C.R. Math. Rep. Acad. Sci. Canada

Vol. VIII, No. 2 **April 1986 avril**

CONTENTS

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

SUMS OF A SERIES, PERMITTING REARRANGEMENTS

Israel Halperin, F.R.S.C.
(dedicated to Prof. W.J. Webber on his 88th birthday)

Part I

1. Introduction

1.1 In Part I, V will denote an m-dimensional real Euclidean vector space, $m = 1,2,\ldots$. Suppose that $v_1, v_2, \cdots$ is a given infinite sequence in V and let S denote the set of sums of the convergent series which have as terms the given v_m, in some order.

Theorem I. (P. Levy [5], E. Steinitz [7]). The set S is either empty or of the form $s_0 + L$ for some vector s_0 and some linear subspace L.

Thus, to take the 2-dimensional case, if the v_n are complex numbers then S is either empty, or a single value, or a line in the complex plane, or the whole complex plane.

1.2 Let $F \equiv \{w \text{ in } V : \sum_{n=1}^{\infty} (w|v_n)^+ < \infty\}$. Here $(w|v)$ denotes the real inner product and if a is a real number, $a^+ \equiv \max(a,0)$.

Obviously S is empty if either of the following properties fails:

(P_1): $v_n \to 0$ as $n \to \infty$.
(P_2): If w is in F then $-w$ is also in F.

On the other hand, if (P_2) holds than F is a linear subspace and Theorem I has a more precise statement:

Theorem II. If $(P_1),(P_2)$ hold, then S is not empty and for any s_0 in S:

$$S = s_0 + F^{\perp} \ (F^{\perp} \text{ denotes the orthogonal complement of } F).$$

1.3 Let $v_n = v'_n + v''_n$ be the orthogonal decomposition with v'_n in F and v''_n in $F^{\perp}$.

Then $\sum_{n=1}^{\infty} v'_n$ is absolutely, and so unconditionally, convergent. Hence Theorem II can be easily deduced from its special case:

Theorem III. Suppose

(i) $v_n \to 0$ as $n \to \infty$,

(ii) for all non-zero w: $\sum_{n=1}^{\infty} (w|v_n)^+ = \infty$,

then $S = V$.

1.4 For $m = 1$, Theorem III is a known theorem of Riemann. A detailed analysis of the incompleteness of Levy's proof, especially for $m > 2$, was given by Steinitz [8], who also gave a different, complete proof in [7], using his theorems on convex sets.

In this exposition we use a variation of Levy's method to present a proof of Theorem III for $m \geq 2$, by induction on m (with a simpler proof for the case $m = 2$). We also sketch Steinitz's other proof of Theorem III.

In Parts II, III we recall work by several authors for the case of infinite-dimensional real topological vector spaces.

2. Preparatory Remarks

2.1 A construction with real numbers (Riemann). Suppose that $\alpha_n, \beta_n, \gamma_n$ are sequences of real numbers, each converging to 0 as $n \to \infty$; suppose also that

$$\alpha_n \geq 0, \quad \sum_{n=1}^{\infty} \alpha_n = \infty, \quad \beta_n \leq 0, \quad \sum_{n=1}^{\infty} \beta_n = -\infty.$$

Then the 3 sequences can be combined, preserving the order within each, to be the terms of a convergent series with preassigned sum s_0.

To show this, take α-terms until the sum is greater than s_0; then take a γ-term, then a β-term, and then additional β-terms until the sum is less than s_0. Repeat this procedure.

2.2 Discarding an unconditionally convergent set of deviations. Without loss of generality, in proving Theorem III we may clearly replace v_n by $v_n + w_n$ whenever $\sum_{n=1}^{\infty} w_n$ is unconditionally convergent.

2.3 A special case permitting the induction. Suppose that for some non-zero u, the given v_n include two subsequences

$$\alpha_n u, \ \beta_n(-u) \text{ with } \alpha_n \geq 0, \ \sum_{n=1}^{\infty} \alpha_n = \infty, \ \beta_n \geq 0, \ \sum_{n=1}^{\infty} \beta_n = \infty.$$

Then for the other terms: $v_n = v'_n + \gamma_n u$ with $v'_n \perp u$. By the inductive assumption the v'_n can be ordered as the terms of a convergent series with preassigned sum in $u^{\perp}$.

Without changing the order of the corresponding v_n: the $\gamma_n u$, the $\alpha_n u$, and the $\beta_n(-u)$, can be combined as in §2.1 to give a convergent series with preassigned multiple of u as sum.

This proves Theorem III in this special case.

2.4 A more general case permitting the induction. Suppose $u, u_1, \cdots, u_r$ are non-zero vectors and

$$-u = p_1u_1 + \cdots + p_ru_r \quad (\text{all } p_i > 0).$$

Suppose also that the given v_n include mutually exclusive sequences $\alpha_n u, \beta_n^{(i)}u_i$, $i = 1,\dots,r$ such that:

$$\alpha_n \geq 0, \quad \sum_{n=1}^{\infty} \alpha_n = \infty$$

$$\beta_n^{(i)} \geq 0, \quad \sum_{n=1}^{\infty} \beta_n^{(i)} = \infty \text{ for each } i.$$

Then for each i, we can select for $t = 1,2,\dots,$ mutually exclusive sets of the $\beta_n^{(i)}u_i$ so that for each t, the sum differs from $\frac{1}{t}p_iu_i$ in length by less than $\frac{1}{t^2}$; by using §2.2 we may even assume that the sum is precisely $\frac{1}{t}p_iu_i$.

Now for each t, collect together the vectors so obtained for $i = 1,\dots,r$. We obtain a block of terms B_t, with sum $\frac{1}{t}(-u)$. The procedure of §2.3 can now be applied to the blocks B_{2t} $(t = 1,2,\dots,)$, the terms $\alpha_n u$, and the other v_n, to give a series converging to preassigned sum, with brackets around each block B_{2t} (the $\beta_n^{(i)}u_i$ in the blocks B_{2t+1} ensure that (ii) of the Theorem III continues to hold in $u^{\perp}$ when the vectors in the B_{2t} are removed). Then the brackets can be removed, since within B_{2t} all partial sums have length $\leq \frac{K}{2t}$ $(\to 0 \text{ as } n \to \infty)$ where $K = \sum_{i=1}^{r} p_i \|u_i\|$ ($\|v\|$ denotes length of v).

3. Levy Vectors

3.1 We will call a vector u Levy if $\|u\| = 1$ and for every $\epsilon > 0$:

$$\sum_{n=1}^{\infty}{}' \|v_n\| = \infty$$

where the prime mark here means that the sum is to be taken just for those non-zero v_n for which the angle between u and v_n is less than ϵ (an equivalent requirement: for each $0 < \epsilon < 1$,
$\sum (\|v_n\| : (u|v_n) > (1-\epsilon) \|v_n\|) = \infty$).

3.2 The set of Levy vectors is clearly a closed subset of the compact unit sphere, so it is a compact set.

Also, every closed half-sphere $H(w) \equiv \left\{ u: \|u\| = 1 \text{ and } (w|u) \geq 0 \right\}$, $w \neq 0$, must contain a least one Levy vector (otherwise, compactness of $H(w)$ would imply that

$$\sum_{n=1}^{\infty}{}'' \|v_n\| < \infty$$

where the double prime here means that the sum is to be taken just for those v_n for which $(w|v_n) \geq 0$, and this would contradict the hypothesis (ii) of Theorem III).

3.3 Suppose u is a Levy vector. Then we can choose a sub-sequence of the v_n of the form $\alpha_n u + w_n$ with $\alpha_n > 0$, $\sum_{n=1}^{\infty} \alpha_n = \infty$ and $\sum_{n=1}^{\infty} \|w_n\| < \infty$. By invoking §2.2 we may even suppose that the subsequence has the form $\alpha_n u$.

More generally, if $u, u_1, \cdots, u_r$ are Levy vectors then we may assume that the given v_n include mutually exclusive subsequences $\alpha_n u, \beta_n^{(i)} u_i$ with $\alpha_n > 0$, $\sum_{n=1}^{\infty} \alpha_n = \infty$, $\beta_n^{(i)} > 0$, $\sum_{n=1}^{\infty} \beta_n^{(i)} = \infty$ for all i.

Thus, to prove Theorem III we need only prove (using §2.4):

Theorem IV. (Steinitz [8]). Suppose that L is a closed subset of the unit sphere of V and that in every closed half-sphere there is at least one L-vector. Then in L, for some $r \geq 1$ and some $p_1, \cdots, p_r$ all greater than 0, there exist $u, u_1, \ldots, u_r$ satisfying $-u = p_1 u_1 + \cdots + p_r u_r$.

Theorem IV is trivial when $m = 1$. We shall prove this theorem for $m \geq 2$ by induction on m. But in the next section we give for the case $m = 2$ (complex numbers), a particularly elementary proof.

4. Proof of Theorem IV for the Case $m = 2$

4.1 We may suppose that

(*) if u is an L-vector then -u is not

(otherwise Theorem IV would hold trivially with $r = 1$, $u_1 = -u$, $p_1 = 1$).

Choose an L-vector u_1. Then choose an L-vector u_2 which maximizes $\|u_1 - u_2\|$. Because of (*), $u_2 \neq (-u_1)$; and no L-vector is in the angle of u_2 and $(-u_1)$.

Next, because of (*), $(-u_2)$ is not an L-vector. Since the set of L-vectors is closed, some w, in the angle of $(-u_2)$ and u_1, is not an L-vector and no L-vector is in the angle of $-u_2$ and w; and also (-w) is not an L-vector. Then some u on the side of w and (-w) which does not contain u_1 must be an L-vector and u must lie in the angle formed by $-u_1$ and $-u_2$. Consequently, for some $p_1 > 0$, $p_2 > 0$: $u = p_1(-u_1) + p_2(-u_2)$, $-u = p_1 u_1 + p_2 u_2$.

This proves, for the case $m = 2$, Theorem IV and so also Theorem III.

5. Proof of Theorem IV for $m \geq 2$ by Induction

5.1 Suppose, if possible, that some open half-sphere $\{u: \|u\| = 1$ and $(w|u) > 0\}$ ($w \neq 0$) contains no L-vector.

Then the boundary $\{u: \|u\| = 1$ and $(w|u) = 0\}$ is a sphere in $m-1$ dimensions with the property that each of its closed half-spheres $\{u: \|u\| = 1, (w|u) = 0$, and $(w_1|u) \geq 0\}$, $w_1 \neq 0$, $(w|w_1) = 0$, must contain at least one L-vector; to see this, note that for each $t > 0$, the closed half-sphere in m-dimensions: $H(w + tw_1)$, contains some L-vector u_t. Then $(w|u_t) \leq 0$, $(w + tw_1|u_t) \geq 0$, so $(w_1|u_t) \geq 0$ and $(w|u_t) \geq -t(w_1|u_t) \geq -t\|w_1\|$. When $t \to 0$, it follows from compactness of the set of L-vectors that there exists an L-vector u with $(w|u) \geq 0$ (hence $(w|u) = 0$) and $(w_1|u) \geq 0$.

Therefore, in this case the L-vectors in the boundary satisfy the hypotheses of Theorem IV in a vector space of $m-1$ dimensions.

Hence, in proving Theorem IV we may assume that every open half-sphere contains at least one L-vector. Consequently there exist m linearly independent L-vectors $u_1, \ldots, u_m$.

5.2 Let C denote the convex cone which has 0 as vertex and is determined by the half-lines pv, all $p \geq 0$, all L-vectors v; let $\overline{C}$ denote its closure. Then $\overline{C}$ is a closed convex cone with 0 as vertex.

Now $w = u_1 + \cdots + u_m$ is an interior point of C. Suppose, if possible, $C \neq V$, say v_0 is not in C. Then $w_1 \equiv 2v_0 - w$ would be an interior point of the set complement of C, i.e. w_1 would not be in $\overline{C}$.

Now w_1 can be separated from $\overline{C}$ by a hyperplane W (to see this, let w_2 be the point in $\overline{C}$ closest to w_1 and take W to be the hyperplane through

$\frac{w_1+w_2}{2}$ and orthogonal to $w_1 - w_2$).

It follows that $\overline{C}$, and so also C, lie on one side of the hyperplane through 0 and parallel to W. This contradicts the assumption that every open half-sphere contains an L-vector.

Thus C must be all of V; so for every L-vector u, the vector -u is a positive linear combination of L-vectors.

This proves Theorem IV and completes the proof of Theorem III.

6. The Polygon Rearrangement Theorem

6.1 (Theorem V). (Grinberg and Sevast'yanov [2]). For every m-dimensional normed vector space W and every finite sequence $x_1, \ldots, x_n$ in W with all $\|x_i\| \leq 1$ (set $x = x_1 + \cdots + x_n$), this sequence can be ordered (as $y_1, \cdots, y_n$, say) so that for $k = 1,\ldots,n$:

$$\left\| \sum_{i=1}^{k} y_i - \frac{k-m}{n} x \right\| \leq K \text{ with } K = K(m) = m .$$

Remark. For the case $x = 0$ and with $K(m) = 2m$, this theorem was formulated and proved by Steinitz [7]. Later, for this case $x = 0$, an elementary proof was found by Gross [3] (but with $K(m) = 2^m - 1$), and Gross showed how to use the theorem to get a simple proof of Theorem I (which is weaker than Theorem III). Still later, F.A. Behrend [*The Steinitz-Gross theorem on sums of vectors,* Canadian Journ. of Math. 6 (1954), 108-124] showed that for this case $x = 0$: $K(m) < m$.

6.2 Suppose $v_1,\ldots,v_{m+2}$ are vectors in an m-dimensional real vector space. Then there exist real numbers $\epsilon_1,\cdots,\epsilon_{m+2}$, not all 0 such that:

$$\sum_{i=1}^{m+2}\epsilon_i = 0 \quad\text{and}\quad \sum_{i=1}^{m+2}\epsilon_i v_i = 0.$$

6.3 Suppose that $v_1,\cdots v_{k+1}, w$ are vectors in an m-dimensional real vector space with $k \geq m$, and consider all representations $w = \lambda_1 v_1 + \cdots + \lambda_{k+1}v_{k+1}$ with $0 \leq \lambda_i \leq 1$ for all i and $\lambda_1 + \cdots + \lambda_{k+1} = k - m$. If there is such a representation, there is a representation with $\lambda_i = 0$ for at least one i.

Proof. We may assume that for every representation: $\lambda_i \neq 1$ for all i (first obtain a representation with $\lambda_i = 1$ for a maximal set of i, then delete the corresponding v_i). Now if $k = m$, then $\lambda_i = 0$ for all i; if $k \geq m+1$, choose $\epsilon_1,\cdots,\epsilon_{k+1}$ not all 0 with $\sum_{i=1}^{k+1}\epsilon_i = 0$ and $\sum_{i=1}^{k+1}\epsilon_i v_i = 0$ (use §6.2 noting that $k+1 \geq m+2$). Replace λ_i by $\lambda_i - t\epsilon_i$ and take the least $t \geq 0$ for which $\lambda_j - t\epsilon_j$ is 0 or 1 (necessarily 0) for some j.

6.4 To prove Theorem V, Grinberg and Sevast'yanov construct (by induction), sets $A_n \equiv \{1,\ldots,n\} \supset A_{n-1} \supset \cdots \supset A_m$ and numbers λ_k^i $(k = n,\ldots,m\,;\, i \in A_k)$ with the properties:

$$(*)\quad \begin{cases} A_k \text{ has } k \text{ members};\ 0 \leq \lambda_k^i \leq 1;\ \sum_{i\in A_k}\lambda_k^i = k-m \text{ and} \\ \sum_{i\in A_k}\lambda_k^i x_i = \dfrac{k-m}{n} \end{cases}$$

as follows:

First, for $k = n$, set $\lambda_n^i = \dfrac{n-m}{n}$.

Next, if A_{k+1} and the λ^i_{k+1} satisfy (*) and $k \geq m$,

set $\mu^i_{k+1} = \frac{k-m}{k+1-m} \lambda^i_{k+1}$. Then use §6.3 to

replace μ^i_{k+1} by $\overline{\mu}^i_{k+1}$ with some $i(k)$ for which $\overline{\mu}^{i(k)}_{k+1} = 0$.

Set $y_{k+1} = x_{i(k)}$; delete this $i(k)$ from A_{k+1} to obtain A_k;

set $\lambda^i_k = \overline{\mu}^i_{k+1}$ for $i \in A_k$.

This determines $y_{m+1}, \cdots, y_n$; order the $x_i, i \in A_m$ in any way, as $y_1, \cdots, y_m$.

