zu jedem Element A können wir ein f_A zuordnen, wie folgt:

$f_A(A) = 1$, $f_A(X) = 0$ falls $X\neq A$. (Offenbar ist $f_A\in G(\mathcal{S}(A))$.)

Nehmen wir an, daß $A\neq B$ ist. Daraus folgt, daß z. B. $A\not\leqq B$ gilt. Wegen $f_A(A)\neq 0$ ist $f_A(A)\notin G(\mathcal{S}(B))$, und so müssen $G(\mathcal{S}(A))$ und $G(\mathcal{S}(B))$ verschieden sein, was die Ein-eindeutigkeit der Abbildung Φ zeigt.

Ist $A \leqq B$, so folgt aus $X \leqq B$ offenbar $X \leqq A$, folglich gilt $G(\mathcal{S}(A)) \subseteq \subseteq G(\mathcal{S}(B))$. Wenn umgekehrt, $G(\mathcal{S}(A)) \subseteq G(\mathcal{S}(B))$ ist, dann gewinnen wir auch $f_A \in G(\mathcal{S}(B))$. Wegen $f_A(A) \neq 0$, ist $A \leqq B$ unmöglich. So ist Φ ein Isomorphismus, wie wir behauptet haben.

SATZ 4. *Die teilweise geordnete Menge $\mathcal{S}$ läßt sich dann und nur dann in der Form $\Sigma(G; H)$ darstellen, wenn sie eine homogen-geordnete Menge ist.*

BEWEIS. Nach Satz 3. ist die Homogenität hinreichend. Wegen $b^{-1}Hb = (a^{-1}b)^{-1}(a^{-1}Ha)(a^{-1}b)$ ist sie aber auch notwendig.

5. Die Darstellung einer angeordneten Menge

Die Darstellung, die im Satz 3. gegeben wurde ist eine vollständig inseparabele Darstellung, weil $N(G(\mathcal{S}(A)))$ – von A unabhängig – mit $G(\mathcal{S})$ übereinstimmt.

Wir werden uns mit zwei extremen Fällen der homogen-angeordneten Mengen beschäftigen. $M_A(\mathcal{S})$ bezeichnet die, zur dem Element $A(\in \mathcal{S})$ gehörende, Stabilitätsuntergruppe; d.h. $\sigma \in M_A(\mathcal{S})$ dann und nur dann, wenn $A^\sigma = A$ ist. Wir nennen die homogen-angeordnete Menge $\mathcal{S}$ *separabel* bzw. *vollständig inseparabel*, wenn keine $M_A(\mathcal{S})$ in einer anderen $M_B(\mathcal{S})$ enthaltend ist bzw. wenn jede $M_A(\mathcal{S})$ nur aus dem Einselement besteht.

SATZ 5. *Jede separabele, homogen-angeordnete Menge hat eine separabele Darstellung und jede vollständig inseparabele homogen-angeordnete Menge hat nur vollständig inseparabelen Darstellungen.*

BEWEIS. Es sei $\mathcal{S}$ eine separabele homogen-angeordnete Menge. Zu jedem $A \in \mathcal{S}$ ordnen wir eine Untergruppe $H_A(\mathcal{S})$ der Gruppe $M(\mathcal{S})$ zu. $\sigma \in H_A(\mathcal{S})$ gilt dann und nur dann, wenn aus $A \leq X$ $X^\sigma = X$ folgt. Es ist leicht zu sehen, daß der Zusammenhang $\sigma^{-1}H_A(\mathcal{S})\sigma = H_{A^\sigma}(\mathcal{S})$ gültig ist. Falls $A \leqq B$ gilt, so liegt die Untergruppe $H_A(\mathcal{S})$ offenbar in der Gruppe $H_B(\mathcal{S})$. Nehmen wir jetzt an daß, außer $A \leqq B$ noch A und B verschieden sind. Wegen der Separabilität existiert ein Element σ so, daß σ in $M_B(\mathcal{S})$ aber nicht in $M_A(\mathcal{S})$ liegt. Mit anderen Worten $B^\sigma = B$, aber $A^\sigma \neq A$. Wir definieren eine monotone Permutation ϱ folgenderweise:

$X^\varrho = X^\sigma$, wenn $X \leqq B$ und $X^\varrho = X$, wenn $B \leqq X$. Die Permutation ϱ ist offenbar in $H_B(\mathcal{S})$, aber nicht in $H_A(\mathcal{S})$; d.h. auch die Untergruppen $H_A(\mathcal{S})$ und $H_B(\mathcal{S})$ sind verschieden. So ist $\Sigma(M(\mathcal{S}); H_B(\mathcal{S})) \simeq \mathcal{S}$, was die erste Behauptung beweist.

Es sei jetzt $\mathcal{S} = \Sigma(G; H)$ eine vollständig inseparabele homogen-angeordnete Menge. Wenn das Element a zur $N = N(H)$ gehört, dann ist $Na = N$. Wegen der Voraussetzung muß σ_a mit der identischen Permutation gleich sein. Daher ist $Nxa = Nx$, für jedes $x \in G$, woraus $xax^{-1} \in N$ für jedes $x \in G$ folgt. So ist $N^* = N$, ferner $HN^* = N^*$. Das bedeutet aber, daß die Darstellung $\Sigma(G; H) = \mathcal{S}$ vollständig inseparabel ist.

Es gibt separabele homogen-angeordnete Menge, z. B. die angeordnete Menge der reellen Zahlen hat diese Eigenschaft, wie das das Beispiel II. zeigt. Wir werden zeigen, daß die angeordnete Menge der ganzen Zahlen vollständig

inseparabel ist. In der Tat, wenn σ eine monotone Permutation der ganzen Zahlen ist, dann aus $n^\sigma = n$ folgt sogar $(n-1)^\sigma = n-1$ auch $(n+1)^\sigma = n+1$.

SATZ 6. *Jede vollständige inseparabele homogene Menge ist der angeordnete Menge einer Untergruppe der additiven Gruppe der reellen Zahlen isomorph.*

BEWEIS. Es sei A ein Element der vollständigen inseparabelen homogenen Menge $\mathcal{S}$. Es sei ferner $B = A^\sigma = A^\varrho$, wo $\sigma, \varrho \in M(\mathcal{S})$. Folglich gilt $\sigma\varrho^{-1} \in M_A(\mathcal{S})$, und wegen der Voraussätzung erhalten wir $\sigma = \varrho$. Daher ist die angeordnete Menge der teilweisen geordneten Gruppe $M(\mathcal{S})$ mit $\mathcal{S}$ isomorph. Es sei $\sigma \in M(\mathcal{S})$, $A_0 = A$, $A_{n+1} = A_n^\sigma$ $(n = 0, 1, 2, \ldots)$. Die monotone Permutation ϱ sei, wie folgt definiert: $X^\varrho = X^\sigma$, wenn es ein n derart existiert, daß $X \leqq A_n$, sonst sei $X^\varrho = X$. Wegen der vollständigen Inseparabilität kann aber kein Element X mit $X^\varrho = X$ existieren. Man kann aus dies schon leicht ableiten, daß die Ordnung der Gruppe $M(\mathcal{S})$ archimedisch ist. Nun, die Behauptung folgt aus der Tatsache, daß jede archimedische angeordnete Gruppe mit einer Untergruppe der additiven Gruppe der reellen Zahlen isomorph ist.

Man kann zeigen, daß unter den abzählbaren Mengen nur die angeordnete Menge der ganzen Zahlen diese Eigenschaft besitzt. Es ist aber eine offene Frage, daß neben dieser Menge auch andere vollständig inseparabele Menge existiert oder nicht.

Bemerkung bei der Korrektur.

Bei der Korrektur wurde es mir bekannt, daß die Verallgemeinerung des Kranzproduktes die ich gab, wurde schon in der [3] Arbeit veröffentlicht.

Literatur

[1] L. FUCHS, *Teilweise geordnete algebraische Strukturen*, Akadémiai Kiadó, 1966, Budapest.
[2] L. RÉDEI, Die Anwendung des schiefen Produktes in der Gruppentheorie, *Journal für die reine und die angewandte Mathematik*, **188** (1950), 201–227.
[3] B. I. PLOTKIN, Verallgemeinierte auflösbare und verallgemeinierte nilpotente Gruppen, (Russisch), *Uspechi Mat. Nauk*, **13** (1958), 89–172.

A NOTE ON COMBINATORICS

By

K. A. CORRADI and I. KÁTAI

Department of Algebra and Number Theory of the Eötvös Loránd University, Budapest

(Received December 12, 1968)

In the present note we deal with finite sets. If A is such a set, we denote by $|A|$ the number of its elements. For subsets B and C in A we denote by B_0C the set of elements in A belonging to exactly one of the subsets B and C.

The aim of the present paper is to prove the following

THEOREM. *Let A be a finite set with $|A| = n$. Suppose that $A_1, \ldots, A_k$ is a system of subsets in A satisfying*

$$|A_{i0}A_j| \geq \frac{n}{2}$$

for any pair i, j with $i \neq j$. Then for k holds the inequality

$$k \leq \begin{cases} n+1, & \text{if } n \text{ is odd}, \\ n+2, & \text{if } n \equiv 2 \pmod 4, \\ 2n, & \text{if } n \equiv 0 \pmod 4. \end{cases} \tag{1}$$

The inequality (1) is a best possible inequality in all three cases for an infinity of the values of n.

We need the following

LEMMA 1. Let n and r be natural numbers with $n \geq 2$, $1 \leq r \leq n$. Let $\mathbf{a}_1, \ldots, \mathbf{a}_{n+r}$ be a system of n-dimensional vectors satisfying

$$(\mathbf{a}_i, \mathbf{a}_j) \leq 0 \tag{2}$$

for any pair i, j with $i \neq j$. Then the vectors of the system mentioned, may be subdivided into r distinct sets $U_1, \ldots, U_r$ so that for $\mathbf{b} \in U_l$ and $\mathbf{c} \in U_m$

$$(\mathbf{b}, \mathbf{c}) = 0 \tag{3}$$

holds, provided that $l \neq m$.

REMARK. In the case $r = 2$ the statement of this lemma may be found in [1].

PROOF OF LEMMA 1. We use induction for n. The case $n = 2$ is obvious. Suppose $n > 2$ and the statement of the lemma for natural numbers smaller than n. We may suppose that $\mathbf{a}_i \neq \mathbf{o}$ ($\mathbf{o}$ the zero vector) holds for $1 \leq i \leq n+r$. Suppose that $\mathbf{a}_1, \ldots, \mathbf{a}_u$ is a maximal system of independent vectors in the system $\mathbf{a}_i$, $1 \leq i \leq n+r$. Then

$$\mathbf{a}_v = \sum_{1 \leq j \leq u} \lambda_j^{(v)} \mathbf{a}_j \qquad u+1 \leq v \leq n+r \tag{4}$$

holds. We begin by proving that for any v the numbers $\lambda_j^{(v)}$ in the representation (4) are non-positive. Suppose the contrary. Then by (2) we have

$$0 \geq \left(\sum_{\substack{1 \leq j \leq u \\ \lambda_j^{(v)} > 0}} \lambda_j^{(v)} \mathbf{a}_j, \mathbf{a}_v \right) = \left(\sum_{\substack{1 \leq j \leq u \\ \lambda_j^{(v)} > 0}} \lambda_j^{(v)} \mathbf{a}_j, \sum_{\substack{1 \leq j \leq u \\ \lambda_j^{(v)} > 0}} \lambda_j^{(v)} \mathbf{a}_j \right) + \tag{5}$$

$$+ \left(\sum_{\substack{1 \leq j \leq u \\ \lambda_j^{(v)} > 0}} \lambda_j^{(v)} \mathbf{a}_j, \sum_{\substack{1 \leq j \leq u \\ \lambda_j^{(v)} \leq 0}} \lambda_j^{(v)} \mathbf{a}_j \right) \geq 0$$

Use (4) and note that both summands on the right-hand side of (5) are non-negative. (5) holds only, if in (5) the sign of equality holds. From this

$$\sum_{\substack{1 \leq j \leq u \\ \lambda_j^{(v)} > 0}} \lambda_j^{(v)} \mathbf{a}_j = \mathbf{o} \tag{6}$$

follows. (6) contradicts to the independence of the system $\mathbf{a}_1, \ldots, \mathbf{a}_u$. The contradiction proves the non-positivity of the $\lambda_j^{(v)} - s$.

Next we show, that for any pair $u+1 \leq v$, $w \leq n+r$ with $w \neq v$, $(\mathbf{a}_v, \mathbf{a}_w) = 0$ holds. Using (2) and the non-positivity of the $\lambda_j^{(v)} - s$

$$0 \geq (\mathbf{a}_v, \mathbf{a}_w) = \sum_{1 \leq j \leq u} \lambda_j^{(v)} (\mathbf{a}_j, \mathbf{a}_w) \geq 0 \tag{7}$$

follows. This proves our assertion.

We observe now that an arbitrary ortogonal system of n-dimensional vectors is independent. By this remark we deduce the inequality $u \geq \frac{n+r}{2}$.

After these preliminaries we deal first with the case in which $n+r$ is even, and by suitable choosing of notation for the vectors of our system the relations

$$\mathbf{a}_{\frac{n+r}{2}+\nu} = \lambda_\nu \mathbf{a}_\nu, \qquad 1 \leq \nu \leq \frac{n+r}{2} \tag{8}$$

hold.

Using the remarks done before, $u = \frac{n+r}{2}$ follows. Further as an easy consideration shows we can construct the sets U_l, $1 \leq l \leq r$ of the lemma by defining

$$U_l \overset{\text{def}}{=} \begin{cases} \{\mathbf{a}_l,\ \mathbf{a}_{\frac{n+r}{2}+l}\}, & \text{if } 1 \le l \le r-1 \\ \bigcup_{t=r}^{\frac{n+r}{2}} \{\mathbf{a}_t,\ \mathbf{a}_{\frac{n+r}{2}+t}\}, & \text{if } l = r. \end{cases} \tag{9}$$

Here $\{\mathbf{a}_l, \mathbf{a}_{\frac{n+r}{2}+l}\}$ denotes the set consisting of the two vectors $\mathbf{a}_l$ and $\mathbf{a}_{\frac{n+r}{2}+l}$.

We treat next with the case $r = n$. In this case we have $u = n$. The vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$ form a maximal system of independent vectors and

$$(\mathbf{a}_v, \mathbf{a}_w) = 0 \tag{10}$$

holds for any pair $n+1 \le v$, $w \le 2n$, $w \ne v$. (10) means that $\mathbf{a}_{n+1}, \ldots, \mathbf{a}_{2n}$ is also a maximal-system of independent vectors in our original system. So by symmetry we deduce, that

$$(\mathbf{a}_v, \mathbf{a}_w) = 0 \tag{11}$$

holds for any pair $1 \le v$, $w \le n$, $w \ne v$. Now using the representation (4), and (11)

$$0 = (\mathbf{a}_v, \mathbf{a}_w) = \sum_{1 \le j \le n} \lambda_j^{(v)} \lambda_j^{(w)} (\mathbf{a}_j, \mathbf{a}_j) \tag{12}$$

holds for any pair $n+1 \le v$, $w \le 2n$, with $w \ne n$. By (12) we deduce that $\lambda_j^{(v)} \cdot \lambda_j^{(w)} = 0$ hold simultaneously for $1 \le j \le n$. From this follows that by a suitable choice of the notation we have

$$\mathbf{a}_{n+v} = \mu_v \mathbf{a}_v, \qquad 1 \le v \le n. \tag{13}$$

Now we can construct the sets U_l, $1 \le l \le n$ by putting

$$U_l \overset{\text{def}}{=} \{\mathbf{a}_l, \mathbf{a}_{n+l}\}, \qquad 1 \le l \le n.$$

In the sequel we may suppose that $r \le n-1$ holds, and by a suitable choosing of the notation if necessary we can assume that

$$\mathbf{a}_i \ne \lambda_i \mathbf{a}_{n+r} \tag{14}$$

holds for all values of i with $1 \le i \le n+r-1$. Define the vectors $\mathbf{b}_i$ and $\mathbf{c}_i$ by

$$\mathbf{a}_i = \mathbf{b}_i + \mathbf{c}_i, \quad (\mathbf{b}_i, \mathbf{a}_{n+r}) = 0, \quad \mathbf{c}_i = \lambda_i \mathbf{a}_{n+r} \tag{15}$$

for $1 \le i \le n+r-1$. Here the numbers λ_i are uniquely determined. By (2) using

$$0 \ge (\mathbf{a}_i, \mathbf{a}_{n+r}) = \lambda_i (\mathbf{a}_{n+r}, \mathbf{a}_{n+r}) \tag{16}$$

follows for $1 \le i \le n+r-1$. This means, that $\lambda_i \le 0$ holds. By this we deduce that

$$(\mathbf{c}_i, \mathbf{c}_j) = \lambda_i \lambda_j (\mathbf{a}_{n+r}, \mathbf{a}_{n+r}) \ge 0 \tag{17}$$

holds for any pair $1 \le i, j \le n+r-1$ with $j \ne i$. By (17) using (2) and (15) we have

$$0 \ge (\mathbf{a}_i, \mathbf{a}_j) = (\mathbf{b}_i, \mathbf{b}_j) + (\mathbf{c}_i, \mathbf{c}_j) \tag{18}$$

and so $(\mathbf{b}_i, \mathbf{b}_j) \le 0$ for the pairs in our consideration.

Now the vectors $\mathbf{b}_i$, $1 \le i \le n+r-1$ $(= 2(n-1))$ — which can be considered as $(n-1)$-dimensional vectors satisfy the requirements of our lemma. So by the hypothesis we can construct the sets U_i^*, $1 \le i \le r$ so that for vectors belonging to different sets the relation (3) holds. So if $l \ne m$ and $\mathbf{b}_l \in U_l^*$, $\mathbf{b}_m \in U_m^*$ hold we have $(\mathbf{b}_l, \mathbf{b}_m) = 0$. By this we deduce using (17) and (18) that for this pair l, m $(\mathbf{a}_l, \mathbf{a}_m) = 0$ holds. By (14) $\mathbf{b}_i \ne \mathbf{o}$ holds for $1 \le i \le n+r-1$. This means that

$$(\mathbf{a}_l, \mathbf{a}_m) = \lambda_l \lambda_m (\mathbf{a}_{n+r}, \mathbf{a}_{n+r}) = 0 \tag{19}$$

(19) holds in the case $\lambda_l \lambda_m = 0$ only. Suppose that $\lambda_l = 0$ holds.

Now we have to distinguish two cases. In the first one we suppose that there is an m with $\lambda_m \ne 0$. Then by (19) it follows, that for any $l \ne m$ and for any $\mathbf{b}_l \in U_l^*$ $\lambda_l = 0$ holds.

So in this case the construction of the sets U_i can run as follows. Define

$$U_t \overset{\text{def}}{=} \begin{cases} U_t^*, & \text{if } 1 \le t \le r,\ t \ne l \\ \{U_t^*, \mathbf{a}_{n+r}\} & \text{if } t = l. \end{cases} \tag{20}$$

By (20) we mean that in the case $t \ne l$ $\mathbf{a}_u \in U_t$ holds if and only if $\mathbf{b}_u \in U_t^*$ holds. In the case $t = l$ $\mathbf{a}_u \in U_t$ holds if $\mathbf{b}_u \in U_t^*$ holds, or if $u = n+r$.

The sets constructed above, fulfil the requirements of the lemma.

In the remaining case $\lambda_l = 0$ holds for $1 \le l \le n+r-1$. In this case the construction of the sets U_i is similar, but we can put $\mathbf{a}_{n+r}$ in an arbitrary of them. This proves the lemma.

Definition. Let $\mathbf{a}$ be an n-dimensional vector, $\mathbf{a} = (a_1, \ldots, a_n)$. If for all k, $1 \le k \le n$ $a_k = \pm 1$ holds we denote $\mathbf{a}$ as an e-vector.

Lemma 2. Suppose that $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c}$ are n-dimensional e-vectors. If

$$(\mathbf{a}, \mathbf{b}) = (\mathbf{a}, \mathbf{c}) = (\mathbf{b}, \mathbf{c}) = 0$$

holds, then $4 \mid n$ follows.

This lemma represents a well-known result of Paley. See [2].

Proof of the Theorem. Let the meaning of A, $A_1, \ldots, A_k$ be the same as in Theorem. Suppose that $|A| = n$, and the assumption of Theorem. Let $a_1, a_2, \ldots, a_n$ be the elements of A. Let B be any subset of A. For B define the vector $\mathbf{b} = (b_1, \ldots, b_n)$ as follows. For all m with $1 \le m \le n$ let

$$b_m \overset{\text{def}}{=} \begin{cases} 1, & \text{if } a_m \in B, \\ -1, & \text{if } a_m \notin B. \end{cases}$$

Denote the vectors corresponding to the subsets $A_1, \ldots, A_k$ by $\mathbf{a}_1, \ldots, \mathbf{a}_k$, respectively. Then by the assumption

$$(\mathbf{a}_i, \mathbf{a}_j) = 0, \quad 1 \le i, j \le k,\ j \ne i \tag{21}$$

holds.

To prove (1) suppose first that n is odd. If the assertion of the theorem would not be true, so $k \ge n+2$ would follow. Take the first $n+2$ vectors from the vec-

tors $\mathbf{a}_1, \ldots, \mathbf{a}_k$. These are $\mathbf{a}_1, \ldots, \mathbf{a}_{n+2}$. By (21) for these vectors Lemma 1 would apply. From this fact the existence of vectors $\mathbf{a}_i, \mathbf{a}_j$, $i \neq j$, $1 \leq i, j \leq n+2$ would follow with

$$(\mathbf{a}_i, \mathbf{a}_j) = 0. \tag{22}$$

Take now into account that $\mathbf{a}_i$ and $\mathbf{a}_j$ are e-vectors. By this, using that n is odd

$$(\mathbf{a}_i, \mathbf{a}_j) \equiv 1 \pmod 2 \tag{23}$$

follows. (22) and (23) give a contradiction. So the statement of the Theorem holds in the case if n is odd.

Suppose next, that $n \equiv 2 \pmod 4$ holds. If (1) would not be true in this case, so $k \geq n+3$ would follow. Take the first $n+3$ vectors $\mathbf{a}_1, \ldots, \mathbf{a}_{n+3}$. By (21) for this system Lemma 1 would apply with $r = 3$. So by this lemma the existence of e-vectors $\mathbf{a} = \mathbf{a}_u$, $\mathbf{b} = \mathbf{a}_v$ and $\mathbf{c} = \mathbf{a}_w$ would follow with

$$(\mathbf{a}, \mathbf{b}) = (\mathbf{a}, \mathbf{c}) = (\mathbf{b}, \mathbf{c}) = 0.$$

This is impossible by Lemma 2. So the statement of the Theorem holds in the case $n \equiv 2 \pmod 4$ too.

In the remaining case $n \equiv 0 \pmod 4$ we work as follows. If $k \geq 2n+1$ would be true, so take the first $2n+1$ vectors $\mathbf{a}_1, \ldots, \mathbf{a}_{2n+1}$. From these for the first $2n$ by (21) Lemma 1 would apply with $r = n$. So in this case by (12) and (13) by a suitable choice of the notation

$$\mathbf{a}_{n+u} = \lambda_u \mathbf{a}_u, \quad 1 \leq u \leq n \tag{24}$$

and

$$(\mathbf{a}_u, \mathbf{a}_v) = 0, \quad 1 \leq u, v \leq n, \ v \neq u \tag{25}$$

would follow with $\lambda_u \neq 0$, $1 \leq u \leq n$. Now by (21) $(\mathbf{a}_u, \mathbf{a}_{2n+1}) \leq 0$ and $(\mathbf{a}_{n+u}, \mathbf{a}_{2n+1}) \leq 0$ would follow for any u with $1 \leq u \leq n$.

So by $\lambda_u \neq 0$ $(\mathbf{a}_{2n+1}, \mathbf{a}_u) = 0$ would follow for any u with $1 \leq u \leq n$. By (25) now the $n+1$ e-vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$ and $\mathbf{a}_{2n+1}$ would form an orthogonal-system. This contradiction proves the theorem in the case $n \equiv 0 \pmod 4$.

It remains to show, that the inequality is best possible for an infinity of the values n. Let $n = 4m$. If for a value of m there is a system of e-vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$ with

$$(\mathbf{a}_i, \mathbf{a}_j) = 0, \quad 1 \leq i, \ j \leq n, \quad j \neq i$$

so by inverting of the definition (20) the sets $A_1, \ldots, A_n$ belonging to the vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$ respectively can be constructed. To these sets construct the sets $A_{n+1}, \ldots, A_{2n}$ by the definition

$$A_{n+m} \overset{\text{def}}{=} A_0 A_m, \quad 1 \leq m \leq n$$

where A denote the original set, also $A_m \subseteq A$ holds. So the example of the sets $A_1, \ldots, A_n, A_{n+1}, \ldots, A_{2n}$ shows that the inequality (1) can not be improved in the case $n \equiv 0 \pmod 4$, if the system of the e-vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$ exists. It is

known that in the case $m = 2^l$ the system exists for every choice of the natural number l.

It is worth-wile to mention, that (1) can-not be improved in the case $n \equiv 1$ (mod 2) in generally. Put $n \equiv 3$ (mod 4). Then $n+1 = 4m$ holds. If the system of the e-vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n, \mathbf{a}_{n+1}$ treated before exists, then in the notation

$$\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in}), \quad 1 \leq i \leq n+1$$

substituting $\mathbf{a}_i$ by $-\mathbf{a}_i$ if necessary, we may suppose that for the vectors $\mathbf{a}_1, \ldots$ $\ldots, \mathbf{a}_{n+1}$ both

$$(\mathbf{a}_i, \mathbf{a}_j) = 0, \quad 1 \leq i, \quad j \leq n+1, \quad j \neq i$$

and $a_{i1} = 1$, $1 \leq i \leq n+1$ holds. But taking $\mathbf{a}'_i$ instead of $\mathbf{a}_i$, where $\mathbf{a}'_i$ is defined by

$$\mathbf{a}'_i = (a_{i2}, \ldots, a_{in+1}), \quad 1 \leq i \leq n+1$$

the system $\mathbf{a}'_1, \ldots, \mathbf{a}'_{n+1}$ of n-dimensional e-vectors satisfies the relations

$$(\mathbf{a}'_i, \mathbf{a}'_j) = -1 < 0, \quad 1 \leq i, \quad j \leq n+1, \quad j \neq i,$$

and so by (20) the construction of the previous case can be repeated.

This completes the proof in the case $n \equiv 3$ (mod 4).

For the case $n \equiv 2$ (mod 4) the construction can be repeated taking the system $\mathbf{a}_1, \ldots, \mathbf{a}_{n+2}$ of $(n+2)$-dimensional vectors with

$$(\mathbf{a}_i, \mathbf{a}_j) = 0 \quad 1 \leq i, \quad j \leq n+2, \quad j \neq i,$$

and in the notation

$$\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in+2})$$

with the normalisation $a_{i1} = 1$, $1 \leq i \leq n+2$ and putting $\mathbf{a}''_i$ for

$$\mathbf{a}''_i \overset{\text{def}}{=} (a_{i3}, \ldots, a_{in+2}), \quad 1 \leq i \leq n+2.$$

So for the system $\mathbf{a}''_1, \mathbf{a}''_2, \ldots, \mathbf{a}''_{n+2}$ of n-dimensional e-vectors for any pair i, j with $1 \leq i, j \leq n+2$, $j \neq i$

$$(\mathbf{a}''_i, \mathbf{a}''_j) \leq 0$$

holds. So the construction by (20) used in the previous two cases can be repeated.

So our Theorem is proved.

References

[1] G. Hajós, *Mat. Lapok* 5 (1954) Problem 50. 144–147.
[2] R. E. A. C. Paley, On orthogonal matrices. *J. Math. and Phys.*, (1933), 311–320.

ОБОБЩЕНИЕ ОДНОГО НЕРАВЕНСТВА ЛЯПУНОВА

ДЛЯ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ С ЗАПАЗДЫВАЮЩИМ АРГУМЕНТОМ

А. ЭЛЬБЕРТ

Математический Институт Академии Наук Венгрии, Будапешт

(Поступило 23. 12. 1968.)

Если решение обыкновенного дифференциального уравнения второго порядка

$$y''(t)+p(t)y(t)=0$$

имеет последовательные нули a и b (т.е. $y(a)=y(b)=0$), то имеет место неравенство Ляпунова при некоторых свойствах функции $p(t)$

$$(b-a)\int_a^b p_+(t)dt>4,$$

где $p_+(t)=(p(t)+|p(t)|)/2$.

В этой работе рассматривается дифференциальное уравнение второго порядка с запаздывающим аргументом

$$y''(t)+p(t)y(q(t))=0, \tag{1}$$

где $q(t)\leqq t$ и будет доказана следующая

ТЕОРЕМА. *Если*

а) *в уравнении* (1) $q(t)$ *непрерывная возрастающая функция от* t, *её обратная функция* $q^*(t)$, *и* $p(t)\geqq 0$,

б) *решение* $y(t)$ *уравнения* (1) *при* $t=a$ *удовлетворяет условиям* $y(a)=0$, $y'(a)>0$,

в) *в случае* $q(a)<a$ *начальная функция* $\varphi(t)$ *неположительна на отрезке* $(q(a), a)$ *и имеет место неравенство*

$$-\int_a^{a^*} p(t)\varphi(q(t))dt<\infty, \tag{2}$$

где $a^*=q^*(a)$,

г) *существует* b, *для которого* $y(t) > 0$ *на отрезке* (a, b) *и* $y(b) = 0$, *то*

$$(3)\qquad (b-a)\int_a^b p(t)\,dt \le \frac{(b-a)^2}{\max\limits_{a^*(a)\le s\le b}(b-s)\,(q(s)-a)}.$$

Доказательство. 1. Пусть имеет место неравенство $q(a) > a$. Решение $y(t)$ уравнения (1) в условиях теоремы имеет первое производное неубывающее [т.е. оно вогнутое] для всех t, которые удовлетворяют неравенству $q(t) \ge a$. Мы покажем, что $q(b) > a$.

Действительно, если $q(b) \le a$, то $q(t) \le a$ для всякого значения $t \in [a, b]$ и решение $y(t)$ вогнутое, возрастающее и, следовательно, нигде не обращается в нуль, что противоречит условию $y(b) = 0$. Таким образом, $q(b) > a$, или $a^* = q^*(a) < b$. Таким образом, решение $y(t)$ вогнутое на отрезке $[a, a^*]$, и его можно представить в виде

$$(4)\qquad y(t) = \int_a^{a^*} y_\mu(t)\,dF(\mu) \qquad a \le t \le a^*,$$

где

$$(5)\qquad y_\mu(t) = \begin{cases} 0 & a \le t \le \mu, \\ \dfrac{t-\mu}{a^*-\mu} & \mu \le t \le a^*, \quad a \le \mu < a^*, \end{cases}$$

и

$$F(s) = \begin{cases} 0 & s < a \\ y'(a)\,(a^*-a) - \displaystyle\int_a^s (a^*-r)p(r)q\,(q(r))\,dr & a \le s \le a^* \\ F(a^*) & a > a^*. \end{cases}$$

Функция $F(s)$ неубывающая функция и в силу (2) ограниченная, поэтому существует интеграл (4) в смысле Стильтьеса – Лебега.

Решение $y(t)$ уравнения (1) удовлетворяет интегральному уравнению

$$(6)\qquad y(t) = y(a^*) + y'(a^*)\,(t-a^*) - \int_{a^*}^t (t-s)p(s)y(q(s))\,ds, \qquad a^* \le t \le b.$$

Из (2) следует конечность величины $y'(a^*)$. Пусть $y_\mu(t)$ решение интегрального уравнения

$$(7)\qquad y_\mu(t) = 1 + \frac{t-a^*}{a^*-\mu} - \int_{a^*}^t (t-s)p(s)y_\mu(q(s))\,ds, \qquad a^* \le t \le b,$$

а для $t \in [a, a^*]$ функция $y_\mu(t)$ определяется соотношением (5). В силу (4), (6) и (7)

$$y(t) = \int_a^{a^*} y_\mu(t)\,dF(\mu) \qquad a \le t \le b.$$

Но $y(b) = 0$ и $d\Gamma(\mu) \geqq 0$, поэтому существует $\mu_0 \in [a, a^*)$, для которого $y_{\mu_0}(b) \leqq 0$. Обозначим первый нуль уравнения $y_{\mu_0}(t) = 0$, $(t > a^*)$ через c. Тогда

$$y_{\mu_0}(t) > 0 \qquad \mu_0 < t < c \leqq b.$$

Функция $p(t)$ не может тождественно обращаться в нуль почти всюду на отрезке $[q^*(\mu_0), c]$, потому что в этом случае было бы и $y_{\mu_0}(c) = 1 + (c - a^*)/(a^* - \mu_0) \geqq 0$, поэтому выполняется неравенство $p(t) > 0$ на множестве положительной меры из $[q^*(\mu_0), c]$. Таким образом, из (7) следует $y_{\mu_0}(t) \leqq (t - \mu_0)/(a^* - \mu_0)$ для $t \in [\mu_0, c]$, но $y_{\mu_0}(\tilde{t}) < (\tilde{t} - \mu_0)/(a^* - \mu_0)$, если $p(t) > 0$ на множестве положительной меры из $[q^*(\mu_0), \tilde{t}]$. Используя эти неравенства, из (7) получим

$$0 = y_{\mu_0}(c) = \frac{c - \mu_0}{a^* - \mu_0} - \int_{a^*}^{c} (c - s) p(s) y_{\mu_0}(q(s))\, ds = \frac{c - \mu_0}{a^* - \mu_0} - \int_{q^*(\mu_0)}^{c} (c - s) p(s) y_{\mu_0}(q(s))\, ds >$$

$$> \frac{c - \mu_0}{a^* - \mu_0} - \int_{q^*(\mu_0)}^{c} (c - s) p(s) \frac{q(s) - \mu_0}{a^* - \mu_0}\, ds \geqq$$

$$\geqq \frac{c - \mu_0}{a^* - \mu_0} - \frac{1}{a^* - \mu_0} \cdot \max_{q^*(\mu_0) \leqq s \leqq c} (c - s)\,[q(s) - \mu_0] \cdot \int_{q^*(\mu_0)}^{c} p(s)\, ds,$$

или

$$\int_{q^*(\mu_0)}^{c} p(s)\, ds > \frac{c - \mu_0}{\max\limits_{q^*(\mu_0) \leqq s \leqq c} (c - s)[q(s) - \mu_0]} \geqq \frac{b - \mu_0}{\max\limits_{q^*(\mu_0) \leqq s \leqq b} (b - s)[q(s) - \mu_0]} \geqq$$

$$\geqq \frac{b - a}{\max\limits_{a^* \leqq s \leqq b} (b - s)\,[q(s) - a]},$$

потому что $a \leqq \mu_0 < a^* < c \leqq b$. Следовательно,

$$(b - a) \int_{a}^{b} p(s)\, ds \geqq (b - a) \int_{q^*(\mu_0)}^{c} p(s)\, ds > \frac{(b - a)^2}{\max\limits_{a^* \leqq s \leqq b} (b - s)\,(q(s) - a)},$$

и для рассматриваемого случая утверждение теоремы доказано.

2. Если $q(a) = a$, тогда $q^*(a) = a$. Заменяя уравнение (1) интегральным уравнением

$$y(t) = y'(a)\,(t - a) - \int_{a}^{t} (t - s) p(s) y(q(s))\, ds \qquad t \geqq a$$

и имея в виду, что $t > a$ и $p(s) > 0$ на множестве положительной меры из $[a, b]$ для всех t, достаточно близких к b, получим

$$y(t) < y'(a)\,(t - a).$$

Отсюда

$$0 = y(b) = y'(a)(b-a) - \int_a^b (b-s)p(s)y(q(s))\,ds > y'(a)(b-a) -$$

$$- \int_a^b (b-s)p(s)y'(a)(q(s)-a)\,ds \geqq y'(a)(b-a) - y'(a) \max_{a \leqq s \leqq b} (b-s)(q(s)-a) \cdot \int_a^b p(s)\,ds,$$

или

$$(b-a) \int_a^b p(s)\,ds > \frac{(b-a)^2}{\max\limits_{a \leqq s \leqq b} (b-s)(q(s)-a)}.$$

Теорема доказана полностью.

ПРИМЕРЫ.

1. $q(t) = qt$, $t > 0$, $0 < q < 1$, тогда $a^* = a/q$ и

$$\max_{a/q \leqq s \leqq b} (b-s)(qs-a) = \frac{q}{4}\left(b - \frac{a}{q}\right)^2.$$

Отсюда

$$(b-a) \int_a^b p(t)\,dt > \frac{4}{q}\left(\frac{b-a}{b-\frac{a}{q}}\right)^2 > \frac{4}{q}.$$

2. $q(t) = t - \tau$, где $\tau > 0$ постоянная. Тогда $a^* = a + \tau$ и $\max\limits_{a+\tau \leqq s \leqq b} (b-s)(s-\tau-a) = (b-a-\tau)^2/4$. Следовательно,

$$(b-a) \int_a^b p(t)\,dt > 4\left(\frac{b-a}{b-a-\tau}\right)^2 > 4.$$

3. $q(t) = \ln t$ $(t \geqq 0)$. Тогда

$$(b-a) \int_a^b p(t)\,dt > 4e.$$

СЛЕДСТВИЕ. Если решение уравнения (1) имеет $n+1$ последовательных нулей $a_0 < a_1 < \ldots < a_n$, выполняются условия теоремы с $a = a_0$ и

$$\min_{a_0 \leqq a \leqq q^*(a) < b \leqq a_n} \frac{(b-a)^2}{\max\limits_{q^*(a) \leqq s \leqq b} (b-s)(q(s)-a)} \geqq Q,$$

где Q постоянная, независящая от a_0, a_n, то

$$(a_n - a_0) \int_{a_0}^{a_n} p(t)\,dt > Q n^2.$$

ЗАМЕЧАНИЕ. В наших примерах Q соответственно равнялась $4/q$, 4, $4e$. Можно доказать, что всегда $Q \geqq 4$. Действительно, из $q(t) \leqq t$ следует

$$\max_{q^*(a) \leqq s \leqq b} (b-s)\,(q(s)-a) \leqq \max_{q^*(a) \leqq s \leqq b} (b-s)\,(s-a) \leqq (b-a)^2/4,$$

и поэтому

$$\min_{a_0 \leqq a \leqq q^*(a) < b \leqq a_n} \frac{(b-a)^2}{\max\limits_{q^*(a) \leqq s \leqq b} (b-s)\,(q(s)-a)} \geqq 4.$$

ДОКАЗАТЕЛСТВО.