6.5 With the $y_1, \cdots, y_n$ determined in §6.4 we have:

$$\text{for } k \leq m: \ \left\| \sum_{i=1}^{k} y_i - \frac{k-m}{n} x \right\| \leq \left\| \sum_{i=1}^{k} y_i \right\| + \left\| \frac{m-k}{n} x \right\|$$

$$\leq k + m - k = m;$$

$$\text{for } k > m: \ \left\| \sum_{i=1}^{k} y_i - \frac{k-m}{n} x \right\|$$

$$= \left\| \sum_{i \in A_k} x_i - \sum_{i \in A_k} \lambda^i_k x_i \right\|$$

$$= \left\| \sum_{i \in A_k} (1 - \lambda^i_k) x_i \right\| \leq \textstyle\sum_{i \in A_k} (1 - \lambda^i_k)$$

$$= k - (k-m) = m.$$

7. The Steinitz Proof of Theorem III

7.1 Let C denote the convex set of all $p_1 s_1 + \cdots + p_r s_r$ where $r = 1, 2, \ldots$, $0 \leq p_i \leq 1$ for all i and $\sum_{i=1}^{r} p_i = 1$, and each $s_j = \sum_{i \in A_j} v_i$ (A_j a finite set of integers). An argument like that used in §5.2 shows if the closure of C is not V then this closure lies on one side of some hyperplane. This would contradict (ii) of Theorem III. Hence for every vector v_0 and every $\epsilon > 0$:

$$\|v_0 - (p_1 s_1 + \cdots + p_r s_r)\| < \epsilon$$

for some $p_1 s_1 + \cdots + p_r s_r$. This means

$$(*) \quad \|v_0 - (\lambda_1 v_1 + \cdots + \lambda_n v_n\| < \epsilon$$

for some n and $0 \le \lambda_i \le 1$ for all i.

Since (ii) of Theorem III holds also for the sequence $v_k, v_{k+1}, \cdots$ for every k, we can obtain (*) with the added conditions: $\lambda_i = 0$ if $i \in A$, for a preassigned finite set of integers A, and for all i: $\|v_i\| < \frac{\epsilon}{m}$.

7.2 Every sum $\sum_{i=1}^{n} \lambda_i v_i$, $0 \le \lambda_i \le 1$ can be expressed with such λ_i for which the number of i with $0 < \lambda_i < 1$ is less than $m+1$ (by an argument like that used in §6.3). Hence for some finite set B of integers, with empty intersection with a preassigned finite set A, we will have

$$\|v_0 - \textstyle\sum_{i \in B} v_i\| < 2\epsilon .$$

7.3 Define mutually exclusive finite subsets of the integers $B_1, B_2, B_3, \cdots$ to satisfy $\|v_0 - \sum_{i \in B_1} v_i\| \le 1$; $B_2 = \{1\}$ if $1 \notin B_1$, otherwise B_2 is empty; and for $k \ge 1$:

$$\left|\left(v_0 - \sum_{i \in B_1 \cup \cdots \cup B_{2k}} v_i\right)\right| - \sum_{i \in B_{2k+1}} v_i < \frac{1}{2k+1}; \; B_{2k+2} = \{k+1\} \text{ if } k+1 \notin \bigcup_{i < 2k+2} B_i,$$

otherwise B_{2k+2} is empty.

Then $(\sum_{i \in B_1} v_i) + (\sum_{i \in B_2} v_i) + \cdots + (\sum_{i \in B_k} v_i) + \ldots = v_0$. Because of Theorem V, the v_i in each B_k can be rearranged in a way that permits removal of the brackets. This shows that $v_0 \in S$.

Part II

8. Theorem of Katznelson and McGehee

8.1 In Part II, V will denote the topological real vector space of all infinite real sequences $v = (\alpha_1, \alpha_2, \cdots)$, with componentwise convergence. We suppose given a sequence $v_j = (\alpha_1^j, \alpha_2^j, \cdots), j = 1,2,\ldots$ and let S denote the set of sums of those convergent series which have the given v_j as terms.

8.2 Clearly S is empty unless:

(P_1) $\alpha_m^j \to 0$ as $j \to \infty$ for each m.

(P_2) For every finite sequence $w = (w_1, \cdots, w_n)$:

if $\sum_{j=1}^{\infty} (\sum_{i=1}^{n} w_i \alpha_i^j)^+ < \infty$

then $\sum_{j=1}^{\infty} (\sum_{i=1}^{n} (- w_i \alpha_i^j))^+ < \infty.$

8.3 We shall assume that (P_1) and (P_2) hold. We shall call the integer n dominated if for some $w_1, \cdots, w_n$ with $w_n = 1$:

$$\sum_{j=1}^{\infty} |\sum_{i=1}^{n} w_i \alpha_i^j| < \infty,$$

in other words, $\alpha_n^j = \sum_{i=1}^{n-1} (-w_i)\alpha_i^j + \beta_n^j$ with $\sum_{j=1}^{\infty} |\beta_n^j| < \infty$, hence $\sum_{j=1}^{\infty} \beta_n^j$ is unconditionally convergent, to sum denoted β_n, say.

Theorem VI. (Katznelson and McGehee [4]). If (P_1) and (P_2) hold, then S is not empty and

$$S = v_0 + M$$

where $v_0 = (\alpha_1^o, \alpha_2^o, \cdots)$ with $\alpha_n^o = \beta_n$ if n is dominated, otherwise $\alpha_n^o = 0$, and M is the linear subspace of all $v = (\alpha_1, \alpha_2, \cdots)$ with α_n arbitrary if n is not dominated and $\alpha_n = \sum_{i=1}^{n-1}(-w_i)\alpha_i$ if n is dominated (if 1 is dominated, $\alpha_1 = 0$).

8.4 Proof of Theorem VI. We may clearly assume that no integer is dominated and we need to show that any given

$$v = (\alpha_1, \alpha_2, \cdots) \text{ is in } S.$$

Because of the Levy-Steinitz Theorem III we can rearrange the v_j so that for some $n_1 < n_2 < \cdots$ we have, for the partial sums

$$\sum_{j=1}^{m} v_j \equiv s_m = (s_1^m, s_2^m, \cdots)$$

the inequalities

$$|s_i^{n_j} - \alpha_i| < \frac{1}{j} \quad \text{for } i = 1, \ldots, j,$$

$$\sum_{i=1}^{j} |\alpha_i^n| < \frac{1}{j^2} \quad \text{for all } n > n_j.$$

Then, using Theorem V of §6.1 we rearrange the v_n with $n_j < n \leq n_j$ so that

$$|s_i^n - \alpha_i| < \frac{1}{j} + \frac{j}{j^2} + \frac{1}{j} = \frac{3}{j}.$$

Then $s_i^n \to \alpha_i$ as $n \to \infty$ for all i. This proves Theorem VI.

Remark. The original, rather long, proof of Theorem VI given by Katznelson and McGehee, used neither the Levy-Steinitz Theorem III nor Theorem V.

Part III

9. The Counter-Example of Marcinkiewicz

9.1 Let ϕ denote the characteristic function of the interval $(0,1)$; let ϕ_L, ϕ_R denote respectively the characteristic functions of $(0, \frac{1}{2})$ and $(\frac{1}{2}, 1)$. If ϕ_W is the characteristic function of some interval (a,b), let ϕ_{WL}, ϕ_{WR} denote respectively the characteristic functions of $\left(a, \frac{a+b}{2}\right)$ and $\left(\frac{a+b}{2}, b\right)$. Let A denote the countably infinite family $\phi, \phi_L, \phi_R, \phi_{LL}, \phi_{LR}, \phi_{RL}, \phi_{RR}, \cdots$ together with the negatives of these functions; let S denote the set of sums of those convergent series in the Hilbert space $L^2(0,1)$ which have the members of A as terms.

9.2 Counter-example of Marcinkiewicz [6, page 106]. Since $\|v_n\| \to 0$ as v_n varies in any way over all members of A, it follows that the brackets can be removed in the series:

$$\phi = \phi + (-\phi + \phi_L + \phi_R) + (-\phi_L + \phi_{LL} + \phi_{LR}) + (-\phi_R + \phi_{RL} + \phi_{RR}) + \cdots,$$

$$0 = (\phi + (-\phi)) + (\phi_L + (-\phi_L)) + (\phi_R + (-\phi_R)) + \cdots$$

so 0 and ϕ are in S.

On the other hand every partial sum s of a finite number of members of A, is integer-valued, so for every k with $0 < k < 1$:

$$\|s - k\phi\| \geq \min(k, 1-k),$$

which shows that $k\phi$ is not in S. So a Levy-Steinitz theorem for $L^2(0,1)$ does not hold.

9.3 The family A, considered in $L^p(0,1)$ for $0 < p < \infty$, has $0, \phi$ (but no $k\phi$, $0 < k < 1$) in S (of $L^p(0,1)$). It is tedious but not difficult to show that if $0 < p < \infty$, S (of L^p) consists precisely of those functions in $L^p(0,1)$ which are integer-valued.

A theorem of Banach [1, page 185] shows that $L^2(0,1)$ can be imbedded isometrically in the Banach space $C(0,1)$ of all continuous functions f on $(0,1)$ with norm $\|f\| = \sup(|f(t)|: 0 \leq t \leq 1)$ which is itself a subspace of $L^\infty(0,1)$.

Thus there fails to be a Levy-Steinitz theorem for $C(0,1)$ and $L^\infty(0,1)$.

9.4 When the members of A in §9.1, considered as elements in $L^2(0,1)$ are orthonormalised the basis consists of ϕ, $\phi_L - \phi_R$, and all $(\phi_{WL} - \phi_{WR})(\|\phi_{WL} - \phi_{WR}\|^{-1})$; each f in $L^2(0,1)$ is mapped into an element $T(f)$ in l^2. If f is in A, then $T(f)$ is a sequence of real numbers of which only a finite number differ from 0.

If f is the function ϕ_W, W a word with n letters, then $T(f) = (\alpha_i; 1 \leq i < \infty)$, $\sum_{i=1}^{\infty} \alpha_i^2 = \frac{1}{2^n}$, $\alpha_i \neq 0$ for $n+1$ values of i. Hence $|\alpha_i| \leq \left(\frac{1}{2^n}\right)^{1/2}$ for all i, and $\alpha_i \neq 0$ for only $n+1$ values of i. So for every p with $0 < p \leq \infty$: $T(f)$ is in l^p with $\|T(f)\|^p \leq \frac{n+1}{(2^{n/2})^p}$. So $T(f) \to 0$ in l^p, for $0 < p \leq \infty$, as f varies over A; and so in this l^p: S for the family of $T(f), f \in A$, contains $T(\phi)$ and 0.

If f is in $L^2(0,1)$ and $T(f) = (\alpha_i; 1 \leq i < \infty)$, then for $0 < p \leq 2$: $\sum_{i=1}^{\infty} |\alpha_i|^p \geq \min(1, \sum_{i=1}^{\infty} |\alpha_i|^2) = \min(1, \|f\|^2 \text{ in } L^2(0,1))$. Thus the $T(f), f \in A$, cannot be arranged to converge to $kT(\phi)$ for any $0 < k < 1$. Thus there fails to be a Levy-Steinitz theorem for $l^p, 0 < p \leq 2$.

The problem: does a Levy-Steinitz theorem hold in l^p for $2 < p \leq \infty$, seems to be open.

References

[1] S. Banach, **Théorie des Operations Linéaires**, 1932.

[2] V.S. Grinberg and S.V. Sevast'yanov, **Value of the Steinitz Constant**, Functional Analysis and its Applications, translated from Funktsional'nyi Analiz i Ego Prilozheniya, Vol. 14, No. 2 (1980), pages 56-57, English pages 125-126.

[3] W. Gross, **Bedingt konvergente Reihen**, Monatshefte für Math. und Physik, Vol. 28 (1917), pages 221-237.

[4] Y. Katznelson and O.C. McGehee, **Conditionally convergent series in** $\mathbf{R}^{\infty}$, Michigan Math. J., Vol. 21 (1974), pages 97-106.

[5] P. Levy, **Sur Les Series Semi-Convergentes**, Nouv. Ann. d. Math., Vol. 64 (1905), pages 506-511.

[6] The Scottish Book, edited by R. Daniel Mauldin (Birkhauser, Boston, 1981).

[7] E. Steinitz, **Bedingt konvergente Reihen und konvexe Systeme**, Journ. f. Math., Vol. 143 (1913), pages 128-175.

[8] E. Steinitz, **Bedingt konvergente Reihen und konvexe System (Fortsetzung)**, Journ. f. Math., Vol. 144 (1914), pages 1-40.

Department of Mathematics
University of Toronto

Received 28 January, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

GALOIS GROUPS OF SOME 2-EXTENSIONS OF ORDERED FIELDS

Ján Mináč

Presented by P. Ribenboim, F.R.S.C.

Abstract: Let F be a formally real Pythagorean field with finite chain length invariant $c\ell(F)$. Let $F(2)$ be the maximal 2-extension of F , and G_F the Galois group of automorphisms of the field extension $F(2)/F$. We shall determine the group G_F using structure of the order space $(X_F, \dot{F}/\dot{F}^2)$.

In this paper we keep to the notation in [4], [5], [6]. We define F (or $K,L,\ldots$) to be a formally real Pythagorean field, $\dot{F}$ is the multiplicative group of F , T - a preordering of F . T_F - the intersection of all orderings of the field F . $[\dot{F}:\dot{T}_F]$ is the group-index. V - a valuation on F . A_V - the valuation ring corresponding to V . U_V - the group of units of A_V . M_V - the maximal ideal of A_V . F_V - the residue field of V . V is said to be fully compatible with T if $1 + M_V \subset T$. $(X,\dot{F}/\dot{T})$ is a space of orderings. Here X means the set of all orderings P of the field F such that $T \subseteq P$. Sometimes, instead of $(X,\dot{F}/\dot{T})$ we shall write only X . X_F denotes the space of all orderings of the field F . If $P_1,P_2 \in X$ then we define $P_1 \sim P_2$ if either $P_1 = P_2$ or there exists a 4-element fan $S \subset X$ such that $P_1,P_2 \in S$. The relation is an equivalence relation ([6]) Equivalence classes of X with respect to $\sim$ are called components of X .

The chain length of the preordering T, $c\ell(T) = c\ell(X)$, is defined e.g. in [4] and [6].

We shall always assume that $c\ell(F) = c\ell(T_F) < \infty$. In that case it is proved in [3] and [6] that if $|X| \neq 1$ and if there is no valuation V on F fully compatible with T_F, such that $|\dot{F}/\dot{F}^2U_V| \neq 1$, then X decomposes into nontrivial components $X_1,\ldots,X_s$, $2 \leq s$. Furthermore $c\ell(X) = c\ell(X_1) + \ldots + c\ell(X_s)$.

G_F means $\mathrm{Gal}(F(2)|F)$. $G = \mathop{*}\limits_1^r G_i$ means that G is a free product of groups G_i, $i = 1,\ldots,r$, in the category of pro-2-groups.

For other definitions and theorems used here, the reader is referred to [3], [4], [6], [11].

In paper [10] was shown an example of two fields F_1,F_2 with $W(F_1) \cong W(F_2)$ but $G_{F_1} \not\cong G_{F_2}$. In [10], (Theorem 2.2), it was proved that $G_{F_1} \cong G_{F_2} \Rightarrow W(F_1) \cong W(F_2)$. Since for Pythagorean fields we have $W(F_1) \cong W(F_2) \Leftrightarrow X_{F_1} \cong X_{F_2}$ (as spaces of orderings) we have $G_{F_1} \cong G_{F_2} \Rightarrow X_{F_1} \cong X_{F_2}$. In this note we shall show that if F_1,F_2 are two formally real Pythagorean fields, with $c\ell(F_1)$, $c\ell(F_2) < \infty$, then

1) $X_{F_1} \cong X_{F_2} \Rightarrow G_{F_1} \cong G_{F_2}$ and consequently

2) $W(F_1) \cong W(F_2) \Leftrightarrow G_{F_1} \cong G_{F_2}$.

Before formulating our Theorem we shall prove the following Proposition. (See also [12], Theorem D and Lemma 6).

Proposition. Let F *be a formally real Pythagorean field. Then there exists an unique (continuous) homomorphism* $\phi : G_F \to \{+1,-1\}$ *such that* $\phi(\sigma) = -1$ *for every involution* σ *in* G_F *. Let* $\ker \phi$ *denote the kernel of the homomorphism* ϕ *. Then* $\ker \phi = G_{F(\sqrt{-1})}$ *. Therefore the subgroup* $G_{F(\sqrt{-1})}$ *of the group* G_F *is uniquely determined by the group* G_F *.*

Proof. Define $\phi : G_F \to \{+1,-1\}$ by $\phi(g) = \frac{g(\sqrt{-1})}{\sqrt{-1}}$; from Theorem 3, Chapter II in [2] we get $\phi(\sigma) = -1$ for every involution σ in G_F . We have $\operatorname{Ker} \phi = G_{F(\sqrt{-1})}$.

Suppose now that ϕ is any homomorphism $\phi : G_F \to \{+1,-1\}$ such that $\phi(\sigma) = -1$ for every involution σ in G_F . Denote by A (resp. B) the set of all elements in G_F which can be written as product of even (resp. odd) number of involutions. Then $\bar{A} \cup \bar{B} = G_F$, $\phi(\bar{A}) = +1$, $\phi(\bar{B}) = -1$. (Here $\bar{A}$ means closure of the set A in G_F). Hence $\bar{A} = \operatorname{Ker} \phi$ and ϕ is given by formula $\phi(g) = \frac{g(\sqrt{-1})}{\sqrt{-1}}$.