Из теоремы следует

$$(a_1-a_0) \int_{a_0}^{a_1} p(t)\,dt > \frac{(a_1-a_0)^2}{\max\limits_{q^*(a_0) \leqq s \leqq a_1} (a_1-s)\,(q(s)-a_0)} \geqq Q.$$

Но из доказательства теоремы следует и неравенство $q^*(b) > a$, т.е. $y(t) > 0$ на отрезке $(q^*(b), b)$, решение $y(t)$ — выпуклая функция на этом отрезке, поэтому $y'(b) < 0$. Используя теорему на отрезках $[a_1, a_2], \ldots [a_{n-1}, a_n]$, получим

$$(a_2-a_1) \int_{a_1}^{a_2} p(t)\,dt > Q,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(a_n-a_{n-1}) \int_{a_{n-1}}^{a_n} p(t)\,dt > Q.$$

Таким образом,

$$(a_n-a_0) \int_{a_0}^{a_n} p(t)\,dt > (a_n-a_0) \left[\frac{1}{a_1-a_0} + \frac{1}{a_2-a_1} + \ldots + \frac{1}{a_n-a_{n-1}} \right] Q \geqq Qn^2,$$

что и требовалось доказать.

ON THE SOLVABILITY OF FINITE GROUPS

By

K. A. CORRADI

Department of Algebra and Number Theory of the Eötvös Loránd University, Budapest

(Received September 19, 1968)

Introduction, notations

Let G be a finite group. Denote by $|G|$ its order. Suppose that $|G|$ has the prime representation

$$|G| = p_1 \dots p_r, \tag{1}$$

where the p_i, $1 \leq i \leq r$ stand for primes not necessarily different from each-other.

We are interested to find a necessary and sufficient condition for the existence of a composition-series

$$G = G_0 \supset G_1 \supset \dots \supset G_{r-1} \supset G_r = \langle \varepsilon \rangle \tag{2}$$

satisfying

$$|G_{i-1}/G_i| = p_i, \qquad 1 \leq i \leq r, \tag{3}$$

supposing that the sequence $p_1, \dots, p_r$ decreases, or increases monotonically, respectively.

To the formulation of our result we need the concept of the one-step non-nilpotent groups. By such a group following L. Rédei [1] we mean a non-nilpotent group whose proper subgroups are all nilpotent.

The structure of the one-step non-nilpotent groups is now perfectly known. The complete result is due to L. Rédei [1]. However for our present purposes the following earlier and weaker result of O. Schmidt [2] and Ju. Golfand [3] is sufficient. We state it as

Lemma 1. Let G be a finite one-step non-nilpotent group. Then G is solvable, further

$$|G| = p^u q^v, \qquad u \geq 1, \ v \geq 1,$$

holds, where p and $q \neq p$ stand for primes. By suitable choice of the notation the commutator group G' of G is the p-Sylow-group of G. The q-Sylow-groups in G are cyclic. If m is the least natural number with

$$p^m \equiv 1 \pmod{q}, \tag{4}$$

then

$$|G'/G''| = p^m$$

holds. Further for G''' one obtains $G''' = \langle \varepsilon \rangle$. $G'' = \langle \varepsilon \rangle$ is fulfilled if and only if G is one-step non-abelian. G'' lies in the centre of G. G'' and G'/G'' are elementary abelian p-groups. The group G/G'' is a one-step non-abelian group.

We need the following

Definition 1. Let U be an arbitrary fixed one-step non-nilpotent group. We shall say that U is an $S^{*}_{p,q}$-group, or an $S^{**}_{p,q}$-group according to that in the notations of Lemma 1 $p<q$ or $p>q$ holds. By $S^{*} \not\subseteq G$ we mean that G does not contain an $S^{*}_{p,q}$-group for any choice of p and q. The meaning of $S^{**} \not\subseteq G$ is similar but in this case we use the $S^{**}_{p,q}$-groups instead of the $S^{*}_{p,q}$-groups.

It is useful to state the

Definition 2. The group G possesses the property ($\square$) if there is a composition-series (2) with (3) in G, where in (1) the sequence $p_1, \ldots, p_r$ decreases monotonically. G possesses the property ($\bigcirc$), if under the same circumstances the sequence $p_1, \ldots, p_r$ increases monotonically.

We are now in a position to formulate the following

Theorem. *Let G be a finite group. G possess the property ($\square$) if and only, if $S^{**} \not\subseteq G$ holds. The group G possesses the property ($\bigcirc$) if and only, if $S^{*} \not\subseteq G$ holds.*

The proof of the two statements in the Theorem runs on similar lines. So we prove the second one only.

Notations. G is the group we investigate. For the elements of G we use small Greek letters. For subgroups in G we use Latin capitels. By $H \leq G$ we mean that H is a subgroup of G. The notation $H < G$ stands for proper subgroups of G. For normal subgroups H we use the notation $H \lhd G$. If H is a subgroup in G, the notations $N(H)$, $C(H)$ and $Z(H)$ will be reserved for the normalizer, for the centralizer and for the centre of H, respectively. The subgroups $N(H; K)$ and $C(H; K)$ are defined for subgroups H and K in G by

$$N(H; K) \overset{\text{def}}{=} K \cap N(H), \qquad C(H; K) \overset{\text{def}}{=} K \cap C(H).$$

ε denotes the identity element of G. For a natural number k and for a subgroup H in G we denote by $\mathfrak{A}(k; H)$ the number of elements α in H satisfying

$$\alpha^k = \varepsilon.$$

If $\alpha_1, \ldots, \alpha_l$ are given elements, and $H_1, \ldots, H_m$ given subgroups in G, then

$$\langle \alpha_1, \ldots, \alpha_l; H_1, \ldots, H_m \rangle$$

denotes the group generated by these elements and subsgroups. The notations $|H|$ and $|\alpha|$ will be used for the order of the subgroup H and for the order of the element α, respectively.

The condition is necessary

We need the following simple

LEMMA 2. Let G be a finite group. Suppose that G possesses the property $(\bigcirc)$. Then the same is true for any subgroup H in G.

PROOF. By the assumption G possesses a composition-series (2) with (3), where in (1) the sequence $p_1, \ldots, p_r$ increases monotonically. Define for a given subgroup H in G the subgroups H'_i, $0 \leq i \leq r$, by

$$H'_i = H \cap G_i .$$

Then

$$H = H'_0 \geq H'_1 \geq \ldots \geq H'_{r-1} \geq H'_r = \langle \varepsilon \rangle$$

is a composition-series in H. By the Lemma of ZASSENHAUS (see [4] p. 47.) one has

$$H'_{i-1}/H'_i \cong G_i H'_{i-1}/G_i .$$

By this, using $G_{i-1} \geq G_i H'_{i-1} \geq G_i$ it can be easily deduced that

$$|H'_{i-1}/H'_i| = \begin{cases} 1, \text{ or} \\ p_i, \qquad 1 \leq i \leq r, \end{cases}$$

holds. The statement of Lemma 2 now follows by mentioning that the sequence $p_1, \ldots, p_r$ increases monotonically, and deleting from the sequence $H'_0, H'_1, \ldots, H'_{r-1}, H'_r$ the terms which occur repeatedly.

Now we are in a position to prove the necessity of the condition in the Theorem.

Assume false. Then G contains an $S^*_{p,q}$-group Q. By Lemma 1 for the p-Sylow-group Q_p of Q the relation $Q_p < Q$ holds. By Lemma 2 Q contains a subgroup R with $R \lhd Q$ satisfying $(Q : R) = p$. R as a proper subgroup of Q is nilpotent. R contains a q-Sylow-group Q_q of Q. By the nilpotence of R it follows that Q_q is a characteristic subgroup in R. Using $R \lhd Q$ we have $Q_q \lhd Q$. By $Q_p \lhd Q$ and by $Q_q \lhd Q$ now follows, that Q is the direct-product of its Sylow-groups. This means that Q is nilpotent. The contradiction obtained completes the proof of the necessity.

The condition is sufficient

We use induction on $|G|$. We suppose that for a finite group G_1 with $|G_1| < |G|$ the condition $S^* \not\subseteq G_1$ has the consequence that G_1 possess the property $(\bigcirc)$.

First we make the additional condition, that the group G is solvable.

We make use of the following important result of P. HALL [5]

LEMMA 3. Let G be a finite solvable group. Suppose that $|G| = m \cdot n$, $(m, n) = 1$ holds. Then

a) G contains a subgroup H with $|H| = m$.

b) All subgroups of order m in G are conjugate to each-other.

c) Any subgroup of G, whose order divides m lies in one of the subgroups of order m.

For the proof of Lemma 3. see [4] p. 237, Theorem 11.1.1.

Using Lemma 3 one obtains by well-known arguments the following

LEMMA 4. Let G be a finite solvable group. Suppose that $|G|$ has besides (1) the prime power representation

$$|G| = q_1^{\lambda_1} \ldots q_s^{\lambda_s}, \qquad q_1 < \ldots < q_s. \tag{5}$$

Then G possesses the property ($\bigcirc$) if and only, if there is a system of characteristic subgroups G_j^*, $0 \leq j \leq s$, in G with

$$G = G_0^* > G_1^* > \ldots > G_{s-1}^* > G_s^* = \langle e \rangle \tag{6}$$

satisfying

$$G_j^* = q_{\lambda_{j+1}}^{\lambda_{j+1}} \ldots q_s^{\lambda_s}, \qquad 1 \leq j \leq s-1. \tag{7}$$

(Of course the chain (6) is uniquely determined.)

The proof of Lemma 4 as mentioned is easy, so we omit the details.

To depict the logical structure of the proof, we mention that we have to deal with two cases separately. In the first one we suppose that in (5) $s=2$ holds. In the remaining one we treat with the case $s \geq 3$. By mentioning that the p-groups are nilpotent, it follows that so all possible cases are covered.

Case 1. As mentioned, in this case we suppose that

$$|G| = q_1^{\lambda_1} q_2^{\lambda_2}, \qquad q_1 < q_2, \qquad \lambda_1 \geq 1, \qquad \lambda_2 \geq 1, \tag{8}$$

holds.

We need the following

LEMMA 5. Let G be the group with (8). Suppose further that G contains a normal subgroup Q satisfying $q_2 / |Q|$ and $q_1 / |G/Q|$. Then if $S^* \not\subseteq G/Q$ holds, so G possesses the property ($\bigcirc$).

PROOF. Denote by Q_{q_2} a q_2-Sylow-group of Q. By the induction using Lemma 4 it follows that Q_{q_2} is a characteristic subgroup in Q. By $Q \lhd G$ we deduce that $Q_{q_2} \lhd G$ holds.

CASE 1. $q_2 \nmid |G/Q|$. In this case Q_{q_2} is the single q_2-Sylow-group of G and by $Q_{q_2} < G$, using Lemma 4 the statement of Lemma 5 follows.

CASE 2. $q_2 / |G/Q|$. In this case by $S^* \not\subseteq G/Q$, by the induction on $|G|$ it follows, appealing to Lemma 4 that for the q_2-Sylow-group T/Q of G/Q the relation $T/Q \lhd G/Q$ holds. By a well-known result, (see [4] p. 46., Theorem 2.4.2) we

deduce that $T < G$ holds. Mentioning that T contains a q_2-Sylow-group of G, using Lemma 4 again, the assertion of Lemma 5 follows in this case also.

G as a solvable group has a normal subgroup H satisfying

$$|G/H| = \begin{cases} q_1, \text{ or} \\ q_2. \end{cases}$$

In the case $|G/H| = q_1$ Lemma 5 applies. So it remains to deal with the case $|G/H| = q_2$.

SUBCASE 1. In this section we suppose that in (8) the equality $\lambda_2 = 1$ holds. We need the following

LEMMA 6. Let G be a finite nilpotent group. Then G possesses the property ($\bigcirc$), and the subgroups G_i in (2) can be choosen as normal subgroups in G.

For the proof of Lemma 6 see [4] p. 206., Theorem 9.4.3 and p. 365. Aufgabe 48.

By the induction on $|G|$ the condition $S^* \not\subseteq G$ results that every proper subgroup of G possesses the property ($\bigcirc$).

Let Y be an arbitrary but fixed proper subgroup of G. We show that Y is nilpotent. By the nilpotence of the p-groups we may suppose that

$$|Y| \equiv o(\text{mod } q_1 q_2) \tag{9}$$

holds. Denote by Y_{q_1} and by Y_{q_2} a q_1-Sylow-group and a q_2-Sylow-group of Y, respectively. Using Lemma 4, and mentioning that Y possesses the property ($\bigcirc$) $Y_{q_2} < Y$ follows. $Y_{q_1} < Y$ holds too. To this end it is enough to observe that in our case H is the q_1-Sylow-group of G and $H < G$ holds, to note further that two different q_1-Sylow-groups of Y cannot lie in H simultaneously. See [4] p. 70. Theorem 3.3.4. By $Y_{q_1} < Y$ and by $Y_{q_2} < Y$ now follows that Y is nilpotent.

So we obtain, that G is either nilpotent, or G is a one-step non-nilpotent group. In the first case by Lemma 6 G possesses the property ($\bigcirc$). In the second one by $S^* \not\subseteq G$ it follows that G is an $S^{**}_{p,q}$-group. By Lemma 1 and by Definition 1 now it follows, that the q_2-Sylow-group of G is a normal subgroup in G. So by Lemma 4 G possesses the property ($\bigcirc$). This completes the proof in the Subcase 1.

SUBCASE 2. In this case we suppose that in (8) the inequality $\lambda_2 > 1$ holds. By the definition of H now we have that $q_2 / |H|$ holds. Denote by K the q_2-Sylow-group of H. By the induction on $|G|$, using $S^* \not\subseteq G$ and appealing to Lemma 4 it follows that K is a characteristic subgroup in H. By $H < G$ we deduce that $K < G$ holds. If $S^* \not\subseteq G/K$ holds so by Lemma 5 G possesses the property ($\bigcirc$). We may therefore suppose in the sequel that G/K contains an $S^*_{p,q}$-group M.

PROPOSITION 1. If G does not possess the property ($\bigcirc$), then G/K is an $S^*_{p,q}$-group.

PROOF. As mentioned before G/K contains an $S^*_{p,q}$-group M. We have to show that $G/K = M$ holds. Assume false. Consider the inverse image in G of M. Denote it by L. L is a proper subgroup in G with $|L| = |K||M|$, and for L

$$\mathfrak{N}(q_2^{\lambda_2}; L) = q_2^{\lambda_2}. \tag{10}$$

holds. Use that by the induction L possesses the property ($\supset$), and appeal to Lemma 4.

On the other-hand Lemma 1 applies to M. So the q_1-Sylow-group of M is a normal subgroup in M. Note that M is an $S^*_{p,q}$-group. Since M is non-nilpotent the q_2-Sylow-groups of M cannot be normal subgroups in M. By $|M| = q_1^{l_1} q_2$, $1 \leq l_1 \leq \lambda_1$, we deduce that

$$\mathfrak{N}(q_2;\ M) > q_2 \tag{11}$$

holds. Consider now the group $\langle \alpha' \rangle$ in M, where α' is an arbitrary element of M with $|\alpha'| = q_2$. Consider further the inverse image in L of $\langle \alpha' \rangle$. Denote it by W. Then W contains q_2 cosets of L according to the normal subgroup K of G. Each of these cosets contains exactly $q_2^{\lambda_2 - 1}$ elements of L. So W is a subgroup of order $q_2^{\lambda_2}$ in L. Noting that the cosets in L, corresponding to distinct elements of M are disjoint, using (11) it follows that

$$\mathfrak{N}(q_2^{\lambda_2};\ L) > q_2^{\lambda_2} \tag{12}$$

holds. (10) and (12) give a contradiction. This completes the proof of Proposition 1.

PROPOSITION 2. If G does not possess the property ($\supset$), then the group H is nilpotent. Further the q_1-Sylow-group G_{q_1} of G is a normal subgroup in G.

PROOF. By Proposition 1 the group G/K is an $S^*_{p,q}$-group. By Lemma 1 and by Definition 1 the q_1-Sylow-group of M is a normal subgroup in M. Denote it by D. By $|M| = q_1^{l} q_2$ it follows that the inverse image in G of D is a subgroup U with $(G : U) = q_2$. By the induction, using $S^* \subsetneq G$

$$\mathfrak{N}(q_2^{\lambda_2 - 1};\ U) = q_2^{\lambda_2 - 1} \tag{13}$$

follows. Note that U possesses the property ($\supset$), and so Lemma 4 applies. By $K \subseteq U$ one has that the elements with (13) all lie in K. Observing now that all elements of M which do not belong to D has an order divisible by q_2, it follows that all elements of G, whose order is a power of q_1 lie in U. So especially the q_1-Sylow-groups of G are all contained in U.

We show first, that $H = U$ holds. To this end we mention that H contains at least one q_1-Sylow-group G_{q_1} of G further $K \leq U$ holds. Using that

$$H = \langle K, G_{q_1} \rangle$$

holds, by $K \leq U$ and by $G_{q_1} \leq U$ the relation $H \leq U$ follows. Now using $|H| = |U|$, $H = U$ is a consequence.

Let the meaning of G_{q_1} be as before. $G_{q_1} \leq H$ holds. By $H \lhd G$ we have that $N(G_{q_1}) \leqq H$ holds. See [4] p. 70, Theorem 3.3.2. Assuming $N(G_{q_1}) \neq G$ we deduce a contradiction.

If $N(G_{q_1}) = G$, then by the induction on $|G|$, using $S^* \subsetneq G$ we deduce that the q_2-Sylow-group of $N(G_{q_1})$ is a normal subgroup in $N(G_{q_1})$. Use Lemma 4 $G_{q_1} \lhd N(G_{q_1})$ holds trivially. So $N(G_{q_1})$ is the direct-product of its Sylow-groups, and so it is nilpotent.

Denote by W an arbitrary q_2-Sylow-group of G. Note further that for any subgroups A and B in G the relation

$$|A||B| \leq |\langle A, B\rangle| \cdot |A \cap B| \tag{14}$$

holds, (see [4] p. 32. Theorem 1.5.4) putting $A=H$, $B=W$ and observing that $\langle H, W\rangle = G$ holds, the relation $|H \cap W| = q_2^{l_2-1}$ follows. This means that $H \cap W = K$ holds. Use $|H| = q_1^{l_1} q_2^{l_2-1}$, and the definition of K.

By $N(G_{q_1}) \not\leq H$ now follows, that the q_2-Sylow-group of $N(G_{q_1})$ contains an element α with $\alpha \notin H$. This q_2-Sylow-group of $N(G_{q_1})$ is contained in one of the q_2-Sylow-groups of G, say in W. Then $W = \langle \alpha; K\rangle$ holds.

Using $W = \langle \alpha; K\rangle$, we deduce that $W \lhd G$ holds. Namely the elements γ of G have a unique representation

$$\gamma = \varphi \cdot \psi, \qquad \varphi \in G_{q_1}, \qquad \psi \in W.$$

Using that $N(G_{q_1})$ is nilpotent, for $\varphi \in G_{q_1}$, $\varphi^{-1}\alpha\varphi = \alpha$ follows. So we have

$$\gamma^{-1}\alpha\gamma = \psi^{-1}(\varphi^{-1}\alpha\varphi)\psi = \psi^{-1}\alpha\psi \in W. \tag{15}$$

Using $K \lhd G$ and (15), by $W = \langle \alpha; K\rangle$, $W \lhd G$ follows.

By $W \lhd G$, using Lemma 4 we have that G possesses the property ($\bigcirc$). This contradicts to the assumption in Proposition 2. So we have $N(G_{q_1}) = G$. By $K \lhd H$ and by $G_{q_1} \lhd H$ we have that H is nilpotent. This completes the proof of Proposition 2.

PROPOSITION 3. Suppose that G does not possess the property ($\bigcirc$). Then the proper subgroups of G are all nilpotent.

PROOF. Using that the p-groups are nilpotent we may concentrate to the subgroups T in G with

$$|T| = o(\mathrm{mod}\ q_1 q_2) \tag{16}$$

Let T be an arbitrary but fixed proper subgroup of G with (16). Denote a q_1-Sylow-group of T by T_{q_1}. The meaning of T_{q_2} let be analogous. Then by the induction, using $|T| < |G|$, and $S^* \not\subseteq G$, T possesses the property ($\bigcirc$). By Lemma 4 $T_{q_2} \lhd T$ follows. By $N(G_{q_1}) = G$, see Proposition 2, we deduce that $T_{q_1} \lhd T$ holds. It is enough to appeal to [4] p. 70 Theorem 3.3.4 again. By $T_{q_1} \lhd T$ and by $T_{q_2} \lhd T$ we deduce that T is nilpotent. This completes the proof of Proposition 3.

Now we are ready to prove that the condition of the Theorem is sufficient in the Subcase 2.

Assume false. Then by Proposition 3 G is either nilpotent, or it is a one-step non-nilpotent group. In the first case using Lemma 6. we get a contradiction. In the second one by $S^* \not\subseteq G$ it follows, that G is an $S^{**}_{p,q}$-group. This leads to a contradiction by mentioning, that by Lemma 1, and by Definition 1 the q_2-Sylow-group of G is a normal subgroup in G, noting further that Lemma 4 applies and so G possesses the property ($\bigcirc$).

This completes the proof in the Subcase 2.

Case 2. In this case we suppose that in (5) the inequality $s \geq 3$ holds. Using Lemma 3 we have that there are subgroups K, L and M in G with

$$K \leq L, \qquad K \leq M$$

and

$$(G:K) = q_1^{k_1} q_2^{k_2}, \qquad (G:L) = q_2^{k_2}, \qquad (G:M) = q_1^{k_1}.$$

By the induction, using $S^* \not\subseteq G$, it follows that L and M possesses the property ($\bigcirc$). By Lemma 4

$$K \lhd L \text{ and } K \lhd M$$

follows. So we have that $L \leq N(K)$, and $M \leq N(K)$ hold simultaneously. By these relations $N(K) = G$ follows. Using $(|K|, |G/K|) = 1$, it follows by Lemma 3 that G has a subgroup T with

$$T \cong G/K \tag{17}$$

By the induction using $S^* \not\subseteq G$, noting that by (17) $S^* \not\subseteq G/K$, we have that the q_2-Sylow-group of G/K is a normal subgroup in G/K. Use Lemma 4. By this we have that $M \lhd G$ holds. Using Lemma 4 again it follows that G possesses the property ($\bigcirc$). This completes the proof in the Case 2.

It remains to show, that the condition concerning to the solvability of G can be omitted.

We use induction on $|G|$. Suppose that for any finite group G_1 with $|G_1| < |G|$ and with $S^* \not\subseteq G_1$, it follows that G_1 possesses the property ($\bigcirc$). It is to prove that the same is true for G, if $S^* \not\subseteq G$ holds.

We need the following

Definition 3. Let S be an arbitrary p-group. Define $d(S)$ by

$$d(S) \overset{\text{def}}{=} \max \{|A|;\ A \text{ an abelian subgroup of } S\}.$$

Let $J(S)$ be the (characteristic) subgroup of S, generated by all the abelian subgroups of order $d(S)$ in S.

The following notation will be useful in the sequel.

Definition 4. Let G be a finite group. Suppose that $p^x \| |G|$ holds. (i.e. $p^x | |G|$, $p^{x+1} \nmid |G|$.) By a normal p-complement for G we mean a normal-subgroup of index p^x in G, which contains all the elements of G, with orders prime to p.

The following statement is an important result of J. G. Thompson [6], which we state in a modificated form due to G. Glaubermann [7].

Lemma 7. Let p be a prime and let S be a p-Sylow-group of the finite group G. If $C(Z(S))$ and $N(J(S))$ have normal p-complements then G has a normal p-complement, except possibly when $p=2$ and S^4 is involved in G.

Here S^4 stands for the symmetric group of four letters.

Suppose first that G is simple. Choose p as the least prime divisor of $|G|$. Denote by S one of the p-Sylow-groups of G. By the assumption $C(Z(S))$ and $N(J(S))$ are proper subgroups in G. By the induction, using $S^* \not\subseteq G$ it follows

that $C(Z(S))$ and $N(J(S))$ possesses the property ($\supset$). So by Lemma 4 they have normal p-complements. By $S^* \trianglelefteq G$ it follows that S^* cannot be involved in G. Now by Lemma 7 it follows that G has a normal p-complement. This contradicts to the assumption that G is simple.

We may therefore suppose that G has a normal subgroup H with $H \neq G$ and with $H = \langle e \rangle$. By the minimality of $|G|$, using $S^* \trianglelefteq G$ it now follows, that the proper-subgroups of G possesses all the property ($\supset$). So especially they are all solvable.

We distinguish two cases. In the first one we suppose that there is a maximal subgroup M in G with $H \leq M$. In the second one we deal with the case, when every maximal subgroup of G contains H.

CASE 1. Using $HM = G$, we have

$$G/H \simeq M/H \supset M \tag{18}$$

See [4] p. 46, Theorem 2.4.1. M is solvable by the assumption. So by (18) the solvability of G/H follows. By the solvability of H and G/H the solvability of G follows. This completes the proof in the Case 1.

CASE 2. Denote by $\Phi(G)$ the Frattini-subgroup of G. Then by the assumption in the Case 2 $\Phi(G) = \langle e \rangle$. $\Phi(G)$ is nilpotent. See [4] p. 203, Theorem 9.3.5.

So we may suppose that $H < G$ holds, and H is an elementary abelian p-group.

It suffices to prove that $S^* \not\trianglelefteq G/H$ holds, and to note that by the induction G/H possesses the property ($\supset$), and so it is solvable.

Asume false. Then G/H contains an $S^*_{p,q}$-group T/H, $T \simeq G$. Suppose that

$$|T/H| = r^h t^l, \qquad r < t, \tag{19}$$

holds r and t are primes. Suppose further that $|H| = q^j$. We may suppose that T/H is a proper-subgroup of G/H. Namely the case $G/H = T/H$ results by Lemma 1 that G/H is solvable and so it remains nothing to prove.

By $T/H < G/H$ it follows that $T < G$. Suppose first that the primes q, r, t are all different. In this case using Lemma 3 it follows that there is a subgroup B in T with

$$B \simeq T/H. \tag{20}$$

(20) contradicts to the assumption $S^* \not\trianglelefteq G$.

It remains to deal with the cases $q = r$ and $q = t$.

Take first the case $q = r < t$. Then $|T| = q^{j+h} t^l$ holds. By the minimality of G we have that T possesses the property ($\supset$). By Lemma 4 we deduce that for the t-Sylow-group T_t of T, $T_t \triangleleft T$ holds. On the other hand by Lemma 1 and by Definition 1 we have that the q-Sylow-group of T/H is a normal subgroup in T/H. By this, using [4] p. 46 Theorem 2.4.2., it follows that for the q-Sylow-group T_q of T, the relation $T_q \triangleleft T$ holds. By $T_t \triangleleft T$ and by $T_q \triangleleft T$ we get that T is nilpotent. Hence the nilpotence of T/H follows. This is a contradiction. This completes the proof in the case $q = r < t$.

It remains to investigate the case $q=t>r$. T possesses the property ($\supset$) as mentioned before. So as we saw in the preceeding case the q-Sylow-group of T is a normal subgroup in T. So

$$\mathfrak{N}(q^{j+1}; T) = q^{j+1} \tag{21}$$

holds.

On the other hand using Lemma 1 and Definition 1 one obtains that

$$\mathfrak{N}(q^{j}; T/H) > q^{j} \tag{22}$$

holds. Using the one-to-one correspondence between the t-Sylow-groups of T/H and those of T given in [4] p. 46 Theorem 2.4.2. one obtains immediately that by (22)

$$\mathfrak{N}(q^{j+1}; T) > q^{j+1} \tag{23}$$

holds. (21) and (23) give a contradiction. This completes the proof in the case considered, and so the proof of the Theorem is finished.

We mention the following corollary of the Theorem.

COROLLARY. Let G be a finite group. Suppose that for $|G|$, (5) holds. Define the natural numbers $\varepsilon_{i,j}$ as the least positive integers satisfying

$$q_i^{\varepsilon_{i,j}} \equiv 1 (\mathrm{mod}\ q_j), \qquad 1 \leq i, j \leq s, \ i \neq j. \tag{24}$$

Define further the natural numbers $a_1, \ldots, a_{s-1}$ by

$$a_j \overset{\mathrm{def}}{=} \min\{\varepsilon_{j,j+1}, \ldots, \varepsilon_{j,s}\} \tag{25}$$

Then using (4) in Lemma 1, one obtains by the Theorem of the present paper, that if in (5)

$$\alpha_j < a_j, \qquad 1 \leq j \leq s-1, \tag{26}$$

hold simultaneously, then the group G possesses the property ($\supset$).

Especially the following statement is true.

THEOREM A. Let G be a finite group. Suppose that $12 \nmid |G|$ holds. Then if for any prime divisor p of $|G|$, which is different from the maximal one, $p^3 \nmid |G|$ holds, so $|G|$ possesses the property ($\supset$).

The example of the group A^4 (the alternating group of four letters) shows that the condition $12 \nmid |G|$ in Theorem A cannot be omitted.

References

[1] RÉDEI, L., Die endlichen einstufig nicht-nilpotenten Gruppen, *Publ. Mat.*, **4** (1955–1956), 303–324.

[2] SCHMIDT, O. JU., Über Gruppen, deren sämtliche Teiler spezielle Gruppen sind, *Mat. Sbornik*, **31** (1924), 366–372. (Russisch mit deutscher Zusammenfassung.)

[3] GOLFAND, JU. A., Über Gruppen deren sämtliche Untergruppen speziell sind, *Dokl. Akad. Nauk.* SSSR, N.S., **60** (1948), 1313–1315 (Russisch).

[4] KOCHENDÖRFFER, R., *Gruppentheorie*, Leipzig, 1966, Akad. Verlag.

[5] HALL, P., A note on soluble groups, *J. London Math. Soc.*, **3** (1928), 98–105.

[6] THOMPSOM, J. G., Normal p-complements for finite groups, *J. Algebra*, **1** (1964), 43–46.

[7] GLAUBERMANN, G., Subgroups of finite groups, *Bull. Amer. Math. Soc.*, **73** (1967), 1–12.

ON THE THEORY OF THE ONE-STEP NON-ABELIAN GROUPS

By

K. A. CORRADI

Department of Algebra and Number Theory of the Eötvös Loránd University, Budapest

(Received September 18, 1968)

Following L. RÉDEI we call a finite non-abelian group one-step non-abelian, if all proper subgroups of it are abelian.

Following L. RÉDEI, we denote by $o(p(\mathrm{mod}\, q))$ the order of p mod q, i.e. the least national number with $p^m \equiv 1(q)$.

L. RÉDEI proved in [2] the following important

THEOREM A. *The finite one-step non-Abelian groups of composite order are obtained as follows: Given two different primes p, q and a natural number n, put*

$$m = o(p(\mathrm{mod}\, q)),$$

take the finite field F of order

$$|F| = p^m$$

and from the group F^* (the multiplicative group of F) an arbitrary fixed element ω with

$$o(\omega) = q.$$

Then a one-step non-abelian group $G = R_{p,q,n}$ (of order $|G| = p^m q^n$) exists such that by help of certain special elements

$$P_\alpha(\alpha \in F),\ Q\ (P_0 \text{ the unity element}, o(P_\alpha) = p \text{ for } \alpha \neq 0,\ o(Q) = q^n)$$

the distinct elements of G may be written uniquely in the form

$$P_\alpha Q^i (\alpha \in F;\ i = 0, \ldots, q^n - 1)$$

and the rule for multiplication of elements is

$$P_\alpha Q^i \cdot P_\beta Q^k = P_{\alpha + \omega^i \beta} Q^{i+k}, \qquad (\alpha, \beta \in F;\ i, k = 0, \ldots, q^n - 1).$$

Taking for each of the above triples p, q, n such a group, we just obtain the mutually non-isomorphic one-step non-Abelian groups which are distinct from the p-groups.

In the present work our aim is to determine the simple characters of an $G=R_{p,q,n}$ group.

First of all we remark, that from the Theorem A it follows, that the commutator-subgroup of G is its Sylow-group of order p^m. Further the centre of G consist of the elements

$$Q^i,\ q_j i,\ i=0,\ldots,q^n-1$$

and so it is of order q^{n-1}. From these two facts it follows, that G has a uniquely determined proper-subgroup U of order $p^m q^{n-1}$, i.e. U is of index q in G.

As easy to see U as a proper subgroup of G is abelian. Denote by ψ_0 the principal character of U. As a non-trivial character of U we call the characters ψ of U satisfying

$$\psi^{q^{n-1}} \neq \psi_0.$$

As easy to see the number of non-trivial characters in U is equal to $q^{n-1}(p^m-1)$. This follows by the rule for multiplication in Theorem A.

After these preliminaries we are now ready to state the following

THEOREM. *Let G be a finite $R_{p,q,n}$ group. Let U be the proper-subgroup of index q in G. There are*

$$q^n+q^{n-2}(p^m-1)$$

simple characters of G. From these q^n are of order one, and can be obtained in the well-known way. The simple characters of G whose order is greater than one can be obtained in the following way.

Take any non-trivial character ψ of U. Put

$$\chi_\psi(a)=\frac{N(a)}{U}\sum_{z\in K(a)\cdot U}\psi(z),\qquad a\in G,$$

where $N(a)$ stands for the normalisator of a, and by $K(a)$ we denote the class of elements in G conjugate to a. Then χ_ψ is a simple character of order q in G. If ψ runs through the non-trivial characters of U, we get all the simple characters of order greater than one of G and each of them occurs exactly q times.

For the proof of the theorem we need some well-known results on group-characters, which we quote as lemmas.

LEMMA 1. Let G be a finite group. Denote by t the number of classes of conjugate elements in G. There are t simple characters of G. Denote them by $\chi^{(r)}$, $(1\leq r\leq t)$. Then if f_r denotes the degree of $\chi^{(r)}$ so

$$\sum_{r=1}^{t} f_r^2=G \tag{1}$$

holds.

LEMMA 2. Let χ_1 and χ_2 be any two characters of G. Let us denote by m_r and n_r the multiplicity of $\chi^{(r)}$ in the representation of χ_1 and χ_2, respectively.

Then

$$\frac{1}{|G|}\sum_{a\in G}\chi_1(a)\bar{\chi}_2(a) = \sum_{r=1}^{t} m_r n_r \tag{2}$$

holds. $m_r \geq 0$, $n_r \geq 0$ are integers.

LEMMA 3. Let G be a finite group, $U \subset G$ a proper subgroup of G. Let ψ be an arbitrary character of U. Then

$$\chi_\psi(a) \overset{\text{def}}{=} \frac{|N(a)|}{|U|}\sum_{z\in K(a)\cap U}\psi(z) \tag{3}$$

defines a character of G.

LEMMA 4. Let G be a finite group. Let us denote by G' its commutator-subgroup. Then G has

$$|G/G'|$$

simple characters of order one. If χ denotes one of them and $G'a$ is a residue-class induced by G', then for $b, c \in G'a$

$$\chi(b) = \chi(c)$$

holds.

REMARK. Using lemma 2 with $\chi_2 \equiv \chi_1$

$$\frac{1}{|G|}\sum_{a\in G}|\chi_1(a)|^2 = \sum_{r=1}^{t} m_r^2$$

follows. From this one obtains, that a character τ of G is if and only if simple when

$$\frac{1}{|G|}\sum_{a\in G}|\tau(a)|^2 = 1$$

holds.

For all these results and their proofs see [3] pp. 300–361.

PROOF OF THE THEOREM. As mentioned already the commutator-subgroup of G is the Sylow-group H of order p^m of G. Thus by Lemma 4 it follows that there are exactly q^n simple characters of order one in G.

Now our next task will be to prove, that the number t of the classes of conjugate elements in G is given by

$$t = q^n + q^{n-2}(p^m - 1). \tag{4}$$

The number t can be calculated using the rule for multiplication in Theorem A. We used here another way. Denote by L a Sylow-group of order q^n of G. Denote the normalisator of L by $N(L)$. As well-known the number of different Sylow-groups of order q^n is equal to $|G/N(L)|$. From the well-known Theorem of Sylow (see [3] p. 68.) it follows, that

$$|G : N(L)| \equiv 1 (\text{mod } q) \tag{5}$$

holds. Note that $|G : N(L)| / p^m$ is satisfied. Note further that by the definition of m, m is the least natural number with

$$p^m \equiv 1 (\mathrm{mod}\ q).$$

These two results using (5) give that

$$|G : N(L)| = \begin{cases} 1, \\ \text{or } p^m \end{cases}$$

are the only possibilities, which can occur. The first of them is impossible. Namely using the rule for multiplication of Theorem A one obtains that all elements of the form Q^i and of the form

$$P_\alpha Q^i, \qquad (\alpha \in F,\ \alpha \neq 0;\ q \nmid i,\ i = 1, \ldots, q^n - 1)$$

has on order dividing q^n and so the number of elements a in G with

$$a^{q^n} = e$$

— where e stands for the unity element of G-would be at least

$$(p^m - 1)(q^n - q^{n-1}) + q^n > q^n.$$

Note that by $p \geq 2$, $p^m > 1$. On the other-hand all elements, whose order is a power of q had to lay in the single Sylow-group L of order q^n.

So there are p^m different Sylow-groups of order q^n in G. Each of them contains the centre C of order q^{n-1} of G. From this follows that any two of them can not have an element in common which do not lay in C. So the number of elements in G whose order is a power of q is given by

$$q^{n-1} + p^m(q^n - q^{n-1}).$$

Using that H is the single Sylow-group of order p^m in G it now follows, that there are exactly

$$p^m q^{n-1} - p^m - q^{n-1} + 1 = (p^m - 1)(q^{n-1} - 1)$$

elements a in G satisfying

$$o(a) \equiv 0 (\mathrm{mod}\ pq). \tag{6}$$

Take now the subgroup U of order $p^m q^{n-1}$ already mentioned. U is abelian, so it contains all $a \in G$ satisfying (6).

By

$$U = \{H, C\} \tag{7}$$

it follows easily that U is a normal subgroup of G. From this it follows by known arguments, that for $a \in U$

$$|K(a)| = |G : \mathrm{N}(a)| = \begin{cases} 1 \text{ if } a \in C, \\ q \text{ ig } a \in U,\ a \notin C \end{cases} \tag{8}$$

holds.

For $a \notin U$ $o(a) = q^n$ follows and for such elements

$$|K(a)| = p^m$$

holds. The number of the classes containing these elements is

$$q^n - q^{n-1}. \tag{9}$$

By (8) and (9) using $|U| = p^m q^{n-1}$ now follows that

$$t = q^{n-1} + (q^n - q^{n-1}) + (p^m - 1)q^{n-2} = q^n + (p^m - 1)q^{n-2}.$$

So (4) is proved. We have also that there are $(p^m - 1)q^{n-2}$ simple characters of G whose degree is greater than one. Use Lemma 1.

Let now ψ be any character of U. Define χ_ψ by

$$\chi_\psi(a) \overset{\text{def}}{=} \frac{|N(a)|}{|U|} \sum_{z \in K(a) \cap U} \psi(z).$$

By Lemma 3, χ_ψ is a character of G.