§2. *Theorem. Let* F *be a formally real Pythagorean field with* $c\ell(F) < \infty$ *. Then*

A) *If* $c\ell(F) = 1$ *, then* $G_F \cong \mathbb{Z}/2\mathbb{Z}$

B) *If* $X_F = X_1 \oplus X_2 \oplus \dots \oplus X_s$, $2 \le s$ *is a decomposition of* X_F *into connected components* $X_1,\dots,X_s$ *and* $F_1,\dots,F_s$ *are 2-Henselizations of* F *with respect to valuations* $V_1,\dots,V_s$ *fully compatible with* $T_i = \bigcap_{P \in X_i} P$, $i = 1,\dots,s$, *(or if* $|X_i| = 1$ *then* F_i *is a Euclidean closure of* F *with respect to* $P_i \in X_i$*) then*

$$G_F = \mathop{\ast}_{i=1}^{s} G_{F_i}$$

C) If $|X_F| \neq 1$ is an indecomposable space and V is the valuation on F fully compatible with T_F, such that X_{F_V} is decomposable space or $|X_{F_V}| = 1$, then

$$G_F \cong \mathbb{Z}_2^I \rtimes G_{F_V}$$

where
$2^I = |\dot{F}/\dot{F}^2 U_V|$ and $\rtimes$ means semidirect product. $\mathbb{Z}_2^I$ is a normal subgroup of G_F and the action of G_{F_V} on $\mathbb{Z}_2^I$ is given by:

(I) $g\ ag^{-1} = a$ for $g \in G_{F_V(\sqrt{-1})}$ and $a \in \mathbb{Z}_2^I$

(II) $g\ ag^{-1} = a^{-1}$ for $g \in G_{F_V} - G_{F_V(\sqrt{-1})}$ and $a \in \mathbb{Z}_2^I$

By conditions a), b), c) the Galois group G_F is determined.

Corollary. Let F_1, F_2 be fields with $X_{F_1} \cong X_{F_2}$. Then $G_{F_1} \cong G_{F_2}$. Hence $W(F_1) \cong W(F_2) \Leftrightarrow G_{F_1} \cong G_{F_2}$.

Proof of the Theorem 1.

A) Let $c\ell(F) = 1$. Then F is an Euclidean field and therefore $G_F \cong \mathbb{Z}/2\mathbb{Z}$. ([1]), SATZ 1).

B) This is an immediate consequence of the Lemma 9' in [3] and the Theorem in [7].

C) We shall prove Assertion C) be induction on $c\ell(F)$. If $c\ell(F) = 2$ then Assertion C) is true by Theorem 16, Chapter III, in [2]. Suppose now that Assertion C) is true for all fields L with $c\ell(L) < c\ell(F)$. Suppose that V is the valuation on F fully compatible with T_F, such that X_{F_V} is decomposable space or $|X_{F_V}| = 1$.

Let $\{\bar{a}_i, i \in I, a_i \in F\}$ be the basis of the vector space $\dot{F}/\dot{F}^2U_V$ over $\mathbb{Z}/2\mathbb{Z}$. Then from Theorem C and its proof in [12] and Example 2.2(ii) in [11] we find that

(I) $G_F = \mathbb{Z}_2^I \rtimes G_K$, where $K = F(\sqrt[2^{n_i}]{a_i} \mid i \in I, n_i \geq 0)$.

(II) K is a Pythagorean field.

We claim that $X_K \cong X_{F_V}$. Indeed, let W be any valuation on K which extends V. Then $(K,W)|(F,V)$ is fully ramified extension. Hence $K_W \cong F_V$. Furthermore $\dot{K}/U_W$ is 2-divisible group. By Krull-Baer's theorem ([4], Theorem 3.10) we have an injective morphism $X_{F_V} \cong X_{K_W} \rightarrow X_K$ and bijective map $X_K \rightarrow X_{F_V}$. Hence $X_{F_V} \cong X_K$.

Since X_{F_V} is decomposable space with $c\ell(F_V) \leq c\ell(F)$ we have

$$X_{F_V} = X_1 \oplus \ldots \oplus X_s$$

$$X_K = Y_1 \oplus \ldots \oplus Y_s \text{ , } s \geq 2$$

where $X_i, Y_i, i = 1,\ldots,s$ are components of the spaces X_{F_V}, X_K respectively. We may assume that $X_i \cong Y_i$, $i = 1,\ldots,s$. By B)

$$G_{F_V} = \mathop{*}_{i=1}^{s} G_{F_i} \text{ , } G_K = \mathop{*}_{i=1}^{s} G_{K_i}$$

where F_i, K_i, $i = 1,\ldots,s$ are some Pythagorean fields, such that $X_{F_i} \cong X_i$, $X_{K_i} \cong Y_i$, $i = 1,\ldots,s$. Since $c\ell(X_i) = c\ell(Y_i) < c\ell(F)$, we find by induction hypothesis that $G_{F_i} \cong G_{K_i}$ for $i = 1,\ldots,s$. Therefore $G_{F_V} \cong G_K$. From Theorems C, D, in [12] and Proposition we get that $G_F \cong \mathbb{Z}_2^I \rtimes G_{F_V}$ where the action of G_{F_V} on $\mathbb{Z}_2^I$ is given by conditions (I),

(II) in Theorem. This proves assertion C.

Using Theorem we can derive properties of the Galois groups G_F and $G_{F(\sqrt{-1})}$ by induction. For review of some results concerning mainly cohomology rings $H^*(G_F,\mathbb{Z}/2\mathbb{Z})$, $H^*(G_{F(\sqrt{-1})},\mathbb{Z}/2\mathbb{Z})$ see [9].

REFERENCES

[1] E. Becker, Euklidische Körper und Euklidische Hüllen von Körpern, J. Reine Angew. Math. 268/269 (1974) 41-52.

[2] E. Becker, Hereditarily Pythagorean fields and orderings of higher level, IMPA Lecture Notes, No. 29, Rio de Janeiro, 1978.

[3] B. Jacob, On the structure of pythagorean fields, J. Algebra, 68 (1981), 247-267.

[4] T. Y. Lam, Orderings, Valuations and Quadratic forms, CBMS, Vol. 52, (1983).

[5] M. Marshall, Classification of finite spaces of orderings. Canad. J. Math. 31 (1979), 320-330.

[6] M. Marshall, Spaces of orderings, IV, Canad. J. Math. 32 (1980), 603-627.

[7] A. S. Merkurjev, On the norm residue symbol of degree 2, Soviet Mat. Daklady 24, 546-551 (1981).

[8] J. Mináč, Stability and Cohomological Dimension, sent to C.R. Math. Rep. Acad. Sci. Canada.

[9] J. Mináč, Poincaré polynomials and ordered fields (sent to C.R. Math. Rep. Acad. Sci. Canada).

[10] R. Ware, Quadratic forms and Profinite 2-groups, J. of Algebra, Vol. 58, No. 1, (1979), 227-237.

[11] R. Ware, Valuation rings and rigid elements in fields, Canad. J. Math. 33 (1981) 1338-1355.

[12] R. Ware, Quadratic forms and pro-2-groups III, Com. in Algebra, 13 (8), 1713-1736 (1985).

ACKNOWLEDGMENT:

This paper has been written whilst pursuing a doctoral degree at Queen's University in Kingston. I am indebted to Professors Paulo Ribenboim and T. M. Viswanathan for their encouragement and suggestions.

Added in proof. I am grateful to the referee for his suggestions which improved the exposition.

QUEEN'S UNIVERSITY, Department of Mathematics and Statistics, Kingston, Ontario, CANADA K7L 3N6

Received 25 June, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

A NOTE ON POWERFUL NUMBERS, QUADRATIC FIELDS AND THE PELLIAN

R.A. MOLLIN AND P.G. WALSH

Presented by P. Ribenboim, F.R.S.C.

The purpose of this note is to give an overview of the relationship between questions concerning powerful numbers (i.e., those positive integers n which are divisible by p^2 whenever n is divisible by the prime p), and the tools from quadratic field theory and the theory of the Pellian equation. The emphasis will be on recasting certain open powerful number problems in terms of quadratic field theory and the theory of the Pellian.

In the early 1930's Erdös and Szerkeres [2] investigated positive integers n such that p^i divides n whenever the prime p divides n where $i > 1$. In the early 1970's Golomb [3] dubbed such n with $i = 2$ as powerful numbers. Therein he conjectured the existence of infinitely many integers n which are not proper differences of two powerful numbers; i.e., not of the form $n = p - q$ where p and q are relatively prime powerful numbers. This was shown to be false by McDaniel [6] who gave an existence proof of the fact that every non-zero integer is representable in infinitely many ways as a proper difference of two powerful numbers. The authors of this note gave an elementary proof of the McDaniel result in [8] using Richaud-Degert type quadratic fields (see [1] and [11]), and the theory of the Pellian. We provided an algorithm, as well, for determining such representations. The algorithm rests on the proper choice of powers of the fundamental unit of Richaud-Degert type quadratic fields. The reader may consult [8] for examples.

In [8] and [9] we established that every integer is representable in infinitely many ways as a proper nonsquare difference of powerful numbers; i.e., as a proper difference of two powerful numbers neither of which is a perfect square. Again we provided an effective algorithm for finding such representations, and it rested upon a suitable choice of powers of the fundamental unit of certain real quadratic fields. For examples which illustrate the process the reader is referred to [9].

We now turn to some open problems and their relationship to the Pellian and quadratic field theory. As indicated by Golomb [3] it is not known whether or not there exist three consecutive powerful numbers. However, if they exist then they must be of the form (4K - 1, 4K, 4K + 1) for some K. In [8] the authors gave examples and an algorithm for finding infinitely many powerful numbers pairs of the form (4K - 1, 4K + 1), without 4K being powerful. We now translate the open problem into terms involving quadratic field theory and the theory of the Pellian via:

Theorem: The following are equivalent:

(1) There exist three consecutive powerful numbers.

(2) There exist powerful numbers P and Q with P even and Q odd such that $P^2 - Q = 1$.

(3) There exists a square-free positive integer $m \equiv 7 \pmod 8$ with $T_1 + U_1\sqrt{m}$ being the fundamental unit of $Q(\sqrt{m})$ and, for some odd integer k, T_k is an even powerful number and $U_k \equiv 0 \pmod m$ is an odd number where $(T_1 + U_1\sqrt{m})^k = T_k + U_k\sqrt{m}$.

Proof. First we demonstrate the equivalence of (1) and (2). If 3 consecutive powerful numbers exist then they are of the form (4k - 1, 4k, 4k + 1) for some positive integer k. Let Q = (4k - 1)(4k + 1) and P = 4k, then (2) follows. Conversely if $P^2 - Q = 1$ is solvable with P an even powerful number and Q an odd powerful number then 3 consecutive powerful numbers are clearly (P - 1, P, P + 1).

Now we prove the equivalence of (2) and (3). First we assume (2). Let $Q = mU^2$ where m is a square-free integer dividing U. Thus (P,U) is a solution of $x^2 - my^2 = 1$ where $m \equiv 7 \pmod 8$ since Q is odd. Let $T_1 + U_1\sqrt{m}$ be the fundamental unit of $Q(\sqrt{m})$ and let $(T_1 + U_1\sqrt{m})^k = T_k + U_k\sqrt{m}$. Hence there is a positive integer k such that $P = T_k$ and $U = U_k$. We claim that k must be odd. Since U_k is odd then from a binomial theorem expansion of U_k it follows that U_1 is odd. Since m is also odd then T_1 is even. If k were even then T_k would be odd by the binomial theorem again. However $T_k = P$ is even from which the claim and (3) follow. The converse is clear with $P = T_k$ and $Q = U_k^2 m$.

Q.E.D.

It is highly unlikely that the equivalent conditions of the Theorem hold. If they do then the solution must be so astronomical so as to be virtually unobtainable in any explicit sense. We now give evidence for this point of view.

Maintaining the notation of the Theorem one clearly has $T_k^2 - U_k^2 m = 1$ with $U_k \equiv 0 \pmod m$ if and only if $kU_1 \equiv 0 \pmod m$. One also easily sees that for any non-negative integer k, $T_{m(2k+1)} \equiv (-1)^k(2k+1)T_m \pmod{T_m^2}$ whence, if T_m is not powerful, but $T_{m(2k+1)}$ is powerful for some $k > 0$ then all primes properly dividing T_m must divide $2k + 1$. Now assume that the Theorem holds for the smallest possible m, namely $m = 7$. Since $T_7 = T_m = 2^3 \cdot 29 \cdot 197 \cdot 2857$ then, if $T_{m(2k+1)}$ is powerful for some $k > 0$, we must have $29 \cdot 197 \cdot 2857$ dividing $2k + 1$. Therefore the first possibility for the existence of 3 consecutive powerful numbers comes from $(8 + 3\sqrt{7})^{114264287}$.

If we wish to show that 3 consecutive powerful numbers do <u>not</u> exist then the Theorem tells us that we must show that for a given $m \equiv 7 \pmod 8$ the fundamental unit of $Q(\sqrt{m})$ does not satisfy the property that T_1 is even powerful while $U_1 \equiv 0 \pmod m$ is odd powerful. Moreover one must show that for a given such m and a given odd integer $k > 1$, there is a proper divisor d of k and a prime p not dividing T_d and properly dividing T_k. We conjecture that the latter holds; i.e., for odd $k > 1$, T_k can never be an even powerful. Lucas-Lehmer theory (see [5] and [6]) may be valuable in this regard. The evidence seems to indicate that as we take higher powers of $(T_1 + U_1\sqrt{m})$ proper prime divisors of T_k are always introduced. If the conjecture holds then we are left with fundamental units of $Q(\sqrt{m})$ for $m \equiv 7 \pmod 8$. If some such fundamental unit satisfies (3) of the Theorem then $U_1 \equiv 0 \pmod m$. Since $m \equiv 7 \pmod 8$ then there is a prime p dividing m where $p \equiv 3 \pmod 4$. Therefore from Yokoi [15, Proposition 1, p. 107] we have an explicit representation for the fundamental unit, namely: there is a positive integer ℓ such that $T_1 = p^2\ell \pm 2$ and $(U_1/p)^2m = p^2\ell^2 \pm 4\ell$, where $T_1^2 - U_1^2m = 4$. This representation may be valuable in solving the problem.

Another open question concerns <u>sums</u> of powerful numbers. In particular: which positive integers are a sum of two (or three) powerful numbers? We claim that all positive integers $n \not\equiv 7 \pmod 8$ are a sum of 3 powerful numbers. To see this we invoke [10, Theorem 1, p. 175] to obtain that all integers <u>not</u> of the form $4^\lambda(8\mu + 7)$, $\lambda \geq 0$, $\mu \geq 0$ are a sum of 3 integer squares. Moreover, by [10, §3, p. 178] all integers <u>not</u> of the form $2^{2\lambda+1}(8\mu + 7)$ are representable in the form $x^2 + y^2 + 2z^2$. In particular, if $\lambda > 0$ then $4^\lambda(8\mu + 7) = (2^\lambda x)^2 + (2^\lambda y)^2 + 2^{2\lambda+1}z^2$ a sum of 3 powerfuls. Hence the only positive integers n left to consider are those $n \equiv 7 \pmod 8$, as claimed. In [13] M.V. Subbarao asks "For n sufficiently large, is n a sum of 3 powerful numbers?". We conjecture that with the exception of 7, 15, 23, 87, 111 and 119 every positive integer is a sum of at most 3 powerful numbers. Evidence which we have been able to gather indicates that as n gets large the number of ways n is expressible as the sum of at most 3 powerful numbers gets large. This is made intuitively more palatable by the observation that all powerful numbers are of the form x^2y^3. For further comments on the history of sums of squares, which is a precursor to our inquiry see the well-written papers by O. Taussky-Todd [14], C. Small [12] and G. Greenfield [4].

It would be worthy of investigation to determine which primes are a sum of two powerful numbers. Clearly all primes $p \equiv 1 \pmod 4$ are a sum of two squares so we are left with those primes $p \equiv 3 \pmod 4$. Gauss gives us some information about certain $p \equiv 1 \pmod 3$; viz. If $p \equiv 1 \pmod 3$ and 2 is a cube modulo p then $p = x^2 + 27y^2$. However if $p \equiv 1 \pmod 3$ but 2 is not a cube modulo p then we may or may not have p as a sum of two powerfuls. For example 7 is not such a sum while $379 = 6^2 + 7^3$. Note that $379 \equiv 1 \pmod 7$ and the class number of $Q(\sqrt{-7})$ is 1 yielding 379 as a norm of $6 + 7\sqrt{-7}$. Which positive integers are sums of two powerful numbers in this fashion? In other words, which positive integers are a sum of two powerful numbers achievable as a norm from an imaginary quadratic field of class number 1? Are all positive integers which are a sum of two powerful numbers so achievable? Finally we ask: Which positive integers are a sum of two nonsquare powerful numbers but not as a sum of a square and a nonsquare powerful number? For example $16879 = 3^2 \cdot 2^3 + 7^5 = 2^2 + 3^3 5^2$ whereas $78157 = 2^5 + 5^7$ is not representable as a square plus a nonsquare powerful number.

It is hoped that this note provides stimulus for an investigation and solution of the open problems discussed herein, and that the quadratic field theory and the theory of the Pellian provide a framework for the inquiry.

References

[1] G. Degert, "Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlokörper", Abh. math. Sem. Univ. Hamburg 22 (1958), 92-97.

[2] P. Erdös and G. Szerkeres, "Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem", Acta Litt. Sci. Szeged 7 (1934) 95-102.