So one has that

$$\chi_\psi(a) = \begin{cases} q\psi(a), & \text{if } a \in C, \\ 0, & \text{if } a \notin U, \\ \sum\limits_{z \in K(a)} \psi(z), & \text{if } a \in U,\ a \notin C. \end{cases}$$

Denote the simple characters of degree one of G by δ_ν $(1 \leq \nu \leq q^n)$. Then

$$\frac{1}{|G|} \left| \sum_{a \in G} \chi_\psi(a) \bar{\delta}_\nu(a) \right| \leq \frac{1}{|G|} \sum_{a \in G} |\chi_\psi(a)| = \frac{1}{|G|} \sum_{a \in U} |\chi_\psi(a)| \leq 1. \tag{10}$$

Here we used (8). The sign of equality in the first inequality of (10) can only occur if for all $a \in U$, $a \notin C$

$$\bar{\delta}_\nu(a) \sum_{z \in K(a)} \psi(z) = q$$

holds simultaneously. This can be the case only, if for all such a

$$\psi(a) \equiv \delta_\nu(a) \tag{11}$$

holds. Besides this (11) has to hold for all $a \in C$ trivially. So

$$\psi^{q^{n-1}} = \psi_0$$

shall be satisfied.

This means that for non-trivial characters ψ of U

$$\frac{1}{|G|} \sum_{a \in G} \chi_\psi(a) \bar{\delta}_\nu(a) = 0$$

holds by Lemma 2. So the $(p^m - 1)q^{n-1}$ non-trivial characters ψ of U defines $(p^m - 1)q^{n-1}$ characters of G which do not contain the characters δ_ν, $(1 \leq \nu \leq q^n)$ in their representation.

Denote the simple characters of G of degree greater than one by $\sigma_1, \ldots, \ldots, \sigma^{(p^m-1)q^{n-2}}$. So for a non-trivial character ψ, χ_ψ has the representation

$$\chi_\psi = \sum_{r=1}^{(p^m-1)q^{n-2}} m_r \sigma_r. \tag{12}$$

Now we investigate the sum

$$\frac{1}{G} \sum_{a \in G} \chi_\psi(a) \left| \sum_{\psi'} \bar{\chi}_{\psi'}(a) \right| \tag{13}$$

where in the inner sum ψ' runs over all $p^m q^{n-1}$ characters of U'. As easy to see $\bar{\chi}_{\psi'}(a) = \chi_{\bar{\psi}'}(a)$ holds. Note that if ψ' runs over all characters of U', $\bar{\psi}'$ does the same. Now

$$\sum_{\psi'} \chi_{\psi'}(a) = \sum_{\psi'} \frac{N(a)}{|U|} \sum_{z \in K(a) \cap U} \psi'(z). \tag{14}$$

The inner sum on the right-hand side of (14) is equal to zero if $a \notin U$. Note that in this case $K(a) \cap U$ is empty. If $a \in U$, $a \neq e$ holds, the right-hand side of (14) can be written in the form

$$\frac{N(a)}{|U|} \sum_{z \in K(a)} \sum_{\psi'} \psi'(z). \tag{15}$$

Note now, that in the case $a \neq e$, $z \neq e$ follows. Take now into account that

$$\sum_{\psi'} \overline{\psi}'(z) = 0 \tag{16}$$

holds if $z \neq e$ by the well-known ortogonality of the characters of an abelian group. So we have

$$\frac{1}{G} \sum_{a \in G} \chi_\psi(a) \left| \sum_{\psi'} \bar{\chi}_{\psi'}(a) \right| = \frac{1}{G} \chi_\psi(e) \left| \sum_{\psi'} \bar{\chi}_{\psi'}(e) \right| = \frac{1}{G} \cdot q \cdot q\, p^m q^{n-1} = q. \tag{17}$$

Consider now for non-trivial characters ψ of U' the characters χ_ψ of G. Let us denote by a_r the number of different characters ψ from those mentioned for which in the representation of χ_ψ under (12) $m_r \neq 0$ holds.

By (12), noting that the number of ψ-s in consideration is equal to $(p^m-1)q^{n-2}$

$$\sum_{r=1}^{(p^m-1)q^{n-2}} a_r \geq (p^m-1)q^{n-1} \tag{18}$$

follows. Note that every χ_ψ induced by a non-trivial ψ has at least one σ_r in his representation (12).

From (18) now follows, that for at least one r, $(1 \leq r \leq (p^m-1)q^{n-2})$, $a_r \geq q$ holds. We show now that $a_r > q$ is impossible. So by (18)

$$a_r = q, \qquad 1 \leq r \leq (p^m-1)q^{n-2}$$

will follow.

Suppose the contrary. Then there exists at least one r with $a_r > q$. Let be the characters which contains σ_r in their representation $\chi_{\nu_1}, \ldots, \chi_{\nu_l}$. By the assumption $l \geq q+1$.

Note firstly that for every pair $\chi_\nu, \chi_{\nu'}$

$$\sum_{a \in G} \chi_\nu(a)\bar{\chi}_{\nu'}(a) \geq 0 \tag{19}$$

holds. So by (17)

$$q\,|G| \geq \sum_{a \in G} \chi_{\nu_1}(a) \left\{ \sum_{\lambda=1}^{l} \bar{\chi}_{\nu_\lambda}(a) \right\} \tag{20}$$

follows. On the other-hand denoting by b_λ the multiplicity of σ_r in the representation (12) of χ_{ν_λ}, $b_\lambda \geq 1$ holds for every λ with $1 \leq \lambda \leq l$.

Using (2) of Lemma 2, one obtains immediately

$$\sum_{a \in G} \chi_{\nu_1}(a) \left\{ \sum_{\lambda=1}^{l} \bar{\chi}_{\nu_l}(a) \right\} \geq |G| \sum_{\lambda=1}^{l} b_1 b_\lambda \geq |G|\, l \geq |G|\,(q+1). \tag{21}$$

(20) and (21) give a contradiction. The same argument shows, that for $l = q$ (20) and (21) holds simultaneously in the case only, if $b_1 = b_2 = \ldots = b_q = 1$ and the characters $\chi_{\nu_1}, \ldots, \chi_{\nu_q}$ contain the character σ_r alone in their representation (12).

This completes the proof our Theorem.

References

[1] Rédei, L., *Algebra*, Leipzig, 1959, Akad. Verlag.
[2] Rédei, L., Die Anwendung des schiefen Produktes in der Gruppentheorie, *J. reine und angew. Math.*, 188 (1950), 201–227.
[3] Kochendörfer, R., *Gruppentheorie*, Leipzig, 1966, Akad. Verlag.

ON SOME EXTREMAL PROPERTIES OF SEQUENCES OF INTEGERS

By

P. ERDŐS, A. SÁRKÖZI and E. SZEMERÉDI

Mathematical Institute of the Hungarian Academy of Sciences, Budapest

(Received 15 March, 1969)

Let $\{A\} = a_1 < a_2 < \dots$ be a sequence of positive integers. Put $A(n) = \sum_{a_i \le n} 1$. Denote by $f_k(n)$ the smallest integer so that every sequence A satisfying $A(n) = f_k(n)$ contains a subsequence of k terms which are pairwise relatively prime. It is easy to see that $f_2(n) = \left[\frac{n}{2}\right] + 1$ and it seems likely that

$$f_k(n) = 1 + \psi_{k-1}(n) \tag{1}$$

where $\psi_{k-1}(n)$ denotes the number of integers not exceeding n which are multiples of at least one of the first $k-1$ primes $2, 3, \dots, p_{k-1}$. Clearly (1) if true is best possible. (1) is easy to show for $k = 3$, but we have not been able to prove it in general. On the other hand we prove in a sharper and more general form several conjectures stated in [1]. First we introduce some notations. $A_{(m,n)}$ denotes the integers $a_i \in A$, $a_i \equiv n \pmod m$ ($A_{(m,n)}(n)$ denotes the number of terms of the sequence $A_{(m,n)}$). $A_{(2,1)}$ respectively $A_{(2,2)}$, we will denote by A_1 respectively A_2. $\varphi(n)$ denotes Euler's φ function.

$$\varphi(A, k) = \sum_{\substack{a_i \le n \\ (a_i, k) = 1}} 1.$$

$\Phi(A)$ denotes the number of pairs $(a_i, a_j) = 1$, $a_i < a_j \le n$. Put

$$F(n) = \min_{A} \max_{a_j \in A} \varphi(A, a_j)$$

where the minimum is to be taken over all sequences A satisfying $A(n) \ge \left[\frac{n}{2}\right] + 1$.

For simplicity we will henceforth assume that n is even, all our results could easily be extended for odd n. $c_1, c_2 \dots$ denote suitable positive absolute constants.

Let $A(n) = \left[\frac{n}{2}\right] + 1$. P. ERDŐS proved that for $n > n_0$ $\Phi(A) > c_1 n/\log\log$

and in fact the minimum of $\Phi(A)$ is assumed if A consists of the even numbers and u_r where

$$u_r = 3\cdot 5, \ldots, p_r, 3\ldots p_r \leq n < 3\ldots p_r\cdot p_{r+1}.$$

He also conjectured that

$$\lim_{n=\infty} F(n) = \infty. \tag{2}$$

We now prove (2). In fact we prove the following sharper

THEOREM 1.

$$F(n) > c_2 n/\log\log n.$$

We first prove two other theorems which will easily imply Theorem 1.

THEOREM 2. *Let A satisfy*

$$A_1(n) = s, \qquad 1 \leq s < c_3 n, \tag{3}$$

$$A(n) > \frac{n}{2}. \tag{4}$$

Then for $n > n_0$

$$\max_{a_i \in A} \varphi(A, a_i) > c_4 n/\log\log\frac{n}{s} \tag{5}$$

and

$$\Phi(A) > c_5 sn/\log\log\frac{n}{s}. \tag{6}$$

We need the following known

LEMMA 1. *The number of integers $1 \leq k \leq n$ satisfying $\varphi(k)/k < 1/t$ is less than* ($\exp z = e^z$) $n \exp(-\exp c_6 t)$, *uniformly in $t > 1$.*

Choose

$$t = \frac{1}{c_6}\log\log\frac{2n}{s}. \tag{7}$$

We obtain from Lemma 1 that the number of integers $1 \leq k \leq n$ which satisfy $\varphi(k)/k < 1/t$ (where t is defined by (7)) is less that $s/2$. Thus the number of integers $a_i \in A_1$ for which $\varphi(a_i)/a_i > 1/t$ is by (3) greater than $s/2$. Denote now by $b_1 < \ldots < b_r \leq n$, $r > s/2$ the integers in A_1 satisfying $\varphi(b_i)/b_i > 1/t$. Clearly the number of integers $2u \leq n$ satisfying $(2u, b_i) = 1$ is greater than $\frac{n}{2}\frac{1}{2}\varphi(b_i)/b_i > n/4t$. Thus (in $\Sigma' a_j$ runs through the numbers of A_2)

$$\sum_{(b_i, a_j)=1}' 1 > A_2(n) - \frac{n}{2} + \frac{n}{4t}, \tag{8}$$

or by (8) and (7) for sufficiently small c_3 and c_4 we obtain by a simple computation for sufficiently large n

$$(9)\qquad \varphi(A, b_i) > A_2(n) - \frac{n}{2} + \frac{n}{4t} = A(n) - A_1(n) - \frac{n}{2} + \frac{n}{4t} > \frac{n}{4t} - s > c_4 n/\log\log\frac{n}{s},$$

which proves (5).

To prove (6) observe that (9) holds for every $1 \le i \le r$ and $r > \frac{s}{2}$, hence from (9)

$$\Phi(A) > \frac{c_4}{2} sn/\log\log\frac{n}{s},$$

which proves (6) and hence the proof of Theorem 2 is complete.

THEOREM 3. *To every c_9 there is a $c_{10} = c_{10}(c_9)$ $\left(c_{10}\right.$ is bounded in terms of $\left.\frac{1}{c_9}\right)$ so that if $A_1(n) = s > c_9 n$ and $A(n) > \frac{n}{2}$ then for $n > n_0$*

$$\Phi(A) > c_{10} n^2.$$

For $s < c_3 n$ Theorem 3 would follow from Theorem 2, but for the large values of s we need a separate proof.

Denote by P_r the product of the primes not exceeding r. We first prove

LEMMA 2. To every $\varepsilon > 0$ and $\delta > 0$ there is an $r = r(\varepsilon, \delta)$ so that if $n > m_0(\varepsilon, \delta, r)$ then for all but $\varepsilon \frac{n}{P_r}$ integers k satisfying

$$1 \le k \le n, \qquad k \equiv u \pmod{P_r}$$

we have

$$\alpha(k) = \prod_{\substack{p|k \\ p>r}} \left(1 - \frac{1}{p}\right) > 1 - \delta.$$

The Lemma is very easy to prove and we only outline it. We evidently have (in $\prod' k \equiv u \pmod{P_r}$, $1 \le k \le n$)

$$(10)\qquad \prod{}'\alpha(k) > \prod_{r<p<n} \left(1 - \frac{1}{p}\right)^{\frac{n}{pP_r}+1} > \prod_{p<n}\left(1 - \frac{1}{p}\right)\left(\prod_{r<p<n}\left(1 - \frac{1}{p}\right)^{1/p}\right)^{n/P_r} >$$
$$> (1 - \eta_r)^{n/P_r},$$

where η_r can be chosen as small as we wish if r is sufficiently large. (10) implies Lemma 2 by a simple argument.

Now we prove Theorem 3. We evidently have

$$(11)\qquad \sum_{i=1}^{\frac{1}{2}P_r} \left(A_{(P_r, 2i-1)}(n) + A_{(P_r, 2i)}(n) + A_{(P_r, 2i+1)}(n)\right) = A_2(n) + 2A_1(n) =$$
$$= A(n) + s > \frac{n}{2} + s.$$

Hence by (11) there is an i_0 for which

$$A_{(P_r,\,2i_0-1)}(n)+A_{(P_r,\,2i_0)}(n)+A_{(P_r,\,2i_0+1)}(n)>\frac{n+2s}{P_r}. \tag{12}$$

Clearly for every u $A_{(P_r,\,u)}(n)<\frac{n}{P_r}+1$. Thus we obtain from (12) that there are two integers u_1 and u_2, u_1 odd, $|u_1-u_2|=1$ or 2 satisfying

$$A_{(P_r,\,u_l)}(n)\geq\frac{1}{2}\left[\frac{2s}{P_r}-1\right]\quad(l=1,2). \tag{13}$$

Denote now by $a_1^*<\ldots<a_t^*$ the sequence of integers for which

$$k\in A_{(P_r,\,u_1)}\text{ and }\prod_{\substack{p|k\\ p>r}}\left(1-\frac{1}{p}\right)>1-c_9/10. \tag{14}$$

From Lemma 2 and (13) we have for $r>r_0$, $\varepsilon=\frac{1}{3}c_9$ $(s>c_9n)$

$$t>A_{(P_r,\,u_1)}(n)-\frac{\varepsilon n}{P_r}>\frac{2}{3}\frac{s}{P_r}-\frac{\varepsilon n}{P_r}>c_9n/3P_r. \tag{15}$$

Now we estimate from below the number of solutions of

$$(a_i^*,a_j)=1,\qquad a_j\in A_{(P_r,\,u_2)}. \tag{16}$$

Assume $p|(a_i^*,b)$, $b\equiv u_2(\mathrm{mod}\,P_r)$. As $|u_1-u_2|\leq 2$ and u_1 is odd, we have $p>r$. Denote by $B_i(P_r,u_2)$ the number of integers $b\leq n$, $b\equiv u_2(\mathrm{mod}\,P_r)$ for which $(b,a_i^*)=1$. We have by a simple argument

$$\left|B_i(P_r,u_2)-\frac{n}{P_r}\prod_{\substack{p|a_i^*\\ p>r}}\left(1-\frac{1}{p}\right)\right|<2^{V(a_i^*)}<2^{2\log n/\log\log n} \tag{17}$$

since it is well known (and follows from the prime number theorem or a more elementary theorem) that for $m<n$ $V(m)<2\log n/\log\log n$.

Thus from (14) and (17) for sufficiently large n

$$B_i(P_r,u_2)>(1-c_9/7)n/P_r. \tag{18}$$

From (18) and (13) we obtain that the number of solutions of (16) is greater than $(s>c_9n)$

$$\frac{1}{2}\left[\frac{2s}{P_r}-1\right]-c_9n/4P_r>c_9n/2P_r. \tag{19}$$

From (15) and (19) we evidently have

$$\Phi(A)>c_9^2n^2/6P_r^2$$

where r is bounded in terms of $1/c_9$ which proves Theorem 3.

It is now easy to prove Theorem 1. Let A be any sequence satisfying $A(n) \geq \frac{n}{2}+1$. We distinguish two cases. Assume first $A_1(n) < c_3 n$. In this case (5) and the definition of $F(n)$ implies Theorem 1. Assume next $A(n) \geq c_3 n$. Then from Theorem 3 we have

$$\max_{a_j} \varphi(A, a_j) \geq \Phi(A)/n > c_{10}(c_3)n$$

which completes the proof of Theorem 1.

We outline the following sharpening of Theorem 1.

THEOREM 4. *Let $n > n_0$. The only class of sequences A^* for which $F(n)$ is assumed is defined as follows: $A^* = A_1^* \cup A_2^*$,* where *A_1^* consists of all odd multiples not exceeding n of u_r $(3 \ldots p_r \leq n < 3 \ldots p_r p_{r+1}$, $u_r = 3 \ldots p_r)$ and A_2^* consists of the set of even numbers* (not exceeding n) *from which $A_1^*(n)-1$ even numbers relatively prime to u_r have been omitted.*

Theorem 4 clearly implies that

$$F(n) = \varphi_n^{(2)}(u_r) - \left[\frac{n}{u_r}\right] + \left[\frac{n}{2u_r}\right] + 1 \tag{26}$$

where $\varphi_n^{(2)}(u_r)$ denotes the number of even integers not exceeding n which are relatively prime to u_r.

We only outline the proof of Theorem 4. Let $A \left| A(n) \geq \frac{n}{2}+1 \right|$ be any sequence which contains an odd number u which is not a multiple of u_r. A simple argument shows (see [1]) that

$$\varphi_n^{(2)}(u) > \varphi_n^{(2)}(u_r) + c_{11} n/(\log n)^2.$$

Thus if

$$\varphi(A, u) \leq \varphi_n^{(2)}(u_r) - \left[\frac{n}{u_r}\right] + \left[\frac{n}{2u_r}\right] + 1$$

we must have $A_1(n) = s > c_{11} \frac{n}{(\log n)^2}$. But then from (5) and Theorem 3 we have

$$\max_{a_i \in A} \varphi(A, a_i) > c_{12} n/\log\log\log n > \varphi_n^{(2)}(u_r)$$

which proves Theorem 4. Theorem 4 implies by a well known theorem of Mertens that (C is Euler's constant)

$$F(n) = (1+o(1))e^{-C} n/\log\log n.$$

References

[1] P. ERDŐS, Remarks on number theory, V. Extremal problems in number theory II. (in Hungarian), *Mat. Lapok*, 17 (1966), 135–155.

[2] P. ERDŐS, Some remarks about additive and multiplicative functions, *Bull. Amer. Math. Soc.*, 52 (1946), 527–537.

AXIALLY SYMMETRIC PACKING OF EQUAL CIRCLES ON A SPHERE, II

By

M. GOLDBERG
Washington, D. C. U.S.A.

(Received August 24, 1967)

1. Introduction

An earlier paper [1] summarized the known results on the determination of the largest angular diameter $a(n)$ of n equal circular rings (or spherical caps) which can be packed on the surface of a sphere without overlapping. The present paper augments these results with a few improvements and additions. The relation of this problem to a problem associated with some biological structures is discussed in a note by the author [2].