[3] S.W. Golomb, "Powerful Numbers", Amer. Math. Monthly 77 (1970), 848-852.

[4] G.R. Greenfield, "Sums of Three and Four Integer Squares", Rocky Mtn. J. Math. 13 (1983), 169-175.

[5] D.H. Lehmer, "An Extended Theory of Lucas' Functions", Annals Math. 2 (1930), 419-448.

[6] E. Lucas, "Theorie des fonctions numeriques simplement periodiques", American J. Math. 1 (1878), 184-240. (English translation available from the Fibonacci Assiciation, San Jose University, San Jose, California, 1969).

[7] W.L. McDaniel, "Representations of Every Integer as the Difference of Powerful Numbers", Fibonacci Quarterly 20 (1980), 85-87.

[8] R.A. mollin and P.G. Walsh, "On Powerful Numbers" (to appear).

[9] R.A. Mollin and P.G. Walsh, "On Nonsquare Powerful Numbers" (to appear: The Fibonacci Quarterly).

[10] L.J. Mordell, "Diophantine Equations", Academic Press, New York (1970).

[11] C. Richaud, Sur la resolution des equations $x^2 - Ay^2 = 1$, Atti. Accad. pontif. Nuori Lincei (1866), 177-182.

[12] C. Small, "Sums of Three Squares and Level of Quadratic Fields", Queen's Papers in Pure and Appl. Math. No. 46, Queen's University (1977), 625-631.

[13] M.V. Subbarao, "Problems of Halifax Number Theory Session", Canad. Math. Bull. 25 (1982) p. 381.

[14] O. Taussky-Todd, "Sums of Squares", Amer. Math. Monthly 77 (1970), 805-830.

[15] H. Yokoi, "On The Fundamental Unit of Real Quadratic Fields with Norm 1", J. Number Theory 2 (1970), 106-115.

Mathematics Department
University of Calgary
Calgary, Alberta
Canada, T2N 1N4

Received 10 September, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

PROPRIETES ARITHMETIQUES DES SERIES FORMELLES A CŒFFICIENTS DANS UN CORPS FINI

Y. HELLEGOUARCH

Presented by P. Ribenboim, F.R.S.C.

Abstract : The aim of this note is to develop an analogy between $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ and certain subfields of $\mathbf{F}_{q^2}((\frac{1}{t}))$ which we shall denote by Z, Q, R, C respectively. Proofs are omitted and a more complete version is to appear later.

1) Notations et définitions

Dans toute la suite, $\mathbf{F}_q$ désigne un corps fini à q éléments dont on suppose la caractéristique $p \neq 2$.

On écrira aussi $\mathbf{F}_{q^2} = \mathbf{F}_q(i)$, où i^2 est un non-reste de $\mathbf{F}_q$. Si -1 est un non-reste, on choisira de préférence i de telle sorte que $i^2 = -1$.

Par analogie avec la situation classique [1], on posera :

$$\begin{cases} Z = \mathbf{F}_q[t], & Q = \mathbf{F}_q(t) \\ R = \mathbf{F}_q((\frac{1}{t})), & C = \mathbf{F}_{q^2}((\frac{1}{t})) \end{cases}$$

Si $z \in C$, on a :

$$z = a_n t^n + \ldots + a_o + \frac{a_{-1}}{t} + \ldots + \frac{a_{-n}}{t^n} + \ldots$$

avec $n \in \mathbf{Z}$ et $a_n \neq 0$ si $z \neq 0$.

On pose $|z| = \rho^n$, avec $\rho > 1$, et $\sigma(z) = a_n$. Si $z = 0$, on écrit $|z| = 0$.

Le groupe $GL_2(Z)$ opère sur les droites projectives associées à Q, R et C par transformations homographiques :

$$z \longmapsto \frac{az+b}{cz+d}$$

Un certain nombre de sous-groupes de transformations agissent aussi sur Z, en particulier celui des translations $\mathcal{T} = \{z \mapsto z+\lambda,\ \lambda \in \mathbb{F}_p\}$ et celui des homothéties $\mathcal{H} = \{z \mapsto \lambda z,\ \lambda \in \mathbb{F}_q^*\}$.

2) Sommes de puissances égales

d étant un entier ≥ 1, on pose

$$S_q^h(d) = \sum_{\substack{x \in Z \\ |x|<|t|^d}} x^h , \quad Z_q^h(d) = \sum_{\substack{x \in Z,\ x \neq 0 \\ |x|<|t|^d,\sigma(x)=1}} x^h$$

En faisant agir $\mathcal{T}$ et $\mathcal{H}$ sur $\{x \in Z\ ;\ |x|<|t|^d\}$ et $\mathcal{T}$ sur $\{x \in Z\ ;\ x \neq 0,\ \sigma(x) = 1,\ |x|<|t|^d\}$ on a le résultat suivant :

Théorème 1 :

1) $S_q^h(d) = S_q^h(0)Z_q^h(d)$

2) Si h n'est pas un multiple de q-1, $S_q^h(d) = 0$.

3) Si p ne divise aucun des dénominateurs des nombres $\frac{1}{h+1}, \binom{h+1}{1}\frac{B_1}{h+1}, \binom{h+1}{2}\frac{B_2}{h+1}, \ldots, \frac{B_h}{h+1}$, où les B_i sont les nombres de Bernoulli, alors $S_q^h(d) = 0$.

Contre-exemples : $S_3^2(0) = 1+1 = -1$, $Z_3^2(1) = 0$.

Fonction zêta

On désire développer $\frac{1}{x^h}$, pour $h \geq 1$, en série en $\frac{1}{t}$. Pour cela, on pose :

$$x = a_n t^n + \ldots + a_o = a_n t^n [1+t^{-1} R(t^{-1})]$$

avec $R(X) = a_n^{-1}(a_{n-1}+a_{n-2}X + \ldots + a_o X^{n-1})$. On a alors :

$$\frac{1}{x^h} = a_n^{-h} t^{-nh} \sum_{i=0}^{\infty} \binom{-h}{i} t^{-i} R^i(t^{-1})$$

avec $\binom{-h}{i} \in \mathbb{F}_p$ quel que soit p, donc cette série a un sens.

Définition : Si h est un entier ≥ 1, on pose

$$s(h) = \sum_{\substack{x \in Z \\ x \neq 0}} \frac{1}{x^h} \quad , \quad \zeta(h) = \sum_{\substack{x \in Z \\ x \neq 0 \\ \sigma(x)=1}} \frac{1}{x^h} .$$

Théorème 2 :

1) $s(h) = S_q^h(0)\zeta(h)$

2) $s(h) = 0$, dans les conditions du théorème 1.

3) $\prod_{p \in \mathcal{P}} \frac{1}{1-p^{-h}} = \zeta(h)$ où $\mathcal{P}$ désigne l'ensemble des polynômes unitaires irréductibles de Z.

4) $\zeta(h) \equiv 1 \pmod{t^{-1}}$.

3) Description de l'action de $GL_2(Z)$ sur R

Remarquons que l'algorithme des fractions continues correspond à l'action du sous-groupe $G \subset GL_2(Z)$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que : $ad-bc = \pm 1$. Si l'on pose $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $h_M(z) = \frac{az+b}{cz+d}$, l'homomorphisme $M \longmapsto h_M$ a pour noyau l'ensemble des matrices $\begin{pmatrix} \lambda & o \\ o & \lambda \end{pmatrix}$, avec $\lambda \in \mathbb{F}_q^*$. Il en résulte que si $\det M = \lambda^2$, avec $\lambda \in \mathbb{F}_q^*$, il existe $M' \in SL_2(Z)$ tel que $h_{M'} = h_M$. Donc si -1 n'est pas un carré dans $\mathbb{F}_q$, $GL_2(Z)$ et G ont même action sur R et C.

Théorème 3 (Serret) :

Pour que z_1 et $z_2 \in R$ aient la même orbite pour l'action de G, il faut et il suffit qu'il existe $\lambda \in \mathbb{F}_q^*$ tel que z_2 et $\pm \lambda^2 z_1$ aient même développement en fraction continue à partir d'un certain rang.

Corollaire :

Supposons que -1 ne soit pas un reste quadratique dans F_q. Pour que z_1 et z_2 aient la même orbite dans l'action de $GL_2(Z)$ il faut et il suffit qu'il existe $\lambda \in F_q^*$ tel que z_2 et λz_1 aient même développement en fraction continue.

Finalement, le théorème de Lagrange se généralise aussi [2] :

Théorème 4 :

Pour que le groupe d'isotropie de $z \in R$, pour l'action de $GL_2(Z)$ ou de G, ne soit pas trivial, il faut et il suffit que le développement en fraction continue de z soit fini ou périodique.

4) Description de l'action de $GL_2(Z)$ sur $C \setminus R$

Supposons que l'on ait :

$$z = \frac{az+b}{cz+d}, \quad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(Z)$$

avec z dans une clôture algébrique de R. On en déduit que $z \in Q(\sqrt{\Delta})$ avec :

$$\Delta = (\mathrm{tr}\ M)^2 - 4 \det M$$

Il est clair que $\sqrt{\Delta} \in C$, donc que $z \in C$.

Ceci conduit à étendre la classification classique des transformations homographiques de la manière suivante :

$$M \text{ est parabolique} \Longleftrightarrow (\mathrm{tr}\ M)^2 = 4 \det M$$

$$M \text{ est hyperbolique} \Longleftrightarrow |\mathrm{tr}\ M| > 1$$

$$M \text{ est elliptique} \Longleftrightarrow \begin{cases} (\mathrm{tr}\ M)^2 \neq 4 \det M \\ |\mathrm{tr}\ M| \leq 1 \end{cases}$$

Domaine fondamental de C

On appellera "domaine fondamental" de C, l'ensemble D des points $x+iy$ tels que $|x| < 1$, $|y| > 1$ et $\sigma(y) = 1$.

Théorème 5 :

1) L'orbite de tout point de $C \setminus R$ pour l'action de $GL_2(Z)$ rencontre D.

2) Si (x,y) et (x',y') sont dans D et si

$$\begin{cases} |x| < 1, & |x'| < 1 \\ |y| > 1, & |y'| > 1 \end{cases}$$

Alors (x,y) et (x',y') ne peuvent avoir la même orbite que s'ils sont égaux.

5) Réseaux de C

Définition : Un Z-module $\Gamma \subset C$ est appelé un réseau, s'il existe une R-base (e_1,e_2) de C qui est une Z-base de Γ.

Si Γ et Γ' sont deux réseaux de C, on dit que Γ et Γ' sont équivalents s'il existe $\gamma \in Q(i)$ tel que $\Gamma' = \gamma\Gamma$. Si $\Gamma' = (e_1',e_2')$, on a :

$$\frac{e_1'}{e_2'} = \frac{ae_1+be_2}{ce_1+de_2} \quad \text{avec} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(Z).$$

En choisissant $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ convenablement, on voit (théorème 5) que l'on peut avoir $\frac{e_1'}{e_2'} \in D$.

Soit $\mathcal{R}$ l'ensemble des réseaux de C et $f : \mathcal{R} \to C$. On dira que f est une fonction de réseau de poids 2k lorsque :

$$f(\lambda\Gamma) = \lambda^{-2k} f(\Gamma)$$

6) <u>Séries d'Eisenstein</u>

Il s'agit d'exemples de fonctions de réseaux de poids 2k.

On considère un réseau Γ et la série double $\Sigma' \frac{1}{j^{2k}}$. En choisissant une base (e_1, e_2) de Γ telle que $\frac{e_1}{e_2} \in D$, on voit facilement que cette série converge dès que $k > 1$.

En effet :

$$|me_1+ne_2| = |e_2||mz+n| \text{ avec } z = \frac{e_1}{e_2} \in D.$$

On voit donc que :

$$|me_1+ne_2| = |e_2| \sup(|y||m|, |xm+n|)$$

et qu'il n'y a qu'un nombre fini de points $\gamma \in \Gamma$ tels que $|\gamma| < C^{te}$. Ceci assure la convergence de la série.

<u>Définition</u> : On pose :

$$E_k(\gamma) = \sum_{\substack{\gamma \in \Gamma \\ \gamma \neq 0}} \frac{1}{\gamma^{2k}} \quad \text{et} \quad G_k(\Gamma) = \sum_{\substack{\gamma \in \Gamma \\ \gamma \neq 0 \\ \sigma(\gamma)=1}} \frac{1}{\gamma^{2k}}$$

<u>Théorème 6</u> :

1) $E_k(\Gamma) = S^{2k}_{q^2}(0)\, G_k(\Gamma)$

2) $G_k(\Gamma)$ n'est pas identiquement nul car $G_k(Z+Zi) = \zeta_{\mathbb{F}_{q^2}}(2k)$

3) $\lim\limits_{|z|\to\infty} E_k(Z+Zz) = s_{\mathbb{F}_q}(2k)$

$\lim\limits_{|z|\to\infty} G_k(Z+Zz) = \zeta_{\mathbb{F}_q}(2k)$.

<u>REFERENCES</u>

[1] J.P. SERRE.- Cours d'Arithmétique P.U.F. 1970.

[2] E. ARTIN.- "Quadratische Körper im Gebiete der höheren Kongruenzen I" in "The Collected papers of Emil Artin", Addison-Wesley. 1965.

Received 7 October, 1985

<u>Université de CAEN, FRANCE</u>

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

PRINCIPAL PIVOT TRANSFORMS OF AN EP MATRIX

AR. Meenakshi

Presented by G. de B. Robinson, F.R.S.C.

1. Introduction:

All matrices considered here are complex matrices. The conjugate transpose of a matrix A is denoted by A^*. A square matrix A is called EP if $N(A) = N(A^*)$ where $N(A)$ is the null space of A or equivalently $AA^+ = A^+A$ where A^+ is the Moore Penrose inverse of A ; further if A is of rank r, it is called EP_r. It is well known that [2, Lemma 3 on p. 92] the class of EP matrices is invariant under principal rearrangements. (By a principal rearrangement of a square matrix M we mean a matrix $\overline{M} = P^TMP$ where P is a permutation matrix). However the property of a matrix being EP is not inherited by each of its principal submatrices. In our earlier paper, we have shown that in an EP_r matrix each of its principal submatrices of rank r is EP_r. (See corollary 4 in [6]). Throughout we shall consider a matrix M of the form,

$$(1.1) \qquad M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

The generalized Schur complement of A in M is a matrix $M/A = D - CA^-B$, where A^- is a generalized inverse of A satisfying $AXA = A$. Similarly we define $M/D = A - BD^-C$. We require the following relations between null spaces of $A,B,C,M/A$:

$$(1.2) \qquad N(A) \subseteq N(C)$$

$$(1.3) \qquad N(A^*) \subseteq N(B^*)$$

$$(1.4) \qquad N(M/A) \subseteq N(B)$$

$$(1.5) \qquad N(M/A)^* \subseteq N(C^*)$$

By Lemma 7 in [7, p. 21] M/A is invariant for all choices of A^- of A if and only if A satisfies (1.2) and (1.3) or equivalently (1.6) $C = CA^-A$ and $B = AA^-B$, for every A^- of A. Thus under certain conditions $M/A = D - CA^+B$ [4]. Here we give necessary and sufficient conditions for an EP matrix to have its principal submatrices and their Schur complements to be EP. This is a generalization of the result found in [1]. As an application it is shown that the property of a matrix being EP_r is preserved under the principal pivot transformation.

2. Principal Pivot on a matrix:

Let us consider a system of linear equations $Mz = t$ where M is of the form (1.1) satisfying (1.2) and (1.3). If z and t are artitioned conformably as $z = \begin{bmatrix} x \\ y \end{bmatrix}$ and $t = \begin{bmatrix} u \\ v \end{bmatrix}$, then the system becomes

$$Ax + By = u \; ; \; Cx + Dy = v$$

Since M satisfies (1.2) and (1.3) using (1.6) we can solve for x and v as

$$x = A^+u - A^+By \; ; \; v = CA^+u + (D - CA^+B)y$$

Thus a matrix M of the form (1.1) that satisfies (1.2) and (1.3) can be transformed into the matrix

$$(2.1) \qquad \tilde{M} = \begin{bmatrix} A^+ & -A^+B \\ CA^+ & M/A \end{bmatrix}$$

$\tilde{M}$ is called a principal pivot transform of M. The operation that transforms $M \to \tilde{M}$ is called a principal pivot. If A is non-singular it reduces to the principal pivot by pivoting the block A [8]. Properties and applications of the principal pivot transforms are well recognized in Mathematical programming [8,9]. The principal pivot transformation is also called a gyration [5].

Lemma 1: Let M be a matrix of the form (1.1) with $N(A) \subseteq N(C)$ and $N(D) \subseteq N(B)$. Then the following are equivalent:

(i) M is EP with $N(M/A) \subseteq N(B)$ and $N(M/D) \subseteq N(C)$.

(ii) $A, D, M/A$, M/D are all EP. Further $N(A) = N(M/D) \subseteq N(B^*)$ and $N(D) = N(M/A) \subseteq N(C^*)$.

Proof: (i) => (ii) Since M is EP with $N(A) \subseteq N(C)$ and $N(M/A) \subseteq N(B)$, by Theorem 1 in [6] A and M/A are EP; $N(A^*) = N(A) \subseteq N(B^*)$ and $N(M/A)^* \subseteq N(C^*)$. Since M is EP, the principal rearrangement $P^T MP = \begin{bmatrix} D & C \\ B & A \end{bmatrix}$ is also EP. Further $N(D) \subseteq N(B)$ and $N(M/D) \subseteq N(C)$ hold. Hence by Theorem 1 in [6] D and M/D are EP, $N(D^*) = N(D) \subseteq N(C^*)$, and $N(M/D) \subseteq N(B^*)$. Since the relations (1.2) to (1.5) hold for A according to the assumptions they can be applied to (v) of Theorem 1 of the paper [3] so that M^+ is given by the formula

$$M^+ = \begin{bmatrix} A^+ + A^+B(M/A)^+CA^+ & -A^+B(M/A)^+ \\ -(M/A)^+CA^+ & (M/A)^+ \end{bmatrix} \tag{2.2}$$

By using $C = (M/A)(M/A)^+C$ and $B = AA^+B$, MM^+ reduces to the form

$$MM^+ = \begin{bmatrix} AA^+ & 0 \\ 0 & (M/A)(M/A)^+ \end{bmatrix} \tag{2.3}$$

Since the relations (1.2) to (1.5) hold for A as well as D according to the assumptions, by corollary 1 in [3] M^+ is also given by the formula

$$(2.4) \qquad M^{+} = \begin{bmatrix} (M/D)^{+} & -A^{+}B(M/A)^{+} \\ -D^{+}C(M/D)^{+} & (M/A)^{+} \end{bmatrix}$$

Further, using $B = AA^{+}B$ and $C = DD^{+}C$ in (2.4), MM^{+} reduces to the form

$$(2.5) \qquad MM^{+} = \begin{bmatrix} (M/D)(M/D)^{+} & 0 \\ 0 & (M/A)(M/A)^{+} \end{bmatrix}$$

Comparing (2.3) and (2.5) we get $AA^{+} = (M/D)(M/D)^{+}$. Since A and M/D are EP , we have $A^{+}A = (M/D)^{+}(M/D)$ which implies $N(A) = N(M/D)$. Similarly using the formulae (2.2) and (2.4) we obtain two expressions for $M^{+}M$. Comparing these yields $D^{+}D = (M/A)^{+}(M/A)$ which implies $N(D) = N(M/A)$. Thus (ii) holds.

Proof: (ii) => (i) : $N(M/A) \subseteq N(B)$ follows directly from $N(M/A) = N(D) \subseteq N(B)$. Similarly $N(M/D) \subseteq N(C)$ follows from $N(M/D) = N(A) \subseteq N(C)$. Now A and M/A are EP satisfying the relations (1.2) to (1.5). Hence by Theorem 1 in [6] M is EP . Thus (i) holds. The proof is complete.

Theorem 1: Let M be an EP_r matrix of the form (1.1) with $N(A) \subseteq N(C)$; $N(D) \subseteq N(B)$; $N(M/A) \subseteq N(B)$ and $N(M/D) \subseteq N(C)$. Then the following hold:

(i) Principal sumatrices A and D are EP .

(ii) The Schur complements M/A and M/D are EP .

(iii) Each principal pivot transforms of M is EP_r .

Proof: (i) and (ii) are consequence of Lemma 1.

(iii): By Lemma 1, M satisfies (1.2) and (1.3), hence by pivoting the block A , the principal pivot transform $\tilde{M}$ of M is of the form (2.1). In $\tilde{M}$, $N(A^+) \subseteq N(CA^+)$ and $N(A^+)^* \subseteq N(A^+B)^*$. Further $\tilde{M}/A^+ = M/A + CA^+B = D$. By the assumption $N(\tilde{M}/A^+) = N(D) \subseteq N(B)$. From Lemma 1, A and D are EP ; therefore A^+ and $\tilde{M}/A^+$ are EP, $N(\tilde{M}/A^+)^* = N(D^*) \subseteq N(C^*)$. Now by applying Theorem 1 of [6] we see that $\tilde{M}$ is EP. The proof of rank $\tilde{M}$ = rank M = r runs as follows:

$$\begin{aligned} r &= rk(M) = rk(A) + rk(M/A) && \text{(By Theorem 1 in [4])} \\ &= rk(A^+) + rk(D) && (rk\ A = rk\ A^+ \text{, by Lemma 1,} \\ & && N(D) = N(M/A)) \\ &= rk(A^+) + rk(\tilde{M}/A^+) && \\ &= rk\ \tilde{M} && \text{(By Theorem 1 in [4]).} \end{aligned}$$

Thus $\tilde{M}$ is EP_r. Similarly under the conditions given on M, M can be transformed to its principal pivot transform by pivoting the block D without changing the rank. Hence the theorem.

Remark 1: In particular if M is positive semi definite, then the conditions in Lemma 1 automatically hold and the Lemma reduces to Albert's result [1]. Further we note that $N(A) = N(M/D)$ and $N(D) = N(M/A)$.

Remark 2: In the special case when M is nonsingular with A and D nonsingular then the conditions $N(A) \subseteq N(C)$ and $N(D) \subseteq N(B)$ automatically hold and by Theorem 1 in [4], M/A and M/D are non-singular; further $rk(\tilde{M}) = rk\ A + rk\ D$. Hence it follows that each principal pivot transform of M is nonsingular. However we note that the nonsingularity of $\tilde{M}$ need not imply that M is nonsingular.

Example 1: Let $M = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 3 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ with $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$B = C^* = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}$$

Here A and D are nonsingular and $M/A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ is EP_1.

$\mathrm{rk}\, M = \mathrm{rk}\, A + \mathrm{rk}(M/A) = 3$. Since M is symmetric, M is EP_3.

By (2.1), $\tilde{M} = \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ is nonsingular. Thus $\tilde{M}$ is EP_4.

Remark 3: By considering the matrix M in Example 1, we note that the conditions $N(M/A) \subseteq N(B)$ and $N(M/D) \subseteq N(C)$ fail and the statement (iii) of Theorem 1 does not hold.

References:

1. Albert, A., Conditions for positive and nonnegative definiteness in terms of Pseudo inverses, SIAM J. Appl. Math. 17 (1969) 434-440.

2. Baskett, T.S. and Katz, I.J., Theorems on products of EP_r matrices, Linear Algebra and Appl. 2 (1969) 87-103.

3. Burns, F., Carlson, D., Haynsworth, E. and Markham, T., Generalized inverse formulas using the Schur complement, SIAM J. Appl. Math. 26 (1974) 254-259.

4. Carlson, D., Haynsworth, E. and Markham, T., A generalization of the Schur complement by means of the Moore Penrose inverse, SIAM J. 26 (1974) 169-195.

5. Duffin, R.J., Hazony, D. and Morrison, N., Network synthesis through hybrid matrices, SIAM J. Appl. Math 14 (1966) 390-413.

6. Meenakshi, AR., On Schur complements in an EP matrix, Periodica. Math. Hung. 16 (1985) 44-51.

7. Rao, C.R. and Mitra, S.K., Generalized inverse of matrices and its applications; Wiley, New York, 1971.

8. Tucker, A.W., Combinatorial Analysis (Bellman and Hall, Eds.), American Math. Soc., Providence, RI (1960) 129-140.

9. Tucker, A.W., Principal pivot transforms of square matrices, SIAM Rev. 5 (1963) 305.

Received 21 October, 1985

Department of Mathematics
Annamalai University
Annamalainagar - 608 002
INDIA

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

NOTE ON HYERS'S THEOREM

L.Székelyhidi

Presented by J. Aczél, F.R.S.C.

ABSTRACT. In this note we prove that on a semigroup the validity of Hyers's theorem for complex valued functions implies its validity for functions with values in semi-reflexive locally convex linear topological spaces.

Given a semigroup G, we say that Hyers's theorem holds for G if the following statement is valid : for every $\varepsilon > 0$ there exists $\delta > 0$ such that, if $f : G \to \mathbb{C}$ ($\mathbb{C}$ being the set of complex numbers) satisfies $|f(xy) - f(x) - f(y)| < \delta$ for all x,y in G, then a homomorphism $a : G \to \mathbb{C}$ exists with $|f(x) - a(x)| < \varepsilon$ for all x in G. Hyers's theorem in its original form [1] states that the additive group of any Banach space possesses this property. Further it can be shown ([2], Theorem 4; [3]) that Hyers's theorem holds for any abelian group or, more generally, for any amenable semigroup, or for any power-associative grupoid whenever f satisfies a weak commutativity condition. Theorem 5 in [2] settles the uniqueness question for the homomorphism a. It is also possible to generalize Hyers's theorem with respect to the range of the function f with the above property to more general spaces instead of the complex field. The aim of this note is to show that the validity of Hyers's theorem for complex valued functions implies its validity for functions with values in semi-reflexive locally convex linear topological spaces; "semi-reflexive" means that the natural embedding from X into X^{**} is bijective. We note that the same technique works also in the case of functions with bounded n-th differences.

THEOREM Let G be a semigroup for which Hyers's theorem holds, and let X be a semi-reflexive locally convex linear topological (Hausdorff) space. If $f : G \to X$ is a function for which the function

$$(x,y) \to f(xy) - f(x) - f(y)$$

is bounded, then there exists a homomorphism $A : G \to X$ for which $f - A$ is bounded.

Research partially supported by a grant from the Swiss National Foundation

PROOF. Let Φ be any continuous linear functional on X and let $F = \Phi \circ f$. Then the function $F : G \to \mathbb{C}$ obviously has the property, that $(x,y) \to F(xy) - F(x) - F(y)$ is bounded. Then by assumption

$$F = a_\Phi + k_\Phi$$

where $a_\Phi : G \to \mathbb{C}$ is a homomorphism and $k_\Phi : G \to \mathbb{C}$ is bounded. As any bounded homomorphism of G into $\mathbb{C}$ is identically zero, it follows that the mapping $\Phi \to a_\Phi$ is well defined and linear. Let z be a fixed element in G. We define the functional $A(z)$ on X^* as follows:

$$< A(z), \Phi > = a_\Phi(z) \quad .$$

Obviously $A(z)$ is a linear functional on X^*. We show that $A(z)$ is a continuous linear functional on X^*, the latter is being equipped with the topology of uniform convergence on bounded sets. Let $\{\Phi_\alpha\}$ be any net converging to zero in X^*, and let $\varepsilon > 0$ be arbitrary. Then, by the assumed property of G, there exists $\delta > 0$ such that, for any function $h : G \to \mathbb{C}$ with $|h(xy) - h(x) - h(y)| < \delta$ for all x,y in G, there exists a unique homomorphism $a : G \to \mathbb{C}$ with $|h(x) - a(x)| < \varepsilon/2$ for all x in G. On the other hand, there exists α_1 such that for $\alpha > \alpha_1$ we have $|\Phi_\alpha(f(xy) - f(x) - f(y))| < \delta$, that is, with the notation $F_\alpha = \Phi_\alpha \circ f$, $|F_\alpha(xy) - F_\alpha(x) - F_\alpha(y)| < \delta$ for all x,y in G. This implies $|k_{\Phi_\alpha}(x)| < \varepsilon/2$ for all x in G. Further, there exists α_2 such that for $\alpha > \alpha_2$ we have $|\Phi_\alpha(f(z))| < \varepsilon/2$, and hence for $\alpha_0 > \alpha_1$, $\alpha_0 > \alpha_2$ and $\alpha > \alpha_0$ we have

$$|<A(z), \Phi_\alpha>| = |a_{\Phi_\alpha}(z)| = |\Phi_\alpha(f(z)) - k_{\Phi_\alpha}(z)| \le |\Phi_\alpha(f(z))| + |k_{\Phi_\alpha}(z)| < \varepsilon,$$

that is, $A(z)$ is continuous. By the semi-reflectivity of X, $A(z)$ can be identified with an element of X, and hence A can be considered as a map of G into X. It is easy to see that $A : G \to X$ is a homomorphism. Finally, the range of the function $f - A$ is weakly bounded, as

$$\Phi(f(x) - A(x)) = \Phi(f(x)) - \Phi(A(x)) = \Phi(f(x)) - a_\Phi(x) = k_\Phi(x)$$

for all x in G, and k_Φ is bounded. But X is locally convex, and hence weakly bounded sets are bounded, and our theorem is proved.

COROLLARY Let G be an amenable semigroup and X a semi-reflexive locally convex linear topological (Hausdorff) space. If $f : G \to X$ is a function for which the function $(x,y) \to f(xy) - f(x) - f(y)$ is bounded, then there exists a homomorphism $A : G \to X$ for which $f - A$ is bounded.

REFERENCES

[1] D.H.Hyers, On the stability of the linear functional equation, Proc. Nat.Acad.Sci. USA 27(1941), 222-224.

[2] J.Rätz, On approximately additive mappings, General Inequalities 2 (ed. E.F.Beckenbach), ISNM Vol. 47, Birkhäuser, Basel, 1980, 233-251.

[3] L.Székelyhidi, The Fréchet equation and Hyers's theorem on noncommutative semigroups, (submitted to Ann.Polon.Math.)

Department of Mathematics
L.Kossuth University
H-4010 Debrecen, Pf.12.
HUNGARY

Received 4 November, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

EXTENSIONS OF CERTAIN GROUP RING PROPERTIES TO ALTERNATIVE LOOP RINGS

Edgar G. Goodaire and M. M. Parmenter

Presented by G. de B. Robinson, F.R.S.C.

ABSTRACT

In this paper we explain that certain well-known properties of group rings, in particular concerning radicals and units, hold more generally in the wider class of alternative loop rings.

0. INTRODUCTION

A loop is a set L together with a binary operation $(g,h) \mapsto gh$ for which there is a two-sided identity element and with the property that the left and right multiplication maps determined by any element of L are one-one and onto. Given any associative and commutative ring R, one can mimic the construction of the group ring to form the loop ring RL. Despite ample evidence to suggest that associativity is the only interesting identity to be found in a loop ring, the first author discovered several years ago a class of Moufang loops whose loop rings are alternative, but not associative; that is, they satisfy the laws $(yx)x = yx^2$, $x(xy) = x^2y$ (and their many consequences), but not $(xy)z = x(yz)$ [4]. More recently, Marshall Osborn [8] has discovered a class of non-commutative Jordan loop rings. These are rings which satisfy the identities $(xy)x = x(yx)$ and $(xy)x^2 = x(yx^2)$. It is therefore apparent that while most loop rings are ugly objects (most are not even power associative), some of them, besides the popular group ring, are worthy of attention.

Since any group ring is an alternative ring, it is reasonable to ask if a given property of group rings is perhaps more generally a property of an alternative loop ring. Such questions, particularly concerning radicals and units in group rings, have been recent subjects of our investigations and it is the purpose of

The research upon which this paper is based was supported in part by the Natural Sciences and Engineering Research Council of Canada, Grants No. A9087 and A8775.

this note to highlight some of the prettier results we have obtained. Several well-known results about units in group rings have natural extensions to alternative loop rings; our theorems about radicals generally illustrate properties peculiar to the nonassociative case. We refer the reader to [5] and [6] for details.

1. RADICALS

In this section, R is any commutative associative ring with identity and L is a loop whose loop ring RL is alternative, but not associative. Of basic importance is the following result.

Lemma. Every non-zero ideal of RL contains a non-zero central element.

This lemma is the key to proving, for example,

Theorem 1. RL is semi-prime if and only if RL contains no non-zero nil ideals. Therefore RL is semi-simple with respect to a particular nil radical if and only if RL is semi-simple with respect to any other nil radical.

The centre of any loop L is an abelian group A. When RL is alternative, properties of RL are often related to properties of the abelian group ring RA.

Theorem 2. RL is semiprime if and only if RA is semiprime. RL is semi-simple with respect to the Jacobson radical if and only if RA is semi-simple (with respect to the Jacobson radical).

Necessary and sufficient conditions for any group ring to be semi-prime are known, as are conditions for Jacobson semi-simplicity of an abelian group ring [3]. Therefore, because of Theorem 2, we know precisely when an alternative loop ring is semi-prime or Jacobson semi-simple. It is interesting that the question of Jacobson semi-simplicity in the associative case is unsettled, even over fields of characteristic zero.

2. UNITS

In this section, all loop rings are integral (i.e. the coefficient ring is the ring Z of integers) and, unlike the previous section, the term "alternative ring" will include the associative case unless otherwise noted. The determination of the group of units in a group ring is an on-going process in the theory of group rings. In any group ring, the elements of ± G are obviously units; such units are called trivial. Many of the early results about units in group rings give conditions under which certain types of units are trivial. It turns out that several such theorems extend to alternative loop rings in a very natural way; for example the following theorem, which was established for group rings by Cohn and Livingstone [2].

Theorem 3. Central units of finite order in an alternative loop ring are trivial.

In 1940, Graham Higman found necessary and sufficient conditions for all the units in an integral group ring of a periodic group to be trivial [7]. Higman's Theorem extends beautifully to the alternative case. (A loop is Hamiltonian if all its subloops are normal.)

Theorem 4. Suppose L is a periodic loop. Then ZL is an alternative ring in which all units are trivial if and only if L is an abelian group of exponent 2, 3, 4 or 6 or a Hamiltonian Moufang 2-loop.