2. Axially symmetric packing

Previous results frequently employed multi-symmetric arrangements. Sometimes, a special type of arrangement which had m-fold symmetry about only one axis was investigated. This paper will illustrate the advantages of investigating m-fold symmetry for various values of m and for different ordering of the successive zones.

3. A new result for $n=19$ and an improved result for $n=33$

In two recently published notes, an arrangement for 19 circles was computed [3], and an improved result for 33 circles was obtained [4]. The arrangements and the values $a(n)$ are given in Table 2.

4. Improvements for $n=21$ and $n=22$

Previously published results [5] for packing of 21 and 22 circles employed five-fold symmetry about an axis. An improved result by ROBINSON [6] for 22 circles employed tetrahedral symmetry and, therefore, it has three-fold symmetry. However, for both 21 circles and 22 circles, further improved results are shown here by using three-fold symmetry for 21 circles, and four-fold symmetry for 22 circles. The locations of the centers of typical circles in each zone are shown in Table 1. The value of $a(n)$ can be verified by computing the distan-

ces between adjacent centers. Figures 1 to 4 show these new arrangements. Note that Figures 1 and 4 have skew symmetry about the equater, but Figures 2 and 3 do not have symmetry about the equator. The comparison of the arrangements and their values of $a(n)$, $R(n)$ and $D(n)$ are shown in Table 2. The quantity $D(n)$, which represents the density of packing on the sphere, is given by $D(n) = n[1-\cos 0{,}5\, a(n)]/2$. If the circles have unit diameter, then the sphere has the radius $R(n)$ given by $R(n) = 1/\sqrt{2-2\cos a(n)}$.

5. New values for $n = 28$

No previous computations have been published for 28 circles. The present arrangements, shown in Figures 5, 6, and 7, show the sensitivity of $a(n)$ to the different ordering of the zones. All of these arrangements have four-fold symmetry and a symmetric notation. Nevertheless, only Figure 7 is symmetric about the equator, while the more efficient arrangements shown in Figures 5 and 6 have no symmetry about the equator.

6. New values for $n = 44, 48, 60, 80, 110, 120$

R. M. Robinson has investigated multi-symmetric arrangements which yield new results for $n = 22, 44, 48, 60, 80, 110$ and 120. Some of these are described in an abstract [7]. Their values of $a(n)$ are given in Table 2 and their arrangements are expressed in an axial symmetry notation. The arrangements for 44 and 48 circles are shown in Figures 8 and 9.

However, because of the low density that is listed for 60 circles, it is likely that a denser arrangement exists. Also, a denser arrangement for 80 circles is likely.

7. A general method of producing new packings

An efficient packing of $n+1$ circles can sometimes be made by inserting a circle in the largest opening of an efficient arrangement of n circles. These n circles are reduced in size until another circle of the same size can be inserted. One should not expect an efficient arrangement to be made by insertion in a triangular opening. Consider, for example, the arrangement 28{1,3,3,3,3,3,3,3,3,3} made by the insertion of a circle in a triangular opening of 27{3,3,3,3,3,3,3,3,3}.

This method of determining new efficient packings requires extensive computation and, therefore, it has not yet been investigated. The arrangements obtained may have only bilateral symmetry and, possibly, no symmetry.

8. Summary

The graphical representation of Fig. 10 is a tabulation of $D(n)$, the density of packing, for the best arrangements known for each value of n. The curve is the upper bound of $D(n)$ as determined by Robinson [8]. The values for 12 and 24 lie on this curve. The lengths of the vertical lines joining the data points to the curve are indications of the deviations from the curve. The value for 23 has been obtained by omitting one of the circles from the arrangement for 24 circles. No better value for 23 has yet been found. Values for 29, 34, 37, 38, 39, etc., where there are missing points, have not yet been determined.

The total number of contacts, and the average number of contacts per circle are given in Table 2. These serve as rough indications of efficiency. The larger the number of contacts per circle, the greater is the expected efficiency. However, there are anomalous cases. For example, note that, in each of the two arrangements 21{1,4,4,4,4,4} and 21{1,5,5,5,5}, there are 40 contacts. Yet the arrangement 21{3,3,3,3,3,3,3}, which has only 39 contacts, is more efficient since 6 more contacts are nearly made.

In my previous paper [1], the value for $a(10)$ is given as 66°19′. This is in error. A more accurate computation of this angle was made by LACHS [9] in connection with an application in technology. From his data, the angle is 66°08′10″.

TABLE 1

21{3,3,3,3,3,3,3}, a = 45°30′			22{1,4,4,4,4,4,1}, a = 45°01′		
CIRCLE	LATITUDE	LONGITUDE	CIRCLE	LATITUDE	LONGITUDE
A	63°28′42″ N	30°37′51″ W	A	90° N	—
B	35°27′19″ N	29°22′09″ E	B	44°59′00″ N	43°04′46″ E
C	15°39′48″ N	16°42′48″ W	C	22°02′52″ N	4°38′51″ W
D	0°	60° E	D	0°	45°00′00″ E
E	15°39′48″ S	16°42′48″ E	E	22°02′52″ S	4°38′51″ E
F	35°27′19″ S	29°22′09″ W	F	44°59′00″ S	43°04′46″ W
G	63°28′42″ S	30°37′51″ E	G	90° S	—

TABLE 2

Figure or Reference	n	ARRANGEMENT	$a(n)$	$R(n)$	$D(n)$	CONTACTS Total	CONTACTS Per Circle	SOURCE
[3]	19	1,3,3,(6),3,3	47°25′22″	1.243	.802	36	3.79	GOLDBERG
Fig. 1	21	3,3,3,3,3,3,3	45°30′	1.293	.817	39	3.72	GOLDBERG
Fig. 2	21	1,4,4,4,4,4	45°10′	1.302	.805	40	3.81	GOLDBERG
[1]	21	1,5,5,5,5	44°57′	1.308	.798	40	3.81	STROHMAJER
Fig. 4	22	1,4,4,4,4,4,1	45°01′	1.307	.838	44	4.00	GOLDBERG
Fig. 3	22	1,3,3,3,3,3,3,3	44°35′	1.318	.822	42	3.82	ROBINSON
[1]	22	1,5,5,5,5,1	44°24′	1.335	.815	40	3.64	STROHMAJER
Fig. 5	28	4,4,4,4,4,4,4	38°49′	1.505	.796	56	4.00	GOLDBERG
Fig. 6	28	4,4,4,4,4,4,4	38°46′	1.507	.794	56	4.00	GOLDBERG
Fig. 7	28	4,4,4,4,4,4,4	38°36′	1.513	.787	48	3.43	GOLDBERG
[4]	33	3,3, . . . , 3,3	36°15′32″	1.607	.819	69	4.18	GOLDBERG
Fig. 8	44	1,3,3, . . . , 3,3,1	31°53′	1.820	.846	84	3.82	ROBINSON
Fig. 9	48	4,4, . . . , 4,4	30°46′	1.885	.860	120	5.00	ROBINSON
	60	5,5, . . . , 5,5	26°49′	2.181	.818	150	5.00	ROBINSON
	80	5,5, . . . , 5,5	23°17′	2.478	.823	150	3.75	ROBINSON
	110	1,3,3, . . . , 3,3	20°06′	2.866	.844	210	3.82	ROBINSON
	120	5,5, . . . , 5,5	19°20′	2.978	.881	300	5.00	ROBINSON

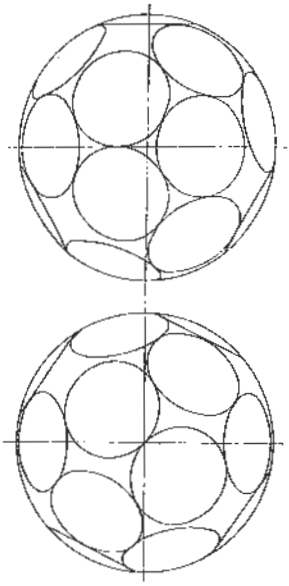

Fig. 1, 21{3,3,3,3,3,3,3}, $a = 45°30'$

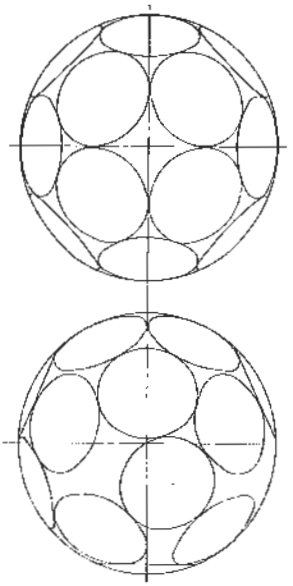

Fig. 2, 21{1,4,4,4,4,4}, $a = 45°10'$

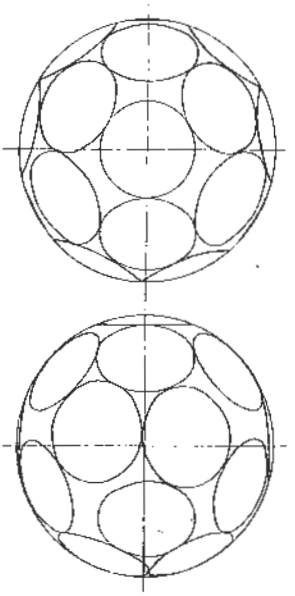

Fig. 3, 22{1,3,3,3,3,3,3,3}, $a = 44°35'$

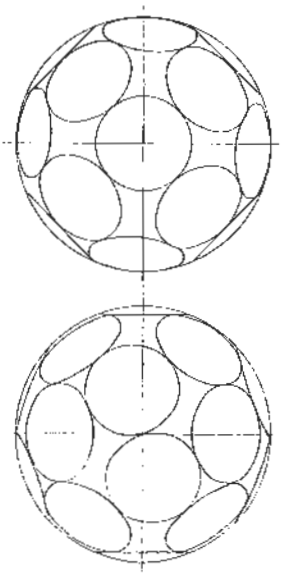

Fig. 4, 22{1,4,4,4,4,4,1,} $a = 45°01'$

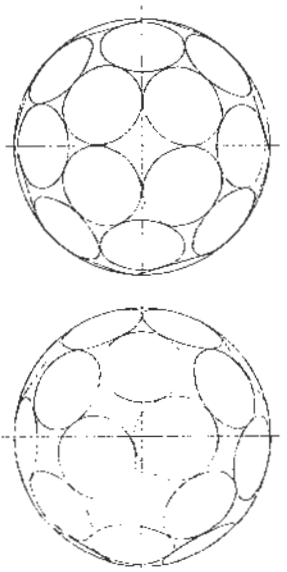

Fig. 5, 28{4,4,4,4,4,4,4,} $a = 38°49'$, Unsym. about equator

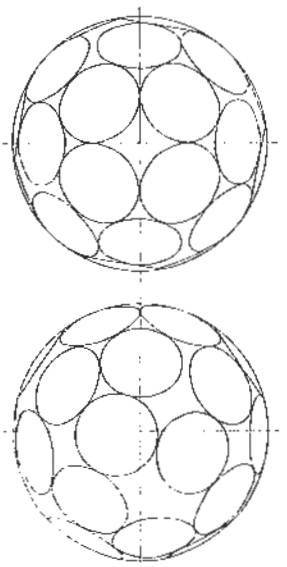

Fig. 6, 28{4,4,4,4,4,4,4} Unsym., $a = 38°46'$

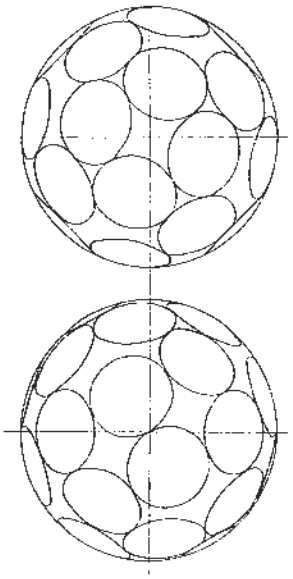

Fig. 7, 28{4,4,4,4,4,4,4}
Sym. about equator, $\alpha = 38°36'$

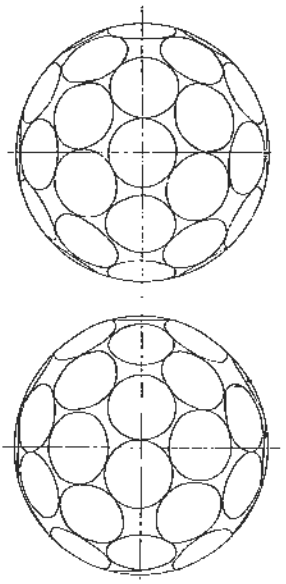

Fig. 8, 44{1,3,3,...,3,3,1}

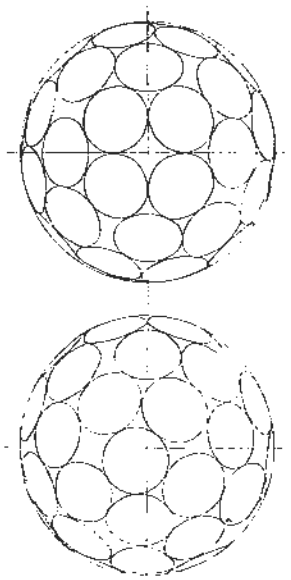

Fig. 9, 48{4,4,...,4,4}

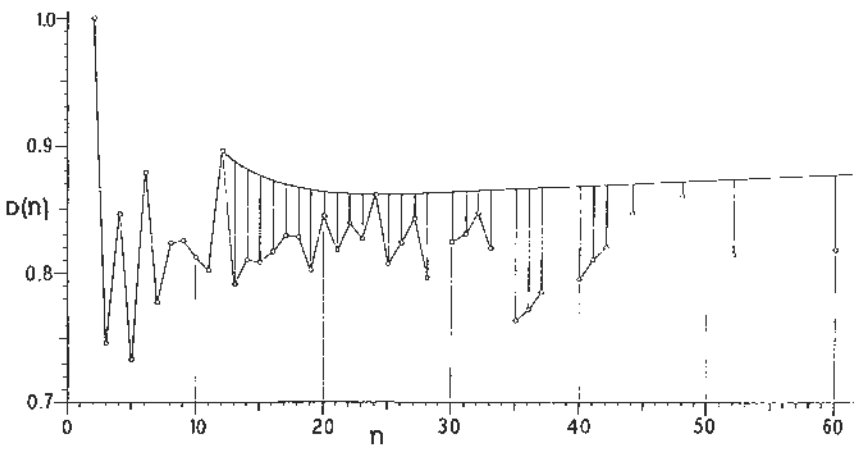

Fig. 10, Graph of density of packing

Bibliography

[1] GOLDBERG, M., Axially symmetric packing of equal circles on a sphere. *Annales Univ. Sci. Budapest*, Sect. Math., **10** (1967), 37–48.

[2] GOLDBERG, M., Viruses and a mathematical problem. *Journal of Molecular Biology*, **24** (1967), 337–338.

[3] GOLDBERG, M., Packing of 19 equal circles on a sphere. *Elem. d. Math.*, **22** (1967), 108–110.

[4] GOLDBERG, M., An improved packing of 33 equal circles on a sphere. *Elem. d. Math.*, **22** (1967), 110–112.

[5] STROHMAJER, J., Über die Verteilung von Punkten auf der Kugel. *Annales Univ. Sci. Budapest*, Sect. Math., **6** (1963), 49–53.

[6] ROBINSON, R. M., Note on some arrangements of points on the sphere. (Private communication).

[7] ROBINSON, R. M., Finite sets of points on a sphere with five nearest neighbors. *Notices of the Amer. Math. Soc.*, **13** (1966), 739.

[8] ROBINSON, R. M., Arrangement of 24 points on a sphere. *Math. Annalen*, **144** (1961), 17–48.

[9] LACHS, G., Optimization of signal waveforms. *IEEE Transactions on Information Theory*, **9** (1963), 95–97.

THE RADICAL OF A CERTAIN INFINITE MATRIX RING

By

A. D. SANDS

The University, Dundee, Scotland

(Received September 26, 1968)

Let R be a ring and I an infinite set. We denote by $M(R)$ the ring of row-finite matrices with rows and columns indexed by I and entries from R; for $\mathbf{m} \in M(R)$ and $i, j \in I$ we denote the ijth entry of $\mathbf{m}$ by $\mathbf{m}(i, j)$. For each $\mathbf{m} \in M(R)$ we denote the subset of I indexing the non-zero columns of $\mathbf{m}$ by $J[\mathbf{m}]$, i.e.

$$J[\mathbf{m}] = \{j \in I \mid \exists i \in I \text{ such that } \mathbf{m}(i, j) \neq 0\}.$$

The for each ideal A of R and each infinite cardinal c we denote by $M(A, c)$ the set of matrices $\mathbf{m} \in M(A)$ such that $J[\mathbf{m}]$ has cardinality less than c. It is readily verified that $M(A, c)$ is an ideal of $M(R)$. If c exceeds the cardinality of the set I then clearly $M(A, c) = M(A)$.

PATTERSON [2], [3] has shown that if J is the Jacobson radical of a ring R then $M(J)$ is the Jacobson radical of $M(R)$ if and only if J is right-vanishing. It is clear that a similar result holds for $M(R, c)$, for $c > \aleph_0$. No general form for the radical of $M(R, c)$, $c > \aleph_0$, is known if J is not right-vanishing. One example of a ring R where the radical is not right-vanishing is the ring P_p of p-adic integers. The radical of P_p is well-known to be the ideal $(p) = pP_p$.

HAIMO* [1] raises the question of the radical of $M(P_p)$.

It is the purpose of this note to show the following

THEOREM. *The radical of $M(P_p, c)$ is $M(pP_p, \aleph_0)$.*

PROOF. For the case $c = \aleph_0$ this follows from the general result of PATTERSON [2] that the radical of $M(R, \aleph_0)$ is $M(J, \aleph_0)$, for any ring R with radical J. Thus we may assume that $c > \aleph_0$.

HAIMO [1] denotes $M(pP_p, \aleph_0)$ by N and shows that N is a quasi-regular ideal and so is contained in the radical. (This follows also from Patterson's

* Professor HAIMO has informed me in a private communication that he has proved this result, by a different method. His proof uses only the fact that the radical of the ring is an integral domain.

general result.) Clearly N is the intersection of the ideals $M(pP_p, c)$ and $M(P_p, \aleph_0)$. We show that each of these is a primitive ideal and from this the result follows, for N is then seen to be a semi-primitive ideal and thus contains the radical.

Since pP_p is a primitive ideal of P_p it follows from Theorem 3 of SANDS [4] that $M(pP_p)$ is a primitive ideal of $M(P_p)$ and, by a similar proof, that $M(pP_p, c)$ is a primitive ideal of $M(P_p, c)$.

We show that $M(P_p, \aleph_0)$ is a left primitive ideal of $M(P_p, c)$, $c > \aleph_0$, by obtaining it as the annihilator of an irreducible left $M(P_p, c)$-module. We assume that all p-adic integers x are expressed in standard form $\Sigma x_r p^r$, with $0 \leq x_r < p$. For $x, y \in P_p$ we say that x divides y if there exists $z \in P_p$ such that $y = xz$. Since P_p is an integral domain, z must be unique. Let U be the set of (row) vectors indexed by I with entries in P_p; for $\mathbf{u} \in U$ and $i \in I$ the ith entry of $\mathbf{u}$ is denoted by $\mathbf{u}(i)$. Clearly U forms an abelian group with respect to addition, where addition of vectors is defined component-wise in the usual way. For $\mathbf{u} \in U$ and n a positive integer we define $\mathbf{u}[n]$ by

$$\mathbf{u}[n] = \{i \in I \mid p^n \text{ does not divide } \mathbf{u}(i)\}.$$

Let V denote the subset of U consisting of all vectors $\mathbf{v}$ such that $\mathbf{v}[n]$ is finite for every positive integer n. For $\mathbf{u} \in U$ we denote by $S(\mathbf{u})$ the support of $\mathbf{u}$, i.e.

$$S(\mathbf{u}) = \{i \in I \mid \mathbf{u}(i) \neq 0\}.$$

For $\mathbf{v} \in V$, $S(\mathbf{v}) = \cup_n \mathbf{v}[n]$, and thus $S(\mathbf{v})$ is a countable union of finite sets and so is a finite or countable subset of I.

It is easily verified that V is a subgroup of U. We define a mapping from $V \times M(P_p, c)$ to V making V into an $M(P_p, c)$-module. Let $\mathbf{v} \in V$ and let $\mathbf{m}_j$ be the jth column of a matrix $\mathbf{m}$ of $M(P_p, c)$. We define $\mathbf{v}\mathbf{m}_j$ to be $\Sigma x_n p^n$ where, for each n, x_n is the coefficient of p^n in $\sum_i \mathbf{v}(i)\mathbf{m}(i, j)$, where the summation is taken over the finite set $\mathbf{v}[n+1]$. It is clear that x_n is not altered by replacing $\mathbf{v}[n+1]$ by any finite subset of I containing $\mathbf{v}[n+1]$. Then $\mathbf{v}\mathbf{m}$ is the vector given by $(\mathbf{v}\mathbf{m})(j) = \mathbf{v}\mathbf{m}_j$, for each $j \in I$. Clearly $\mathbf{v}\mathbf{m} \in U$. In fact $\mathbf{v}\mathbf{m} \in V$. Let n be a positive integer and let $(\mathbf{v}, \mathbf{m})[n]$ be defined by

$$(\mathbf{v}, \mathbf{m})[n] = \{j \in J \mid \mathbf{m}(i, j) \neq 0 \text{ for some } i \in \mathbf{v}[n]\}.$$

Since $\mathbf{m}$ is row-finite and $\mathbf{v}[n]$ is finite it follows that $(\mathbf{v}, \mathbf{m})[n]$ is a finite union of finite sets and so is a finite subset of I. If $j \in (\mathbf{v}, \mathbf{m})[n]$ then $\sum_i \mathbf{v}(i)\mathbf{m}(i, j)$, $i \in \mathbf{v}[n]$, consists of terms in which $\mathbf{m}(i, j) = 0$ and thus in $\mathbf{v}\mathbf{m}_j = \Sigma x_k p^k$, we have $x_r = 0$ for $r < n$. Hence p^n divides $\mathbf{v}\mathbf{m}_j$. Therefore $(\mathbf{v}\mathbf{m})[n] \subset (\mathbf{v}, \mathbf{m})[n]$, and this set is finite for each positive integer n. Hence $\mathbf{v}\mathbf{m} \in V$.

It is readily verified that, for $\mathbf{v}_1, \mathbf{v}_2 \in V$ and $\mathbf{m}_1, \mathbf{m}_2 \in M(P_p, c)$,

$$(\mathbf{v}_1 + \mathbf{v}_2)\mathbf{m}_1 = \mathbf{v}_1\mathbf{m}_1 + \mathbf{v}_2\mathbf{m}_1, \quad \mathbf{v}_1(\mathbf{m}_1 + \mathbf{m}_2) = \mathbf{v}_1\mathbf{m}_1 + \mathbf{v}_1\mathbf{m}_2.$$

Let $c(n, i)$ and $d(n, i)$ denote the coefficient of p^n in the ith component of $(\mathbf{v}_1\mathbf{m}_1)\mathbf{m}_2$ and $\mathbf{v}_1(\mathbf{m}_1\mathbf{m}_2)$ respectively. Then $c(n, i)$ is the coefficient of p^n in $\sum_k (\mathbf{v}_1\mathbf{m}_1)(k)\mathbf{m}_2(k, i)$, where the summation may be taken over k in $(\mathbf{v}_1, \mathbf{m}_1)[n+1]$, since this is a finite set containing $(\mathbf{v}_1\mathbf{m}_1)[n+1]$. $d(n, i)$ is the coefficient of p^n in $\sum_l \mathbf{v}_1(l)(\mathbf{m}_1\mathbf{m}_2)(l, i)$, where the summation is taken over l in $\mathbf{v}_1[n+1]$.

Now $(\mathbf{m}_1\mathbf{m}_2)(l, i) = \sum_k \mathbf{m}_1(l, k)\mathbf{m}_2(k, i)$, where, for each $l \in \mathbf{v}_1[n+1]$, the summation is taken over k belonging to the finite set such that $\mathbf{m}_1(l, k) \neq 0$ and so may be taken over the possibly larger finite set $(\mathbf{v}_1, \mathbf{m}_1)[n+1]$. Thus $d(n, i)$ is the coefficient of p^n in $\sum_l \mathbf{v}_1(l) \sum_k \mathbf{m}_1(l, k)\mathbf{m}_2(k, i)$ where l runs through $\mathbf{v}_1[n+1]$ and k runs through $(\mathbf{v}_1, \mathbf{m}_1)[n+1]$. Since these summations are finite we may rearrange terms to obtain $\sum_k (\sum_l \mathbf{v}_1(l)\mathbf{m}_1(l, k))\mathbf{m}_2(k, i) = \sum_k (\mathbf{v}_1\mathbf{m}_1)(k)\mathbf{m}_2(k, i)$. Hence $d(n, i) = c(n, i)$. Since this is true for all n and i it follows that $(\mathbf{v}_1\mathbf{m}_1)(\mathbf{m}_2) = \mathbf{v}_1(\mathbf{m}_1\mathbf{m}_2)$. Therefore V is a left $M(P_p, c)$-module.

V is not irreducible. Let W be defined by $W = \{\mathbf{v} \in V \mid S(\mathbf{v}) \text{ is finite}\}$. Clearly W is a subgroup of V. Let $\mathbf{w} \in W$ and $\mathbf{m} \in M(P_p, c)$. Since $S(\mathbf{w})$ is finite it follows that $\mathbf{m}[S(\mathbf{w})] = \{j \in I \mid \mathbf{m}(i, j) \neq 0 \text{ for some } i \in S(\mathbf{w})\}$ is finite. Clearly $S(\mathbf{wm}) \subset \mathbf{m}[S(\mathbf{w})]$. Therefore $\mathbf{wm} \in W$ and W is a submodule of V.

We shall now show that W is a maximal submodule of V. Let $\mathbf{v} \in V$, but suppose that $\mathbf{v} \notin W$. Then $S(\mathbf{v})$ is not finite. Since each set $\mathbf{v}[n]$ is finite it follows that there exists an infinite increasing sequence of integers $n_1 < n_2 < \ldots < n_p < \ldots$ and an infinite subsequence $i_1, i_2, \ldots, i_k, \ldots$ of elements of I such that, for each k, p^{n_k} divides $\mathbf{v}(i_k)$, but p^{n_k+1} does not divide $\mathbf{v}(i_k)$. Then if $x \in P_p$ and p^{n_k} divides x, it follows that $\mathbf{v}(i_k)$ divides x.

Let $\mathbf{u} \in V$. For each positive integer n let $I_n = \mathbf{u}[n+1] \setminus \mathbf{u}[n]$. For each positive integer k, let $J_k = \cup I_n$, where the union is taken over n such that $n_k \leq n < n_{k+1}$. Then J_k is finite. For each $i \in J_k$, p^{n_k} divides $\mathbf{u}(i)$ and so $\mathbf{v}(i_k)$ divides $\mathbf{u}(i)$. Let $\mathbf{v}(i_k)x(k, i) = \mathbf{u}(i)$. Let the matrix $\mathbf{m}$ be defined by $\mathbf{m}(i_k, i) = x(k, i)$ for $i \in J_k$, $k = 1, 2, \ldots$ and $\mathbf{m}(k, i) = 0$, otherwise. Since J_k is finite, $\mathbf{m}$ is row finite. Since $\mathbf{u}(i) = 0$ implies $x(k, i) = 0$ and $S(\mathbf{u})$ is finite or countable it follows that $\mathbf{m} \in M(P_p, c)$, for $c > \aleph_0$. Then $(\mathbf{u} - \mathbf{vm})(i)$ is zero except for a finite number of positions $i \in \mathbf{u}[n_1]$. Hence $\mathbf{u} - \mathbf{vm} \in W$. Therefore W and $\mathbf{v}$ together generate V and so W is a maximal submodule of V.

Thus V/W is an irreducible $M(P_p, c)$-submodule. The annihilator of V/W is the set of matrices $\mathbf{m}$ such that $V\mathbf{m} \subset W$. Since P_p is an integral domain it is clear that $\mathbf{m}$ belongs to the annihilator of V/W if and only if $\mathbf{m}$ has only a finite number of non-zero columns. Thus the annihilator of V/W is $M(P_p, \aleph_0)$.

It follows that $M(P_p, \aleph_0)$ is a primitive ideal and this completes the proof that the radical of $M(P_p, c)$ is $N = M(pP_p, \aleph_0)$.

References

[1] F. Haimo, Endomorphism radicals which characterize some divisible groups, *Annales Univ. Sci. Budapest* Sect. Math., **10** (1967), 25–29.

[2] E. M. Patterson, On the radicals of certain rings of infinite matrices, *Proceedings of Royal Soc. Edinburgh*, Section A, **65** (1957–61), 263–271.

[3] E. M. Patterson, On the radicals of rings of row-finite matrices, *Proceedings of Royal Soc. Edinburgh*, Section A, **66** (1961–62), 42–46.

[4] A. D. Sands, Primitive rings of infinite matrices, *Proceedings Edin. Math. Soc.*, **14** (II) (1964), 47–53.

ON THE EQUATION $\cos\alpha_1+\cos\alpha_2+\cos\alpha_3+\cos\alpha_4=0$

By

Ł. WŁODARSKI
(Łódź)

(Received January 29, 1969)

F. KÁRTESZI in connection with his paper [3] put forward the question to find all solutions of the equation

$$\cos\alpha_1+\cos\alpha_2+\cos\alpha_3+\cos\alpha_4=0 \tag{1}$$

in α_i commensurable with π. One may assume without loss of generality that

$$0<\alpha_i<\pi \qquad (1\leq i\leq 4). \tag{2}$$

There exist two infinite families of solutions

$$\{\beta,\ \gamma,\ \pi-\gamma,\ \pi-\beta\} \qquad \left(0\leq\beta\leq\gamma\leq\frac{1}{2}\pi\right), \tag{3}$$

$$\left\{\delta,\ \frac{2}{3}\pi-\delta,\ \frac{2}{3}\pi+\delta,\ \frac{1}{2}\pi\right\} \qquad \left(0\leq\delta\leq\frac{1}{3}\pi\right) \tag{4}$$

and we shall prove that besides there are only 10 solutions (by a solution we mean an unordered quadruple $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$).

THEOREM. *If α_i commensurable with π satisfy* (1) *and* (2) *then $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ either belongs to family* (3) *or* (4) *or is one of the following quadruples*

$$\left\{\frac{2}{5}\pi,\ \frac{1}{2}\pi,\ \frac{4}{5}\pi,\ \frac{1}{3}\pi\right\}, \qquad \left\{\frac{1}{5}\pi,\ \frac{1}{2}\pi,\ \frac{3}{5}\pi,\ \frac{2}{3}\pi\right\}, \tag{5}$$

$$\left\{\frac{1}{5}\pi,\ \frac{3}{5}\pi,\ \frac{1}{3}\pi\right\}, \qquad \left\{0,\ \frac{2}{5}\pi,\ \frac{4}{5}\pi,\ \frac{2}{3}\pi\right\}, \tag{6}$$

$$\left\{\frac{2}{5}\pi,\ \frac{7}{15}\pi,\ \frac{13}{15}\pi,\ \frac{1}{3}\pi\right\}, \qquad \left\{\frac{2}{15}\pi,\ \frac{8}{15}\pi,\ \frac{3}{5}\pi,\ \frac{2}{3}\pi\right\}, \tag{7}$$

$$\left\{\frac{1}{15}\pi,\ \frac{11}{15}\pi,\ \frac{4}{5}\pi,\ \frac{1}{3}\pi\right\}, \qquad \left\{\frac{1}{5}\pi,\ \frac{4}{15}\pi,\ \frac{14}{15}\pi,\ \frac{2}{3}\pi\right\}, \tag{8}$$

$$\left\{\frac{2}{7}\pi,\ \frac{4}{7}\pi,\ \frac{6}{7}\pi,\ \frac{1}{3}\pi\right\}, \qquad \left\{\frac{1}{7}\pi,\ \frac{3}{7}\pi,\ \frac{5}{7}\pi,\ \frac{2}{3}\pi\right\}. \tag{9}$$

COROLLARY. If α_i commensurable with π satisfy (2) and the equation $\cos\alpha_1+\cos\alpha_2+\cos\alpha_3=0$, then $\{\alpha_1\ \alpha_2,\ \alpha_3\}$ either belongs to one of the families

$$\left\{\beta,\ \pi-\beta,\ \frac{1}{2}\pi\right\}\quad (0\leq\beta\leq\pi),\qquad \left\{\delta,\ \frac{2}{3}\pi-\delta,\ \frac{2}{3}\pi+\delta\right\}\quad \left(0\leq\delta\leq\frac{1}{3}\pi\right)$$

or is one of the triples

$$\left\{\frac{2}{5}\pi,\ \frac{4}{5}\pi,\ \frac{1}{3}\pi\right\},\qquad \left\{\frac{1}{5}\pi,\ \frac{3}{5}\pi,\ \frac{2}{3}\pi\right\}.$$

This corollary is known and was proved by W. J. R. CROSBY [1] however his argument is based on a different idea than the following proof.

LEMMA 1. If $\sum_{i=1}^{4} x_i=\sum_{i=1}^{4} x_i^3=0$, then $(x_1+x_2)(x_1+x_3)(x_2+x_3)=0$.

PROOF. We have

$$3(x_1+x_2)(x_1+x_3)(x_2+x_3)=(x_1+x_2+x_3)^3-x_1^3-x_2^3-x_3^3=-x_4^3+x_4^3=0.$$

LEMMA 2. If (1) holds,

$$\alpha_i=\frac{n_i}{N}2\pi,\quad n_i \text{ integers } (1\leq i\leq 4), \tag{10}$$

N and r are integers and $(r, N)=1$ then

$$\sum_{i=1}^{4}\cos r\alpha_i=0. \tag{11}$$

PROOF. Since $(r, N)=1$, $\cos\frac{2\pi r}{N}$ is conjugate to $\cos\frac{2\pi}{N}$. On the other hand, by (10)

$$\cos\alpha_i=T_{n_i}\left(\cos\frac{2\pi}{N}\right),\quad \cos r\alpha_i=T_{n_i}\left(\cos\frac{2\pi r}{N}\right)\qquad (1\leq i\leq 4),$$

where T_n as the n-th Chebyshev polynomial has integral coefficients. Therefore $\sum_{i=1}^{4}\cos\alpha_i$ is conjugate to $\sum_{i=1}^{4}\cos r\alpha_i$ and (11) follows from (1).

LEMMA 3. If

$$\sum_{i=1}^{3}\cos\beta_i=\sum_{i=1}^{3}\cos 3\beta_i=\sum_{i=1}^{3}\cos 9\beta_i=-\frac{1}{2}\varepsilon\qquad (\varepsilon=\pm 1) \tag{12}$$

and

$$0\leq\beta_i\leq\pi\qquad (0\leq i\leq 3)$$

then $\left\{\beta_1,\beta_2,\beta_3,\left|\varepsilon\frac{\pi}{2}-\frac{\pi}{6}\right|\right\}$ is one of quadruples (5), (6) or (9).

PROOF. Let

$$\varepsilon \cos \beta_i = x_i (1 \leq i \leq 3), \quad x_1x_2x_3 = p, \quad x_1x_2+x_1x_3+x_2x_3 = q, \quad x_1^n+x_2^n+x_3^n = s_n.$$

Since

$$\cos 3\beta = 4\cos^3\beta - 3\cos\beta, \ \cos 9\beta = 4\cos^3 3\beta - 3\cos^3\beta \tag{13}$$

it follows from (12) that

$$s_1 = -\frac{1}{2}, \qquad s_3 = \frac{1}{4}\left(-\frac{1}{2}+3s_1\right) = -\frac{1}{2}, \tag{14}$$

$$\sum_{i=1}^{3}(4x_i^3-3x_i)^3 = \frac{1}{4}\left(-\frac{1}{2}+3\sum_{i=1}^{3}(4x_i^3-3x_i)\right) = -\frac{1}{2}. \tag{15}$$

On the other hand,

$$\sum_{i=1}^{3}(4x_i^3-3x_i)^3 = 64s_9-144s_7+108s_5-27s_3$$

and we have (see [2] p. 311–314 a)

$$\begin{aligned} -s_3 &= -3p+3qs_1-s_1^3, \\ -s_5 &= 5pq-5ps_1^2-5q^2s_1+5qs_1^3-s_1^5, \\ -s_7 &= -7p^2s_1-7pq^2+21pqs_1^2-7ps_1^4+7q^3s_1-14q^2s_1^3+7qs_1^5-s_1^7, \\ -s_9 &= -3p^3+27p^2qs_1+9pq^3-18p^2s_1^3-54pq^2s_1^2+45pqs_1^6-9ps_1^6-9p^4s_1+ \\ &\quad +30q^3s_1^3-27q^2s_1^5+9qs_1^7-s_1^9. \end{aligned} \tag{16}$$

It follows by (14) and (16) that

$$q = -2p-\frac{1}{4}, \tag{17}$$

hence (by a rather tedious computation)

$$\sum_{i=1}^{3}(4x_i^3-3x_i)^3 = -576p^3+216p^2 = 18p-\frac{1}{2}.$$

Now we obtain from (15)

$$576p^3-216p^2+18p = 0,$$

hence $p = 0, \frac{1}{4}$ or $\frac{1}{8}$ and by (14) and (17)

$$8(x-x_1)(x-x_2)(x-x_3) = f(x) \text{ or } g(x) \text{ or } h(x), \text{ where}$$

$$f(x) = 8x^3+4x^2-2x = 2x\left(x-\frac{-1+\sqrt{5}}{4}\right)\left(x-\frac{-1-\sqrt{5}}{4}\right),$$

$$g(x) = 8x^3+4x^2-6x-2 = 2(x+1)\left(x-\frac{1+\sqrt{5}}{4}\right)\left(x-\frac{1-\sqrt{5}}{4}\right),$$

$$h(x) = 8x^3+4x^2-4x-1.$$

The zeros of f and g are $\cos\frac{1}{2}\pi$, $\cos\frac{2}{5}\pi$, $\cos\frac{4}{5}\pi$ and $\cos\pi$, $\cos\frac{1}{5}\pi$, $\cos\frac{3}{5}\pi$, respectively. The zeros of $h(x)$ are $\cos\frac{2}{7}\pi$, $\cos\frac{4}{7}\pi$, $\cos\frac{6}{7}\pi$ since

$$x^3 h\left(\frac{x+x^{-1}}{2}\right) = \frac{x^7-1}{x-1}.$$

On the other hand, these zeros are $\varepsilon\cos\beta_1$, $\varepsilon\cos\beta_2$, $\varepsilon\cos\beta_3$ thus $\left\{\beta_1, \beta_2, \beta_3, \left|\varepsilon\frac{\pi}{2}-\frac{\pi}{6}\right|\right\}$ is for $\varepsilon = 1$ (5_1), (6_1) or (7_1), for $\varepsilon = -1$, (5_2), (6_2) or (7_2), q.e.d.