A result due to S. D. Berman [1] characterizes those finite groups whose group rings have the property that all the torsion units are trivial. Berman's result is a special case of

Theorem 5. Let L be a finite loop. Then ZL is an alternative loop ring in which all torsion units are trivial if and only if L is an abelian group or a Hamiltonian Moufang 2-loop.

We conclude with a result which illustrates one difference between the associative and nonassociative situations. The authors are unaware of any published result which gives necessary and sufficient conditions for all the central units in a group ring to be trivial. In any case, the following Theorem is certainly not true for group rings. Once again we note the role that the group ring of the centre of a loop plays in the structure of an alternative loop ring.

Theorem 6. Suppose L is a periodic Moufang loop and ZL is an alternative loop ring which is not associative. Let A denote the centre and L′ the commutator subloop of L. Then the central units in ZL are trivial $\iff$ all units in ZA and Z(L/L′) are trivial; that is, $\iff$ both A and L/L′ are abelian groups of exponent 2, 3, 4 or 6.

REFERENCES

[1] S. D. Berman, On the equation $x^m = 1$ in an integral group ring, Ukrain. Mat. Z. 7 (1955), 253-261.

[2] J.A. Cohn and D. Livingstone, On the structure of group algebras, Can J. Math. 17 (1965), 583-593.

[3] Ian G. Connell, On the Group Ring , Can. J. Math 15 (1963), 650-667.

[4] Edgar G. Goodaire, Alternative Loop Rings, Publ. Math. Deb. 30 (1983), 31-38.

[5] Edgar G. Goodaire and M.M. Parmenter, Semi-Simplicity of Alternative Loop Rings, Acta Math. Hungar., to appear.

[6] Edgar G. Goodaire and M. M. Parmenter, Units in Alternative Loop Rings, Israel J. of Math., to appear.

[7] Graham Higman, The Units of Group Rings, Proc. London Math. Soc (2), 46 (1940), 231-248.

[8] Osborn, J. Marshall, Lie-Admissible Noncommutative Jordan Loop Rings, preprint (1985).

Department of Mathematics and Statistics,
Memorial University of Newfoundland,
St. John's, Newfoundland
Canada A1C 5S7

Received 20 December, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol.VIII, No. 2, Apr. 1986 avr.

HIGHER ORDER POLYMORPHIC LAMBDA CALCULUS AND CATEGORIES

R.A.G. Seely

Presented by J. Lambek, F.R.S.C.

Abstract A categorical semantics is presented, suitable for interpretations of the polymorphic lambda calculus of Girard and Reynolds; indeed, an equivalence of categories is established between such categories and the type theories. To illustrate the semantics, the well-known $P\omega$ model is presented in this context.

0. Introduction Since its development in the early 1970's by Girard [2] (and independently Reynolds [4]) the polymorphic lambda calculus (PLC) has been the object of increasing study. In this note we define a categorical structure suitable for interpreting PLC, thus providing a smooth, algebraic semantics for PLC. There are several variants of PLC in the literature; I present one which is similar to that of [1], so that the comparison with the semantics presented there may be easily made. (I have described the $P\omega$ model in some detail for the same reason.) However, I have kept the higher order feature of Girard's original system, since it makes for no extra difficulty.

1. Definition 1 A PL theory consists of collections of orders, operators (including types), and terms, and relations ϵ (giving the order of an operator and the type of a term) and = (between operators of the same order and between terms of the same type.) Each collection may have given constant symbols; in addition we have the following rules:

Orders: 1, Ω are orders; if A, B are orders, so are $A \times B$, Ω^A.

Operators: For each order, there is a countable set of variable operators ("indeterminates"). $* \in 1$.

If s, $t \in \Omega$ and α is an indeterminate of order A, then $s \wedge t$, $s \supset t$, and $\Pi\alpha\epsilon A.s \in \Omega$.

(PI) If α is an indeterminate of order A, $s \in \Omega$, then $[\alpha\epsilon A:s] \in \Omega^A$.

(PE) If $t \in A$, $s \in \Omega^A$, then $s(t) \in \Omega$.

(×I) If $s \in A$, $t \in B$, then $<s,t> \in A \times B$.

(×E) If $s \in A \times B$, then $\pi_1 s \in A$, $\pi_2 s \in B$.

Operators of order Ω are called <u>types</u>.

<u>Terms</u>: For each type there is a countable set of variable terms.

(⊃I) If $a \in t$, x a variable of type s, then $\lambda x \in s.a \in s \supset t$.

(⊃E) If $a \in s \supset t$, $b \in s$, then $a(b) \in t$.

(∧I) If $a \in s$, $b \in t$, then $<a,b> \in s \wedge t$.

(∧E) If $a \in s \wedge t$, then $\pi_1 a \in s$, $\pi_2 a \in t$.

(ΠI) If $a \in s$, α an indeterminate of order A not free in the type of any free variable in a, then $\Lambda\alpha\in A.a \in \Pi\alpha\in A.s$.

(ΠE) If $a \in \Pi\alpha\in A.s$, $t \in A$, then $a\{t\} \in s[t/\alpha]$ (t replaces α in s).

<u>Equalities</u>: In addition to the usual rules for reflexivity, symmetry, transitivity, substitution, and change of bound variables, and equalities imposed by the particular theory, we have:

<u>for operators</u>: (P red) $[\alpha:s](t) = s[t/\alpha]$ (P exp) $s = [\alpha:s(\alpha)]$

(× red) $\pi_i<s_1,s_2> = s_i$ $(i=1,2)$ (× exp) $s = <\pi_1 s, \pi_2 s>$

<u>for terms</u>: (⊃ red) $(\lambda x.a)(b) = a[b/x]$ (⊃ exp) $a = \lambda x.\ a(x)$

(∧ red) $\pi_i<a_1,a_2> = a_i$ $(i=1,2)$ (∧ exp) $a = <\pi_1 a, \pi_2 a>$

(Π red) $(\Lambda\alpha.a)\{t\} = a[t/\alpha]$ (Π exp) $a = \Lambda\alpha.\ a\{\alpha\}$

<u>Definition 2</u> A <u>PL category</u> (<u>G</u>, <u>S</u>) consists of:

(i) a category <u>S</u> with finite products, a distinguished object Ω, and exponentiation of the form Ω^A for A in <u>S</u>, (<u>i.e.</u> for each A, there is an object Ω^A so that $\mathrm{Hom}(B,\Omega^A) \cong \mathrm{Hom}(A\times B,\Omega)$.)

(ii) an indexed category <u>G</u> over <u>S</u>, satisfying

(a) for each A in <u>S</u>, $\mathrm{Obj}(\underline{G}(A)) = \mathrm{Hom}(A,\Omega)$, and for each $f: A \to B$, $f^* = \underline{G}(f)$ acts as $\mathrm{Hom}(f,\Omega)$ on objects.

(b) for each A in <u>S</u>, <u>G</u>(A) is cartesian closed, and this structure is preserved by all f^*.

(c) <u>G</u> is "complete": for each C in <u>S</u>, the canonical indexed functor $\kappa:\underline{G} \to \underline{G}^C$ has a right adjoint $\Pi:\underline{G}^C \to \underline{G}$.

2. An <u>interpretation</u> I of a PL theory <u>T</u> in a PL category (<u>G</u>, <u>S</u>) is a function which sends orders of <u>T</u> to objects of <u>S</u>, operators of <u>T</u> to morphisms of <u>S</u>, and terms of <u>T</u> to morphisms of <u>G</u>(A), for appropriate A. I must satisfy certain conditions; I shall only give a brief summary of the highlights.

$\mathcal{I}(1) = 1$, $\mathcal{I}(\Omega) = \Omega$, $\mathcal{I}(A \times B) = \mathcal{I}(A) \times \mathcal{I}(B)$, $\mathcal{I}(\Omega^A) = \Omega^{\mathcal{I}(A)}$. $\mathcal{I}(\alpha) = \mathrm{id}: \mathcal{I}(A) \to \mathcal{I}(A)$, where $\alpha \in A$. $\mathcal{I}(*) = \mathrm{id}_1$. $\mathcal{I}$ is defined for $s \wedge t$, $s \supset t$ via the cartesian closedness of $\underline{G}$, and for $\Pi\alpha\epsilon A.s$ by composition with Π. $\mathcal{I}$ is defined for $[\alpha\epsilon A{:}s]$, $s(t)$, $\langle s,t \rangle$, and $\pi_i s$ via the (partial) cartesian closedness of $\underline{S}$. Finally, $\mathcal{I}$ is defined on terms via the canonical morphisms given by the various adjunctions. One can then prove by standard means:

<u>Proposition 1 (Soundness)</u> <u>For any interpretation $\mathcal{I}:\underline{T} \to (\underline{G}, \underline{S})$, the equality rules are all valid under $\mathcal{I}$.</u>

In fact, this process may be modified to define a PL category $(\underline{G}(\underline{T}), \underline{S}(\underline{T}))$, and an interpretation $\mathcal{I}_{\underline{T}}:\underline{T} \to (\underline{G}(\underline{T}), \underline{S}(\underline{T}))$ with the universal property: given any interpretation $\mathcal{I}:\underline{T} \to (\underline{G}, \underline{S})$, there is a unique PLC functor $F:(\underline{G}(\underline{T}), \underline{S}(\underline{T})) \to (\underline{G}, \underline{S})$ so that $F\,\mathcal{I}_{\underline{T}} = \mathcal{I}$.

3. <u>Equivalences</u> Given a PL category $(\underline{G}, \underline{S})$, we can define a PL theory $\underline{T}(\underline{G}, \underline{S})$ whose orders are the objects of $\underline{S}$, whose operators are the morphisms of $\underline{S}$, and whose terms are the morphisms of $\underline{G}(A)$ for suitable A. $\underline{T}(\underline{G}, \underline{S})$ has the property that interpretations $\underline{T}(\underline{G}, \underline{S}) \to (\underline{G}', \underline{S}')$ are in bijective correspondance with PLC functors $(\underline{G}, \underline{S}) \to (\underline{G}', \underline{S}')$. Finally, we can show:

<u>Theorem 2</u> <u>The categories of PL theories and of PL categories are equivalent.</u>

The equivalences are given by the functors $\underline{T}$ and $(\underline{G}(\ ), \underline{S}(\ ))$.

4. <u>The $P\omega$ model</u> We give an example of a PL category, based on the model of closure operators in $P\omega$, due to Scott and McCracken, [5], [3]; this should be compared to the presentation of [1]. For the basics of the description of $P\omega$ as a model of the lambda calculus, see [5].

<u>Definition 3</u> $K = \{a \epsilon P\omega : I \subseteq a = a \circ a\}$ is the subspace of $P\omega$ of closure operators; K is made a category $\underline{K}$: $f{:}a \to b$ is $f \in P\omega$

satisfying $f = b \circ f \circ a$.

Definition 4 For $a \in K$, $T(a) = \{x \in P\omega : a(x) = x\}$. Note that $Hom_{\underline{K}}(a,b) = Cont(T(a),T(b))$, the set of continuous maps $T(a) \to T(b)$.

Facts (1) $\underline{K}$ is cartesian closed.

(2) There is an object $V \in K$ so that $T(V) = K$.

Definition 5 For $d \in K$, $\underline{G}(d)$ is the following category: $Obj(\underline{G}(d)) = Hom_{\underline{K}}(d,V)$, and $f:a \to b$ is a morphism if $f:T(d) \to P\omega$ is a continuous map satisfying $f(t):a(t) \to b(t)$ for all $t \in T(d)$. Given $g:d \to e$ in $\underline{K}$, $g^* = \underline{G}(g)$ is defined by composition, making $\underline{G}$ an indexed category over $\underline{K}$. (Think of $\underline{G}(d)$ as $[T(d), \underline{K}]$, the category of continuous maps $T(d) \to \underline{K}$.)

Proposition 3 (1) For each $d \in K$, $\underline{G}(d)$ is cartesian closed, with the structure given pointwise by the structure on $\underline{K}$.

(2) $\underline{G}$ is complete, and so is a PL category.

Proof (2) The definition of $\Pi:\underline{G}^c \to \underline{G}$, for $c \in K$, is induced by composition with the map (almost the S combinator) $\Pi:[T(c),K] \to K$ (equivalently $\Pi:c \supset V \to V$), $\Pi = \lambda x \lambda y \lambda z \epsilon c.x(z)(y(z))$. (We write $\lambda x \epsilon a.s[x]$ to mean $\lambda x.s[a(x)]$. This has the effect of restricting x to $T(a)$.) This works for the following reason: we are, in essence, interpreting types as closure operators and terms as fixed points. Given $f:T(c) \to K$, $\Pi(f)$ ought to be the "product" of all $f(t)$, $t \in T(c)$, so that if $b = \Pi(f)(b)$ is a "term of type" $\Pi(f)$, then for $t \in T(c)$, $b(t) = f(t)(b(t))$ must be a "term of type" $f(t)$; i.e. $\Pi(f)(b)(t) = f(t)(b(t))$.

Remark $(\underline{G}, \underline{K})$ is a "rich" model, in that it has a lot of orders. We could have done with less: instead of $\underline{K}$ as the base category, use the full subcategory containing 1 and V, and closed under $\times$ and $(\ ) \supset V$.

A Personal note I wish to thank F. Lamarche for his helpful comments and insights. This work was done with the support of a grant from the Ministry of Education, Quebec.

References

[1] Bruce, K.B. and A.R. Meyer, The semantics of second order polymorphic lambda calculus, in: Semantics of Data Types, Lecture Notes in Computer Science 173 (Springer-Verlag, 1984) 131 - 144.

[2] Girard, J-Y, "Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur", Ph.D. Thesis, Université Paris VII (1972).

[3] McCracken, N.J., "An investigation of a programming language with a polymorphic type structure", Ph.D. Thesis, Syracuse University (1979).

[4] Reynolds, J.C., Towards a theory of type structure, in: Proc. Colloque sur la Programmation, Lecture Notes in Computer Science 19 (Springer-Verlag, 1974) 408 - 425.

[5] Scott, D.S., Data types as lattices, SIAM J. Comput. 5 (1976) 522 - 587.

Department of Mathematics
John Abbott College
C.P. 2000
Ste. Anne de Bellevue
Quebec H9X 3L9

Received 2 January, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

NOTE ON O.BOTTEMA'S INEQUALITY FOR TWO TRIANGLES

D.S.Mitrinović and J.E.Pečarić

Presented by H.S.M. Coxeter, F.R.S.C.

Abstract. In this note we showed that the known Bottema inequality for two triangles and an interior point of one of triangles is also valid for any point.

The following result is well known ([2],[4, 12.18]):

THEOREM A. Let x,y,z be the distances from any point P from the plane of a triangle ABC of area F to the respective vertices. Then

(1) $$\Sigma x \geqq 2\sqrt{F\sqrt{3}}.$$

Equality occurs if and only if the triangle is equilateral and P is its centre.

Inequality (1) is stronger than ([8],[4, 12.14]): $\Sigma x \geqq 6r$, where r is the radius of incircle, because ([4, 5.11]) $6r \leqq 2\sqrt{F\sqrt{3}}$.

The following result is also known ([6],[4, 12.55]):

THEOREM B. If all angles are less than 120°, then

$$\Sigma x \geqq (\tfrac{1}{2}\Sigma a^2 + 2F\sqrt{3})^{\frac{1}{2}}.$$

If $A \geqq 120^\circ$, then

$$\Sigma x \geqq b + c.$$

Here x,y,z are the distances from an interior point P of triangle to the respective vertices.

Equality holds if P coincides with Torricelli's point.

Remark. Let $A_1A_2B_3$, $A_2A_3B_1$, $A_3A_1B_2$ be the equilateral triangles constructed on the edges of an arbitrary triangle $A_1A_2A_3$ in the exterior of the triangle. The segments A_1B_1, A_2B_2, A_3B_3 are concurrent at a point T, the Torricelli point of the triangle (see for example [7]).

O.Bottema [3] proved the following inequality for two triangles (see also [4, 12.56]):

THEOREM C.

(2) $$\Sigma a_1 x \geq \left(\tfrac{1}{2}M + 8FF_1\right)^{\frac{1}{2}}$$

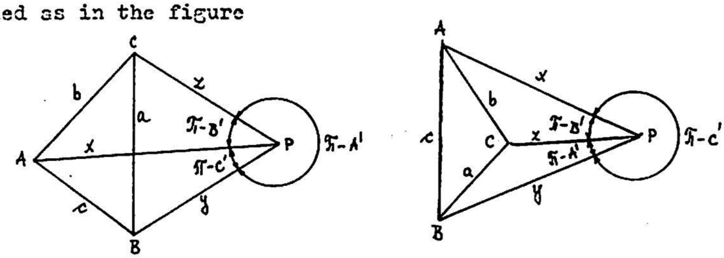
where $M = \Sigma a_1^2(b^2+c^2-a^2)$; a_1, b_1, c_1, and a, b, c are sides of two arbitrary triangles of area F_1 and F, respectively, and x, y, z are the distances from an interior point P of triangle ABC to the respective vertices.

In his book, dealing with the Torricelli point (being the case $a_1 = b_1 = c_1$) Bottema generalized a known proof for the case that a_1, b_1, c_1 are the sides of an arbitrary triangle. The proof was complicated and has been much simplified by Bottema and Klamkin in [5]. A new proof of Theorem C is given in [1], too.

In this note we shall show that (2) is also valid in the case when x,y,z are the distances from an arbitrary point in space to the respective vertices.

Of course, it is sufficient: consider the case when the point P belongs to the plane of the triangle ABC.

We shall use the idea of the proof from [5]. Let A′, B′, C′ be defined as in the figure



Situation 1. Situation 2.

Fig.1.

Note that $A' + B' + C' = \pi$, and

$$a^2 = y^2 + z^2 + 2yz\cos A\ , \text{ etc.}$$

Thus

$$b^2+c^2-a^2 = 2x^2 + 2x(z\cos B' + y\cos C') - 2yz\cos A\ , \text{ etc.}$$

and depending upon whether situation 1 or 2 holds, we have

$$8F_1F = \pm 4F_1 \Sigma yz\sin A' .$$

On substituting back in (2), we obtain

$$(\Sigma a_1x)^2 \geqq \Sigma a_1{}^2\{x^2+x(z\cos B'+y\cos C') - yz\cos A'\} \pm 4F_1 \Sigma yz\sin A' ,$$

or

$$\Sigma yz\{2b_1c_1 + (a_1{}^2-b_1{}^2-c_1{}^2)\cos A' \mp 4F_1\sin A'\} \geqq 0,$$

or finally,

$$4\Sigma\, yzb_1c_1\sin^2(A_1 \mp A')/2 \geqq 0.$$

This is obviously true because the terms on the left hand side are all non-negative. This implies that (2) holds not only for interior points but for exterior points P as well.

There is equality only if each term of the sum vanishes, i.e.,

Case 1. $xyz \neq 0,\ A_1 = A',\ B_1 = B',\ C_1 = C'$,

Case 2. $xyz = 0$ (say $x = 0$), $A_1 = A'$.

It is obvious that equality doesn't exist in the case when P is an exterior point of a triangle ABC.

By coupling the above result and the Neuberg-Pedoe inequality ([4, 10.8]) we get similar extension of a result from [5]:

(3) $$\Sigma a_1x \geqq (M/2 + 8FF_1)^{\frac{1}{2}} \geqq 4\sqrt{FF_1},$$

wherefrom in the case $a_1 = b_1 = c_1$, we get

(4) $$\Sigma x \geqq (\tfrac{1}{2}\Sigma a^2 + 2F\sqrt{3})^{\frac{1}{2}} \geqq 2\sqrt{F\sqrt{3}}.$$

D.S. Mitrinović, J.E. Pečarić

⁎

⁎ ⁎

ACKNOWLEDGEMENT. The authors are grateful to Professor O.Bottema for useful suggestions.

REFERENCES:

1. G.BENNETT, Multiple Triangle Inequalities. Univ.Beograd.Publ.Elektrotehn.Fak.Ser.Mat.Fiz. No 577-598 (1977), 39-44.
2. U.T.BÖDEWADT, Jber. Deutsch.Math.-Verein. 46 (1936), 7 kursiv.
3. O.BOTTEMA, Hoofdstukken uit de elementaire meetkunde, Den Haag 1944, pp. 97-99.
4. O.BOTTEMA, R.Ž.DJORDJEVIĆ, R.R.JANIĆ, D.S.MITRINOVIĆ, P.M.VASIĆ, Geometric Inequalities, Groningen, 1969.
5. O.BOTTEMA and M.S.KLAMKIN, Joint Triangle Inequalities. Simon Stevin 48 (1974/75), I-II (1974), 3-8.
6. T.LALESCO, La géométrie du triangle, Paris 1937, p. 41.
7. J.NAAS, H.L.SCHMID, Mathematisches Wörterbuch, band II, Berlin-Stuttgart, 1961, p. 732.
8. M.SCHREIBER, Aufgabe 196. Jber.Deutsch.Math.-Verein. 45 (1935), 63 kursiv.

Faculty of Electrical Engineering
Faculty of Civil Engineering
University of Belgrade
Yugoslavia

Received 15 January, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

ON THE GENERAL INVERSE PROBLEM OF GALOIS THEORY

C.U. Jensen

Presented by G.A. Elliott, F.R.S.C.

Summary.

For a finite group G and a field K let $\nu(G,K)$ be the number of non-K-isomorphic separable normal extensions of K with G as a Galois group. Some results are announced concerning the distribution of the values of $\nu(G,K)$. For instance, there exists a field over which every finite simple group but not every finite group can be realized as a Galois group.

Let K be a field with algebraic closure $\overline{K}$. For a finite group G let $\nu(G,K)$ be the number (cardinality) of the distinct separable normal extensions of K (inside $\overline{K}$) with Galois group isomorphic to G.

If A is a family of (isomorphism classes of) finite groups we say that K is A-admissible if $\nu(G,K) > 0$ for every $G \in A$. We call a field K universally admissible if $\nu(G,K) > 0$ for every finite group G.

For a fixed finite group G the fields K for which $\nu(G,K) > 0$ can be defined by a first order sentence σ_G in the language of fields. Hence, for any family A the A-admissible fields form an axiomatizable class of fields; if A is finite this class is finitely axiomatizable. If A is the family of all finite groups or an infinite family of finite simple groups the

Part of this work was done while the author was visiting the University of Toronto during the fall of 1985.

A-admissible fields do not form a finitely axiomatizable class. If A is the family of all cyclic groups whose orders are the powers of a fixed prime number, the A-admissible fields form a finitely axiomatizable class. It is not known to the author for which (infinite) families A, the A-admissible fields are finitely axiomatizable.

Let S be the family of all finite simple groups. The corresponding first order sentences σ_S, $S \in S$, are completely independent. Actually, something stronger holds.

Firstly, we notice that if S is a cyclic group of prime order p and K is a field for which $\nu(S,K) < \infty$, then $\nu(S,K) = (p^n-1)/(p-1)$ for a suitable positive integer n.

Basically, this is the only condition the cardinalities $\nu(S,K)$, $S \in S$, have to satisfy, as the following shows.

Theorem 1. *Let* $\mu(S)$, $S \in S$, *be any family of cardinal numbers subject to the condition that* $\mu(S)$ *has the form* $(p^n-1)/(p-1)$ *for some positive integer* n *when* $\mu(S) < \infty$ *and* S *is cyclic of order* p. *Then there exists a field* K *of arbitrarily prescribed characteristic such that* $\nu(S,K) = \mu(S)$ *for every* $S \in S$.

Theorem 2. *If* K *is universally admissible then* $\nu(G,K) \geq \aleph_0$ *for every finite group* G. *If* $\mu(S)$, $S \in S$, *is any family of infinite cardinalities, then there exists a universally admissible field* K *of arbitrarily prescribed characteristic such that* $\nu(S,K) = \mu(S)$ *for every* $S \in S$.

Corollary 1. There exists a field K of any prescribed characteristic such that $\nu(S,K) > 0$ for every $S \in \mathcal{S}$, but K is not universally admissible. If the prescribed characteristic is 0, then K may be taken as an infinite algebraic number field.

Example. Let K be the Pythagorean closure of the field $\mathbb{R}(t)$. In this case $\nu(S,K) > 0$ for any $S \in \mathcal{S}$, while $\nu(G,K) = 0$ for any cyclic group G whose order is divisible by 4.

The phenomenon from corollary 1 can be strengthened as the following shows.

Proposition 1. For any family $\mu(S)$, $S \in \mathcal{S}$, of infinite cardinal numbers there exists a field K (of prescribed characteristic) which is not universally admissible while $\nu(S,K) = \mu(S)$ for every $S \in \mathcal{S}$.

From theorem 1 we conclude

Corollary 2. For any division $\mathcal{S} = \mathcal{A} \cup \mathcal{B}$ into disjoint families there exist a field K (of prescribed characteristic) such that $\nu(S,K) > 0$ for any $S \in \mathcal{A}$ and $\nu(S,K) = 0$ for any $S \in \mathcal{B}$. If the prescribed characteristic is zero K may be taken to be an infinite algebraic number field.

By the length of a finite group G we mean the length of one (and hence of every) composition series of G.

The following can be considered as another strengthening of corollary 1.

Theorem 3. For any positive integer n *there exists a field* K *which is not universally admissible, while* $\mu(G,K) > 0$ *for any group* G *of length* $\leqq n$.

Let A be a family of centerless finite groups of length $\leqq 2$ satisfying the following condition: If N is a proper normal subgroup of a group $G \in A$, then G/N is cyclic of prime order. For instance, the symmetric groups S_n, $n > 4$, the dihedral groups D_p, p a prime, and the Frobenius groups $F_{p\ell}$, $\ell \mid p-1$, p a prime, satisfy the above conditions.

Theorem 4. Let A *be a family of groups satisfying the above conditions and* $\mu(A)$, $A \in A$, *a family of (finite or infinite) cardinal numbers. Then there exists a field* K *(of prescribed characteristic) for which* $\nu(A,K) = \mu(A)$ *for any* $A \in A$.

Example. The family of finite groups consisting of the alternating groups A_n and symmetric groups S_n, $n > 4$ has the division property: If $\bigcup_{n>4} \{A_n\} \cup \{S_n\} = B \cup C$, $B \cap C = \emptyset$, then there exists a field (of any prescribed characteristic) such that $\nu(G,K) > 0$ for any $G \in B$ and $\nu(G,K) = 0$ for any $G \in C$.

The following results are quite straightforward and are stated for completeness.

Proposition 2. Let A *be a family of finite groups which are closed under formation of finite direct products. Then any finite extension of an* A*-admissible field is* A*-admissible. In particular, any finite extension of a universally admissible field is universally admissible.*

Proposition 3. *Any (finite or infinite) abelian extension of a universally admissible field is universally admissible.*

Proposition 4. *For any finite group* G $(\neq 1)$ *there exists a normal separable extension* L/K *whose Galois group is isomorphic to* G *such that* L *but not* K *is universally admissible.*

Matematisk Institut
Universitetsparken 5
2100 Copenhagen Ø
Denmark.

Received 16 January, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

STRONG APPROXIMATIONS FOR RENEWAL PROCESSES

Miklós Csörgő, Lajos Horváth and Josef Steinebach

Presented by D.R. Brillinger, F.R.S.C.

Abstract: Best approximations are presented for renewal processes.

Let X, $\{X_i;\ i \geq 1\}$ be independent identically distributed random variables (i.i.d.r.v.'s) with mean and variance

(1) $$EX = \mu > 0 \quad \text{and} \quad 0 < E(X-\mu)^2 = \sigma^2 < \infty .$$

We define $Z(t) = \Sigma_{i=1}^{t} X_i$ and its inverse, the renewal process or random walk point process by

(2) $$N(t) = \inf\{x : Z(x) > t\}, \quad 0 \leq t < \infty .$$

We are assuming without loss of generality that the underlying probability space (Ω, A, P) is so rich that it accommodates all r.v.'s and processes introduced so far as well as later on. We have the following results.

THEOREM. Assume (1). We can define a Wiener process $\{W(t),\ t \geq 0\}$ such that

(i) if $E\exp(tX) < \infty$ in a neighbourhood of zero, then

(3) $$P\{\sup_{0 \leq t \leq T} |(N(t)-t/\mu)/(\sigma\mu^{-3/2}) - W(t)| > A_1 \log T + x\} \leq B_1 \exp(-C_1 x)$$

for all $x > 0$, and as $T \to \infty$

(4) $$\sup_{0 \leq t \leq T} |(N(t)-t/\mu)/(\sigma\mu^{-3/2}) - W(t)| \overset{a.s.}{=} O(\log T),$$

where A_1, B_1 *and* C_1 *are positive constants*

(ii) *if* $E|X|^r < \infty$ *for some* $r > 2$, *then*

(5) $$P\{\sup_{0\le t\le T} |(N(t)-t/\mu)/(\sigma\mu^{-3/2})-W(t)|>x\} \le B_2(T)Tx^{-r}$$

for all $A_2T^{1/r} \le x \le C_2(T \log T)^{1/2}$, *and as* $T \to \infty$

(6) $$\sup_{0\le t\le T} |(N(t)-t/\mu)(\sigma\mu^{-3/2})-W(t)| \stackrel{a.s.}{=} o(T^{1/r}),$$

where A_2, C_2 are positive constants and $B_2(T) \to 0 \quad (T \to \infty)$.

This problem was posed in a more general setting in Csörgő, Horváth and Steinebach (1985), where further details and proofs can also be found. Here we give a new proof for statement (4).

PROOF OF (4). We can assume without loss of generality that $\mu = \sigma = 1$. By the Komlós, Major and Tusnády approximation (cf. Theorem 2.6.2 in Csörgő and Révész (1981)) there is a Wiener process $\{W_1(t),\ t \ge 0\}$ such that

(7) $$\sup_{0\le t\le T} |(Z(t)-t)-W_1(t)| \stackrel{a.s.}{=} O(\log T)$$

Let

(8) $$M_1(t) = \inf\{x : W_1(x) = t-x\}.$$

Using (2), (7) and Theorem 1.2.1 of Csörgő and Révész (1981) we obtain

(9) $$\sup_{0\le t\le T} |N(t)-M_1(t)| \stackrel{a.s.}{=} O(\log T)$$

(cf. Lemma 5 of Steinebach (1986)).

Let $\{Y_i; i \geq 1\}$ be i.i.d. exponential r.v.'s with mean one. We define $S(t) = \Sigma_{i=1}^{t} Y_i$ and let $\nu(t)$ be its renewal process. Using again the Komlós, Major and Tusnády approximation, there exists a Wiener process $\{W_2(t), t \geq 0\}$ such that

(10) $$\sup_{0\leq t\leq T} |(S(t)-t)-W_2(t)| \overset{a.s.}{=} O(\log T).$$

Next we define $M_2(t) = \inf\{x : W_2(x) = t-x\}$ and, similarly to (9), we obtain

(11) $$\sup_{0\leq t\leq T} |\nu(t)-M_2(t)| \overset{a.s.}{=} O(\log T).$$

On account of $\nu(t)$ being a Poisson process with stationary independent increments, we can again apply the Komlós, Major and Tusnády approximation and conclude that one can define a Wiener process $\{W_3(t), t \geq 0\}$ such that

(12) $$\sup_{0\leq t\leq T} |(\nu(t)-t)-W_3(t)| \overset{a.s.}{=} O(\log T).$$

Consequently by (11) and (12) we get

(13) $$\sup_{0\leq t\leq T} |(M_2(t)-t)-W_3(t)| \overset{a.s.}{=} O(\log T).$$

Since

(14) $$\{M_1(t), t \geq 0\} \overset{\mathcal{D}}{=} \{M_2(t), t \geq 0\},$$

i.e., the two processes in question are equal in distribution, it follows by Lemma 4.4.4 of Csörgő and Révész (1981) and (13) that we can construct a Wiener process $\{W(t), t \geq 0\}$ such that

$$\sup_{0\le t\le T} |(M_1(t)-t)-W(t)| \overset{a.s.}{=} O(\log T). \tag{15}$$

This also completes the proof of (4).

The optimality of the rates of Theorem is proved in [1].

ACKNOWLEDGEMENT. This research was supported in part by a Natural Sciences and Engineering Research Council Canada Grant of Miklós Csörgő at Carleton University.

REFERENCES

[1] CSÖRGŐ, M., HORVÁTH, L. and STEINEBACH, J. (1985). Invariance principles for renewal processes. In: Technical Report Series of the Laboratory for Research in Statistics and Probability, No. 59 - Aug. 1985, Carleton University - University of Ottawa.

[2] CSÖRGŐ, M. and RÉVÉSZ, P. (1981). Strong Approximations in Probability and Statistics. Academic, New York.

[3] STEINEBACH, J. (1986). Improved Erdős-Rényi and strong approximation laws for increments of renewal processes. Ann. Probab. To appear.

MIKLÓS CSÖRGŐ
DEPARTMENT OF MATHEMATICS
AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, CANADA
K1S 5B6

LAJOS HORVÁTH
BOLYAI INSTITUTE
SZEGED UNIVERSITY
ARADI VÉRTANÚK TERE 1
H-6720 SZEGED
HUNGARY

Received 20 January, 1986

JOSEF STEINEBACH
FACHBEREICH MATHEMATIK
UNIVERSITÄT MARBURG
HANS-MEERWEIN-STRASSE
D-3550 MARBURG, WEST GERMANY

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

ON SOME SPECTRAL INGREDIENTS FOR THE INTEGRAL EQUATIONS OF SCATTERING THEORY

Robert Carroll

Presented by M. Shinbrot, F.R.S.C.

Abstract. It is shown how the fundamental quantities in the various integral equations of inverse scattering theory can be represented in spectral form based on transmutation kernels for underlying differential operators.