Proof of the Theorem. Represent α_i in the form (10), where

$$(N, n_1, n_2, n_3, n_4) = 1. \tag{18}$$

Suppose first that $N \not\equiv 0 \bmod 3$. Then by Lemma 2 with $r = 3$ and by (13)

$$\sum_{i=1}^{4}\cos 3\alpha_i = 4\sum_{i=1}^{4}\cos^3\alpha_i - 3\sum_{i=1}^{4}\cos\alpha_i = 0,$$

thus by (1)

$$\sum_{i=1}^{4}\cos\alpha_i = \sum_{i=1}^{4}\cos^3\alpha_i = 0.$$

It follows by Lemma 1 that

$$(\cos\alpha_1+\cos\alpha_2)(\cos\alpha_1+\cos\alpha_3)(\cos\alpha_2+\cos\alpha_3) = 0$$

and by (2), $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ belongs to (3).
Suppose next $N \equiv 0 \bmod 3$ and replace (2) by a less stringent assumption

$$0 \le |\alpha_i| \le \pi \qquad (1 \le i \le 4). \tag{19}$$

Then we have to prove that $A = \{|\alpha_1|, |\alpha_2|, |\alpha_3|, |\alpha_4|\}$ is one of quadruples (3)–(9) but since $\cos\alpha = \cos(-\alpha)$ we may suppose without loss of generality that

$$n_i \equiv 0 \bmod 3 \ (1 \le i \le k),\ n_i \equiv 1 \bmod 3 \ (k < i \le 4). \tag{20}$$

We have by (18) $0 \le k \le 3$ and by (10)

$$\cos\frac{N}{3}\alpha_i = 1, \qquad \sin\frac{N}{3}\alpha_i = 0 \qquad (1 \le i \le k), \tag{21}$$

$$\cos\frac{N}{3}\alpha_i=-\frac{1}{2},\ \sin\frac{N}{3}\alpha_i=\frac{\sqrt{3}}{2}\qquad(k<i\leq 4). \tag{22}$$

We distinguish two cases $N\equiv 0 \bmod 9$ and $N\not\equiv 0 \bmod 9$.

1. Case $N\equiv 0 \bmod 9$. We apply Lemma 2 with $r=\frac{N}{3}\pm 1$ and get

$$\sum_{i=1}^{4}\cos\left(\frac{N}{3}\pm 1\right)\alpha_i=0,$$

whence by addition and subtraction

$$2\sum_{i=1}^{4}\cos\frac{N}{3}\alpha_i\cos\alpha_i=2\sum_{i=1}^{4}\sin\frac{N}{3}\alpha_i\sin\alpha_i=0$$

and by (21), (22)

$$2\sum_{i=1}^{k}\cos\alpha_i-\sum_{i=k+1}^{4}\cos\alpha_i=0, \tag{23}$$

$$\sum_{i=k+1}^{4}\sin\alpha_i=0. \tag{24}$$

Consider successively $k=0, 1, 2, 3$.

a) $k=0$. It follows from (23), (24) that

$$\cos\alpha_1+\cos\alpha_2=-\cos\alpha_3-\cos\alpha_4,$$
$$\sin\alpha_1+\sin\alpha_2=-\sin\alpha_3-\sin\alpha_4.$$

If $\cos\alpha_1+\cos\alpha_2=\cos\alpha_3+\cos\alpha_4=0$, A in virtue of (19) belongs to (3). Otherwise it follows by division that

$$\operatorname{tg}\frac{1}{2}(\alpha_1+\alpha_2)=\operatorname{tg}\frac{1}{2}(\alpha_3+\alpha_4),$$

thus $\alpha_1+\alpha_2\equiv\alpha_3+\alpha_4 \bmod 2\pi$. In view of symmetry $\alpha_1+\alpha_3\equiv\alpha_2+\alpha_4 \bmod 2\pi$, hence $\alpha_1\equiv\alpha_2\equiv\alpha_3\equiv\alpha_4 \bmod 2\pi$ and $4\cos\alpha_1=4\sin\alpha_1=0$, which is impossible.

b) $k=1$. It follows from (1), (23), (24) that

$$\cos\alpha_1=0,$$
$$\cos\alpha_2+\cos\alpha_3=-\cos\alpha_4,$$
$$\sin\alpha_2+\sin\alpha_3=-\sin\alpha_4.$$

and since by (10) and (20) $\cos\alpha_4\neq 0$, we get by division

$$\operatorname{tg}\frac{1}{2}(\alpha_2+\alpha_3)=\operatorname{tg}\alpha_4,$$

$\alpha_2+\alpha_3\equiv 2\alpha_4 \bmod 2\pi$. In view of symmetry $\alpha_2+\alpha_4\equiv 2\alpha_3 \bmod 2\pi$, hence

$$3\alpha_2\equiv 3\alpha_3\equiv 3\alpha_4 \bmod 2\pi.$$

In view of (19) we have $\{\alpha_1\} = \frac{1}{2}\pi$ and $\{\alpha_2, \alpha_3\} = \left\{\alpha_2+\frac{2\pi}{3}, \alpha_2+\frac{4\pi}{3}\right\}$ $\left\{-\pi < \alpha_2 < -\frac{\pi}{3}\right\}$ or $\left\{\alpha_2-\frac{2\pi}{3}, \alpha_2+\frac{2\pi}{3}\right\}$ $\left\{-\frac{\pi}{3} < \alpha_2 < \frac{\pi}{3}\right\}$ or $\left\{\alpha_2-\frac{4\pi}{3}, \alpha_2-\frac{2\pi}{3}\right\}$ $\left\{\frac{\pi}{3} < \alpha_2 \leq \pi\right\}$, thus A belongs to (4).

c) $k = 2$. It follows from (1) and (23) that

$$\cos\alpha_1+\cos\alpha_2 = \cos\alpha_3+\cos\alpha_4 = 0$$

and A belongs to (3).

d) $k=3$. It follows from (1) and (23) that $\cos\alpha_1=0$ which is incompatible with (24).

2. Case $N\neq 0 \bmod 9$. Changing α_i to $-\alpha_i$ if need be, we can assume that

$$N \equiv -3 \bmod 9. \tag{25}$$

We apply Lemma 2 with $r=\frac{N}{3}\pm 3$ and $r=\frac{N}{3}\pm 9$. We get, like before (23), (24) the equations

$$2\sum_{i=1}^{k}\cos 3\alpha_i - \sum_{i=k+1}^{4}\cos 3\alpha_i = 0, \tag{26}$$

$$2\sum_{i=1}^{k}\cos 9\alpha_i - \sum_{i=k+1}^{4}\cos 9\alpha_i = 0, \tag{27}$$

$$\sum_{i=k+1}^{4}\sin 3\alpha_i = \sum_{i=k+1}^{4}\sin 9\alpha_i = 0.$$

Since $\sin 9\alpha_i = 3\sin\alpha_i - 4\sin^3 3\alpha_i$, it follows

$$\sum_{i=k+1}^{4}\sin 3\alpha_i = \sum_{i=k+1}^{4}\sin^3 3\alpha_i = 0. \tag{28}$$

Consider successively $k = 0, 1, 2, 3$.

a) $k = 0$. It follows from (1), (13) and (26) that

$$\sum_{i=1}^{4}\cos\alpha_i = \sum_{i=1}^{4}\cos^3\alpha_i = 0,$$

thus by Lemma 1

$$(\cos\alpha_1+\cos\alpha_2)(\cos\alpha_1+\cos\alpha_3)(\cos\alpha_2+\cos\alpha_3) = 0$$

and A belongs to (3).

b) $k = 1$. By (28) and Lemma 1

$$\sin 3\alpha_2 = \sin 3\alpha_3 + \sin 3\alpha_4 = 0$$

or another equality holds obtainable from the above by a permutation of $\alpha_2, \alpha_3, \alpha_4$. Disregarding the last possibility since we are interested only in the triple $\{\alpha_2, \alpha_3, \alpha_4\}$ we get

$$3\alpha_2 = 0 \bmod \pi \tag{29}$$

and either

$$3(\alpha_3-\alpha_1)\equiv\pi \bmod 2\pi \tag{30}$$

or

$$3(\alpha_3+\alpha_1)\equiv 0 \bmod 2\pi. \tag{31}$$

On the other hand, by (10) and (20)

$$\frac{N}{3}\alpha_2\equiv\frac{N}{3}\alpha_3\equiv\frac{N}{3}\alpha_4\equiv\frac{2}{3}\pi \bmod 2\pi, \tag{32}$$

$$\frac{N}{3}(\alpha_3-\alpha_1)\equiv 0 \bmod 2\pi, \tag{33}$$

$$\frac{N}{3}(\alpha_3+\alpha_1)\equiv\frac{4}{3}\pi \bmod 2\pi. \tag{34}$$

(25), (29) and (32) imply $\alpha_2\equiv\frac{1}{3}\pi \bmod 2\pi$, hence by (19)

$$\alpha_2=-\frac{\pi}{6}+\varepsilon\frac{\pi}{2}\qquad(\varepsilon=\pm 1). \tag{35}$$

(30) and (33) imply $\alpha_3-\alpha_1\equiv\pi \bmod 2\pi$, hence by (19) A belongs to (3).
(25), (31) and (34) imply $\alpha_3+\alpha_1\equiv\frac{2}{3}\pi \bmod 2\pi$, hence by (19)

$$\alpha_3+\alpha_1=-\frac{\pi}{3}+\eta\pi\qquad(\eta=\pm 1). \tag{36}$$

It follows that

$$\cos\alpha_3+\cos\alpha_1=2\cos\frac{1}{2}(\alpha_3+\alpha_1)\cos\frac{1}{2}(\alpha_3-\alpha_1)=\eta\cos\frac{1}{2}(\alpha_3-\alpha_1) \tag{37}$$

$$\cos 3\alpha_3+\cos 3\alpha_1=2\cos\frac{3}{2}(\alpha_3+\alpha_1)\cos\frac{3}{2}(\alpha_3-\alpha_1)=-2\eta\cos\frac{3}{2}(\alpha_3-\alpha_1), \tag{38}$$

$$\cos 9\alpha_3+\cos 9\alpha_1=2\cos\frac{9}{2}(\alpha_3+\alpha_1)\cos\frac{9}{2}(\alpha_3-\alpha_1)=-2\eta\cos\frac{9}{2}(\alpha_3-\alpha_1). \tag{39}$$

After the substitution of (35) and (37)–(39) into (1), (26) and (27) we obtain

$$\cos\alpha_1+\eta\cos\frac{1}{2}(\alpha_3-\alpha_1)+\frac{1}{2}\varepsilon=0,$$

$$2\cos 3\alpha_1+2\eta\cos\frac{3}{2}(\alpha_3-\alpha_1)+\varepsilon=0,$$

$$2\cos 9\alpha_1+2\eta\cos\frac{9}{2}(\alpha_3-\alpha_1)+\varepsilon=0.$$

Let now

$$\beta_1 = |\alpha_1|, \quad \beta_2 = \frac{\eta}{2}|\alpha_3-\alpha_4| + \frac{\pi}{2}(1-\eta), \quad \beta_3 = \frac{\pi}{2}(1-\varepsilon). \tag{40}$$

We get

$$\sum_{i=1}^{3} \cos\beta_i = \sum_{i=1}^{3} \cos 3\beta_i = \sum_{i=1}^{3} \cos 9\beta_i = -\frac{1}{2}\varepsilon$$

and besides by (19) and (36) $0 \leq \beta_i \leq \pi$ $(1 \leq i \leq 3)$,

$$\eta = \operatorname{sgn}\left(\frac{2}{3}\pi - \beta_2\right). \tag{41}$$

By Lemma 3, $\left\{\beta_1, \beta_2, \beta_3, \left|\varepsilon\frac{\pi}{2} - \frac{\pi}{6}\right|\right\}$ is one of quadruples (5), (6) or (9). However the quadruples (5) and (9) do not contain a multiple of π, thus either $\varepsilon = 1$ and $\{\beta_1, \beta_2\} = \left\{\frac{2}{5}\pi, \frac{4}{5}\pi\right\}$ or $\varepsilon = -1$ and $\{\beta_1, \beta_2\} = \left\{\frac{1}{5}\pi, \frac{3}{5}\pi\right\}$.
By (35), (36), (40) and (41)

$$\{|\alpha_1|, \alpha_2, \alpha_3, \alpha_4\} = \left\{\beta_1, -\frac{\pi}{6} + \varepsilon\frac{\pi}{2}, \frac{1}{3}\pi - \beta_2, \beta_2 - \frac{2}{3}\pi - \pi\operatorname{sgn}\left(\beta_2 - \frac{2}{3}\pi\right)\right\},$$

thus wet get four possibilities

$$\{|\alpha_1|, \alpha_2, \alpha_3, \alpha_4\} = \left\{\frac{2}{5}\pi, \frac{1}{3}\pi, -\frac{7}{15}\pi, -\frac{13}{15}\pi\right\}, \quad \left\{\frac{4}{5}\pi, \frac{1}{3}\pi, -\frac{1}{15}\pi, \frac{11}{15}\pi\right\},$$

$$\left\{\frac{1}{5}\pi, \frac{2}{3}\pi, -\frac{4}{15}\pi, \frac{14}{15}\pi\right\}, \quad \left\{\frac{3}{5}\pi, -\frac{2}{3}\pi, \frac{2}{15}\pi, \frac{8}{15}\pi\right\}$$

which correspond to (7_1), (8_1), (7_2) and (8_2), respectively.

c) $k = 2$. By (28) $\sin 3\alpha_3 \mid \sin 3\alpha_4 = 0$, hence (30) or (31) and like before either A belongs to (3) or (36) holds. Using (37) and (38) we get from (1) and (26)

$$\cos\alpha_1 + \cos\alpha_2 + \eta\cos\frac{1}{2}(\alpha_3 - \alpha_4) = 0,$$

$$2\cos 3\alpha_1 + 2\cos 3\alpha_2 + 2\eta\cos\frac{3}{2}(\alpha_3 - \alpha_4) = 0,$$

hence by (13) and Lemma 1

$$(\cos\alpha_1 + \cos\alpha_2)\left(\cos\alpha_1 + \eta\cos\frac{1}{2}(\alpha_3 - \alpha_4)\right)\left(\cos\alpha_2 + \eta\cos\frac{1}{2}(\alpha_3 - \alpha_4)\right) = 0.$$

If $\cos\alpha_1 + \cos\alpha_2 = 0$, A belongs to (3), otherwise we can assume in view of symmetry that

$$\cos\alpha_1 = \cos\alpha_2 + \eta\cos\frac{1}{2}(\alpha_3-\alpha_1) = 0.$$

Hence by (19)

$$|\alpha_1| = \frac{1}{2}\pi, \quad \left|\frac{1}{2}(\alpha_3-\alpha_1)\right| = \left|\frac{\pi}{2}(1+\eta)-|\alpha_2|\right|$$

and by (36)

$$\{\alpha_3, \alpha_4\} = \left\{|\alpha_2|-\frac{2}{3}\pi, \frac{\pi}{3}(1+3\eta)-|\alpha_2|\right\},$$

thus A belongs to (4).

d) $k = 3$. By (28) $\sin 3\alpha_1 = 0$, $3\alpha_1 \equiv 0 \bmod \pi$ and it follows like before (35) from (29) that

$$\alpha_1 = -\frac{\pi}{6}+\varepsilon\frac{\pi}{2} \qquad (\varepsilon = \pm 1).$$

After the substitution into (1), (26) and (27) we obtain

$$\sum_{i=1}^{3}\cos\alpha_i = \sum_{i=1}^{3}\cos 3\alpha_i = \sum_{i=1}^{3}\cos 9\alpha_i = -\frac{1}{2}\varepsilon,$$

thus by Lemma 3 and (19), A is one of quadruples (5), (6), or (9). The proof is complete.

The above proof is almost self contained (the irreducibility of a cyclotomic polynomial is implicit in the proof of Lemma 2), but may seem artificial. Another more advanced but also more natural treatment is possible based on the work of H. B. Mann [4].

I conclude by expressing my thanks to Professor A. Schinzel who has suggested the idea of the above proof and has prepared the final version of the paper.

References

[1] W. J. R. Crosby, Solution of the problem 4136, *Amer. Math. Monthly*, **53** (1946), 103–107.
[2] F. Faà di Bruno, *Einleitung in die Theorie der binären Formen*, Leipzig, 1881.
[3] F. Kárteszi, Intorno a punti allineati di certi reticoli circolari, *Rend. Sem. Matem. Messina*, **9** (1964–65), 1–12.
[4] H. B. Mann, On linear relations between the roots of unity, *Mathematika*, **12** (1965), 107–117.

INDEX

CORRADI, K. A., On the solvability of finite groups 113

CORRADI, K. A., On the theory of the one-step non-Abelian groups 123

CORRADI, K. A., and KÁTAI, I., A note on combinatorics 101

ЭЛЬБЕРТ, А., Обобщение одного неравенства Ляпунова для дифференциальных уравнений с запаздывающим аргументом 107

ERDŐS, P., SÁRKÖZI, A. and SZEMERÉDI, E., On some extremal properties of sequences of integers 131

FRIED, E., Über die teilweise geordnete Menge der konjugierten Untergruppen 95

GALAMBOS, J., Quadratic inequalities among probabilities 11

GOLDBERG, M., Axially symmetric packing of equal circles on a sphere, II. 137

GYŐRY, K., Note on the paper of W. M. Schmidt „Some diophantine equations in three variables with only finitely many solutions" 67

KÁTAI, I., On an algorithm for additive representation of integers by prime numbers 23

KÁTAI, I., A note on a paper of Gordon and Rogers 29

KÁTAI, I., Characterization of additive functions by its local behaviour 35

KÁTAI, I. and CORRADI, K. A., A note on combinatorics 101

PETRUSKA, G., A contribution on Bloch's theorem 39

RUZSA, I., Random models of some quasi-intuitionistic logics 77

SANDS, A. D., The radical of a certain infinite matrix ring 143

SÁRKÖZI, A., ERDŐS, P. and SZEMERÉDI, E., On some extremal properties of sequences of integers 131

SCHIPP, F., Über Walsh-Fourierreihen mit nichtnegativen Partialsummen 43

SCHIPP, F., Über die Divergenz der Walsh-Fourierreihen 49

SZÁSZ, F., Ein radikaltheoretischer Vereinigungsendomorphismus des Idealverbandes der Ringe 73

SZEMERÉDI, E., ERDŐS, P. and SÁRKÖZI, A., On some extremal properties of sequences of integers 131

SZIGETI, F., On ordinary linear differential equations in Banach space 17

WIEGANDT, R., A note on Kurosh-Amitsur radical properties 63

WLODARSKI, Ł., On the equation $\cos \alpha_1 + \cos \alpha_2 + \cos \alpha_3 + \cos \alpha_4 = 0$ 147

ZEITLER, H., Über eine Parkettierung des dreidimensionalen hyperbolischen Raumes 3

Technikai szerkesztő:
SCHARNITZKY VIKTOR

69.683. Állami Nyomda, Budapest
A kiadásért felelős: az Eötvös Loránd Tudományegyetem rektora
A kézirat nyomdába érkezett: 1969 február. Megjelent: 1969 december
Terjedelem 13,75 A/5 ív, 13 ábra. Példányszám 820
Készült monó- és kéziszedéssel, ives magasnyomással,
az MSZ 5601 — 59 és MSZ 5602 — 55 szabványok szerint