1. Introduction. The various integral equations (Gelfand-Levitan = G-L, Marčenko = M, Krein = K, Gopinath-Sondhi = G-S, etc.) which arise in studying inverse problems in quantum mechanics, geophysics, transmission lines, linear stochastic estimation and filtering, etc. can be derived in, and regarded in, various ways. They take on significance in various roles, mathematical and physical, and one way of unifying this via transmutation ideas goes back to Fadeev [17]. This was expanded and refined by the author in [4-6;8;9;14] where transmutation and related spectral ideas lead to various points of view and derivations of the fundamental G-L and M equations (this is reorganized in [11] in a composite manner). On the other hand the unifying method of Bruckstein-Kailath-Levy (see [1; 2]) gives a simultaneous derivation of various G-L, M, K, and G-S equations from transmission line models where a disturbance is propagated into a medium and we can recast this in terms of sideways Cauchy problems plus transmutation machinery to give spectral representations of the fundamental quantities. Our methods also yield spectral versions for the Green's functions and integral equations of [3] and for the half line system equations of [18] (the latter arising from the con-

text of [19]). One notes that the M equation of [19] is mainly significant in the case of full line scattering where a certain Riemann-Hilbert problem connects the Jost and scattering matrices; for the half line problem the Jost matrix can be explicitly represented in terms of scattering data and the theory is not as deep or complicated. Thus we show here how some techniques of handling systems (*) $D_x\binom{v}{\mathcal{I}} = -D_t\begin{pmatrix}0 & Z\\ 1/Z & 0\end{pmatrix}\binom{v}{\mathcal{I}}$ ($v \sim$ voltage, $\mathcal{I} \sim$ current, $Z \sim$ impedance with $Z(0) = 1$) developed in [6-8;10], using information about canonical systems based on [15;16], lead to representation formulas for the various fundamental objects. In a sense our basic sideways Cauchy problem provides a background framework of sideways evolution for the layer stripping procedure of [1;2].

2. Basic information. In (*) take $V = vZ^{-\frac{1}{2}}$, $I = \mathcal{I}Z^{\frac{1}{2}}$, $r = (1/2)D_x\log Z$ = reflectivity, $p = r^2-r'$, $q = r^2+r'$, $J = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $W = \begin{pmatrix}0 & r\\ r & 0\end{pmatrix}$, $\hat{J} = \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$, $W_R = (V+I)/2$, and $W_L = (V-I)/2$. Set $Q = JD_x - W$, $Pu = (Zu')'/Z$, $Qu = (Z^{-1}u')'Z$, $\dot{P} = D^2-\dot{p}$ ($\dot{p} = q = r^2+r'$), and $\dot{Q} = D^2-\dot{q}$ ($\dot{q} = p = r^2-r'$); we retain the notation $\dot{p} = q$ and $\dot{q} = p$ since it appeared in [10]. Then $(D_x^2-p)V = D_t^2V$, $(D_x^2-q)I = D_t^2I$, and

$$(2.1) \qquad Q\binom{V}{I} = \hat{J}D_t\binom{V}{I};\ D_x\binom{W_R}{W_L} - \hat{J}D_t\binom{W_R}{W_L} = -W\binom{W_R}{W_L}$$

One speaks of canonical equations (▲) $QU = \lambda U$, $U = \begin{pmatrix}A & C\\ B & D\end{pmatrix}$, $U(0,\lambda) = I$. Note that this is different from a Fourier transform in (2.1) since if $D_t \to -ik$ say then (2.1) becomes (■) $Q\binom{\hat{V}}{\hat{I}} = -ik\hat{J}\binom{\hat{V}}{\hat{I}}$ and one cannot identify λ with $\pm ik$. However if we look at second order equations arising from say (♦) $B_x-rB = \lambda A$, $-A_x-rA = \lambda B$, $D_x-rD = \lambda C$, $-C_x-rC = \lambda D$ and (•) $\hat{I}_x-r\hat{I} = ik\hat{V}$ and $-\hat{V}_x-r\hat{V} = -ik\hat{I}$ they are the same. Thus (••) $\dot{P}B = -\lambda^2B$, $\dot{P}D = -\lambda^2D$, $\dot{Q}A = -\lambda^2A$, and $\dot{Q}C = -\lambda^2C$, while $\dot{Q}\hat{V} = -k^2\hat{V}$, and $\dot{P}\hat{I} = -k^2\hat{I}$. Similarly (▲▲) $a_x = -\lambda Zb$, $b_x = \lambda Z^{-1}a$, $\tilde{a}_x = -\lambda Z\tilde{b}$, and $\tilde{b}_x = \lambda Z^{-1}\tilde{a}$ where $a = AZ^{\frac{1}{2}}$, $b = BZ^{-\frac{1}{2}}$, $\tilde{a} = CZ^{\frac{1}{2}}$, and $\tilde{b} = DZ^{-\frac{1}{2}}$. Further from $a(0) = \tilde{b}(0) = 1$, $a'(0) = \tilde{b}'(0) = 0$, $b(0) = \tilde{a}(0) = 0$, and $b'(0) = -\tilde{a}'(0) = \lambda$ we have (■■) $a = \varphi_\lambda^Q = c_Q\Phi_\lambda^Q + c_{\bar{Q}}\Phi_{-\lambda}^Q$, $b = \lambda\theta_\lambda^P = [F_{\bar{P}}\Phi_\lambda^P - F_P\Phi_{-\lambda}^P]/2i$, $\tilde{a} = -\lambda\theta_\lambda^Q = [F_Q\Phi_{-\lambda}^Q - F_{\bar{Q}}\Phi_\lambda^Q]/2i$, and $\tilde{b} = \varphi_\lambda^P =$

$c_P\Phi_\lambda^P + c_P^-\Phi_{-\lambda}^P$ in the notation of [5;6;8]. Moreover ($\Phi_{\pm\lambda}^P(x) \sim Z_\infty^{-1/2}e^{\pm i\lambda x}$ and $\Phi_{\pm\lambda}^Q(x) \sim Z_\infty^{1/2}\exp(\pm i\lambda x)$ as $x \to \infty$ where $Z \to Z_\infty$ rapidly is assumed) one shows as in [10] that $d\nu_P = 2d\lambda/\pi|F_P|^2 = d\omega_Q = d\lambda/2\pi|c_Q|^2$ and $d\nu_Q = 2d\lambda/\pi|F_Q|^2 = d\omega_P = d\lambda/2\pi|c_P|^2$ (in fact $2c_Q = F_P^-$ and $2c_P = F_Q^-$ for λ real with $2c_Q^- = F_P$ and $2c_P^- = F_Q$). Standard properties of the $c_{Q,P}$, $\varphi_\lambda^{P,Q}$, etc. can be found in [5;6;8]. We recall also from [5;6;8] that one distinguishes between one and two sided delta functions, or better, half and full line delta functions, defined via Fourier representations $\delta_+ = (2/\pi)\int_0^\infty \text{Cos}\lambda x d\lambda = 2[(1/2\pi)\int_{-\infty}^\infty \exp(i\lambda x)d\lambda] = 2\delta$. Next, one can write for $d\mu = (2/\pi)d\lambda$ (♠♠) $\langle A(x,\lambda),\text{Cos}\lambda t\rangle_\mu = [\delta_+(x-t) + \delta_+(x+t)]/2 + k_Q(x,t)$, $\langle B(x,\lambda),\text{Sin}\lambda t\rangle_\mu = [\delta_+(x-t) - \delta_+(x+t)]/2 + \check{k}_P(x,t)$, $\langle D(x,\lambda),\text{Cos}\lambda t\rangle_\mu = [\delta_+(x-t) + \delta_+(x+t)]/2 + k_P(x,t)$, and $-\langle C(x,\lambda),\text{Sin}\lambda t\rangle_\mu = [\delta_+(x-t) - \delta_+(x+t)]/2 + \check{k}_Q(x,t)$ (see [5;8;10] for details).

3. Cauchy problems. We note first some formulas from [1] for the right and left propagating waves W_R and W_L. Thus one writes (▲★) $\binom{W_R}{W_L}(x,t) = M(x,t) * \binom{W_R}{W_L}(0,t)$ with $M = (M_{ij})$ and $M(0,t) = \delta(t)I$. Further $M_{11}(x,t) = M_{22}(x,-t)$, $M_{21}(x,t) = M_{12}(x,-t)$, and supp $M_{ij}(x,\cdot) \subset [-x,x]$ while (▲■) $M_{11}(x,t) = \delta(x-t) + m_{11}(x,t)[Y(t+x) - Y(t-x)]$ and $M_{21}(x,t) = m_{21}(x,t)[Y(t+x) - Y(t-x)]$ where Y is the Heavyside function. One obtains for $-x \le t \le x$ (▲♠) $\int_{-x}^t W_R(0,t-\tau)m_{11}(x,\tau)d\tau + \int_{-t}^x W_L(0,t+\tau)m_{21}(x,\tau)d\tau = 0$ and $W_L(0,t+x) + \int_{-t}^x W_L(0,t+\tau)m_{11}(x,\tau)d\tau + \int_{-x}^t W_R(0,t-\tau)m_{21}(x,\tau)d\tau = 0$. One assumes now (★▲) $W_R(x,t) = \delta(t-x) + w_R(x,t)Y(t-x)$ with $W_L(x,t) = w_L(x,t)Y(t-x)$ and the G-L, M, K, and G-S equations can be obtained by specializing the input via (▲●) (A) $w_R(0,t) = 0$ with $w_L(0,t) = R(t)Y(t)$ or (B) $w_R(0,t) = w_L(0,t) = h(t)$ (see here [1;2] for philosophy). Define now (★●) $K(x,t) = m_{11}(x,t) + m_{21}(x,t)$, $L(x,t) = m_{11}(x,t) + m_{12}(x,t)$, $K_S(x,t) = [K(x,t) + K(x,-t)]/2$. Then for appropriate choices of data in (▲●) one obtains e.g. a G-L type equation (★■) $K_S(x,t) + [h(x+t) + h(x-t)]/2 + \int_0^x [h(|t-\tau|) + h(t+\tau)]K_S(x,\tau)d\tau = 0$ $(0 < t < x)$ with $p(x) = 4D_xK_S(x,x)$ or an M type equation (★♠) $(-x < t < x)$ $0 = R(t+x) + K(x,t) + \int_{-t}^x R(t+\tau)K(x,\tau)d\tau$ with $p(x) = 2D_xK(x,x)$. Other equations are also indicated in

[1;10] which we omit here. Note that it has become the practice to refer to integral equations such as (★♣) with kernels $R(t+\tau)$ (Hankel operators) as M equations. Now consider the equation for $\mathfrak{v}$ (●★) $Q\mathfrak{v} = Z(Z^{-1}\mathfrak{v}_x)_x = \mathfrak{v}_{tt}$. If one considers an upward Cauchy problem with $\mathfrak{v}(0,x) = \delta(x)$, $\mathfrak{v}_t(0,x) = 0$ $(x,t \geq 0)$ then a solution (notation of [5;6;8]) $\mathfrak{v}(x,t) = \langle \varphi_\lambda^Q(x), \mathrm{Cos}\lambda t\rangle_\omega = \tilde{\beta}_Q(x,t)$ $(\omega \sim \omega_Q)$ with readout impulse response $\mathfrak{v}(0,t) = \delta(t) + g(t) = G(t) = \langle 1, \mathrm{Cos}\lambda t\rangle_\omega = \langle W(\lambda), \mathrm{Cos}\lambda t\rangle_\nu$ where $W(\lambda) = \hat{\omega}_Q/\hat{\nu}$ $(\nu \sim d\nu = \hat{\nu}d\lambda = 2d\lambda/\pi)$. One notes that $\mathfrak{v}(x,t) = 0$ for $x > t$ (causality) and $\tilde{\beta}_Q(x,t)$ corresponds to a causal Green's function. Now look at the same problem sideways. Let $\mathfrak{v}(0,t) = G(t)$ be given with say $\mathfrak{v}_x(0,t) = 0$. Following general principles from [6;8] one tries to find a sideways solution in the form (●▲) $\mathfrak{v}(x,t) = \langle \beta_Q(x,t), T_\tau^t G(\tau)\rangle$ where T_τ^t is a generalized translation based on D^2 given via (●■) $T_\tau^t\psi(\tau) = (2/\pi)\int_0^\infty (\mathcal{F}_C\psi)\mathrm{Cos}\lambda t\mathrm{Cos}\lambda\tau d\lambda = [\psi(t+\tau) + \psi(|t-\tau|)]/2$. Here $\beta_Q(x,t) = \langle \varphi_\lambda^Q(x), \mathrm{Cos}\lambda t\rangle_\nu$ acts as an anticausal Green's function ($\beta_Q(x,t) = 0$ for $t > x$) and (●▲) can be written as (●♣) $\mathfrak{v}(x,t) = \frac{1}{2}\beta_Q(x,\cdot) * G(\cdot) = \frac{1}{2}\int_{-x}^x \beta_Q(x,\tau)G(t-\tau)d\tau$. One can also express $\mathfrak{v}(x,t)$ via a formula (■●) $\langle \varphi_\lambda^Q(x)F(\lambda), \mathrm{Cos}\lambda t\rangle_\nu$ and then $\mathfrak{v}(0,t) = G(t) = \langle F(\lambda), \mathrm{Cos}\lambda t\rangle_\nu$. It follows that $F(\lambda) = \mathcal{F}_C G(\lambda) = W(\lambda)$ which is also a proper choice to produce the correct (causal) triangularity in (■●)!

Now extend these ideas for the sideways Cauchy problem to the system context and take the $\binom{V}{I}$ equations in (2.1) (which are equivalent to the $\binom{W_R}{W_L}$ system) with data $\binom{V}{I}(0,t) = \binom{\delta}{\delta} = \frac{1}{2}\binom{\delta_+}{\delta_+}$. A solution can be expressed in the form

$$(3.1)\qquad \binom{V}{I} = \begin{pmatrix} \langle A(x,\lambda)F(\lambda), \mathrm{Cos}\lambda t\rangle_\nu - \langle C(x,\lambda)G(\lambda), \mathrm{Sin}\lambda t\rangle_\nu \\ \langle B(x,\lambda)F(\lambda), \mathrm{Sin}\lambda t\rangle_\nu + \langle D(x,\lambda)G(\lambda), \mathrm{Cos}\lambda t\rangle_\nu \end{pmatrix}$$

Choosing $G = F = 1/2$ to satisfy the condition at $x = 0$ one obtains (upon comparing solutions with (▲★)) (■▲) $4M_{11} = \langle A,\mathrm{Cos}\rangle - \langle C,\mathrm{Sin}\rangle + \langle B,\mathrm{Sin}\rangle + \langle D,\mathrm{Cos}\rangle$ and $4M_{21} = \langle A,\mathrm{Cos}\rangle - \langle C,\mathrm{Sin}\rangle - \langle B,\mathrm{Sin}\rangle - \langle D,\mathrm{Cos}\rangle$. Then recall (♣♣) and (▲■) to obtain

<u>Theorem 3.1</u>. <u>The elements of M are determined via</u> $4m_{11}(x,t) = k_Q + k_P + \check{k}_Q$

$+ \check{k}_P$ and $4m_{21} = k_Q - k_P - \check{k}_P + \check{k}_Q$. Consequently $2K(x,t) = k_Q + \check{k}_Q$, $2L(x,t) = k_Q + \check{k}_P$, and $K_S = (1/2)k_Q$.

In addition one has formulas $D_x k_Q(x,x) = p/2$, $D_x \check{k}_P(x,x) = q/2$, $D_x \check{k}_Q(x,x) = p/2$, and $D_x k_P(x,x) = q/2$ which are consistent with (*■) and (*♣). We note also that the canonical G-L equation from [8;13], namely, $0 = \langle \beta_Q(y,t), \mathcal{A}(t,x)\rangle$ for $x < y$ with $\mathcal{A}(t,x) = \int_0^\infty \hat{\omega}\mathrm{Cos}\lambda x \mathrm{Cos}\lambda t d\lambda$ ($d\omega_Q = \hat{\omega}d\lambda$) is exactly (*■).

4. Further comparisons and use of spectral techniques. One can also give spectral versions of the formulas in [3] derived from time domain principles. In fact our spectral technique led to time domain G-L equations in [5;6;8;12;13; 20]. Thus briefly here (cf. [10] for more detail) the Green's functions G_1 and G in [3] can be identified with our standard transmutation kernels as follows. $G_1(x,t) \sim \tilde{\beta}^Q(x,t) = \langle A(x,\lambda), \mathrm{Cos}\lambda t\rangle_\omega$ is a causal kernel while $G(x,t) \sim \beta^Q(x,t) = \langle A(x,\lambda), \mathrm{Cos}\lambda t\rangle_\nu$. One obtains the same G-L equation (*■) and an M type equation (■♣) for $t < x$, $0 = k_Q(x,t) + g(x+t) + \int_{-t}^x k_Q(x,\tau)g(t+\tau)d\tau$ where $g(t)$ is an impulse response readout as before. This equation involves different quantities from (*♣) and arises from a different problem. We note in passing that (*♣) arises from a $\binom{V}{I}$ problem with data $\binom{V}{I}(0,t) = \binom{\delta+RY}{\delta-RY}$ with solution of the form (3.1) with $F = (1/2) + \hat{R}$ and $G = (1/2) - \hat{R}$ ($\hat{R} = \mathcal{F}_C R$).

Next let us show briefly how the M type equation derived in [18;19] for half line systems can be put into spectral form and identified with a variation of (*♣) (see [11] for more details). Thus consider (2.1) under Fourier transform in the form (■) ($r(x) = 0$ for $x < 0$). One constructs $\vec{f}_r$ and $\vec{f}_\ell$ ($f^1 \sim (V+I)/2$, $f^2 \sim (V-I)/2$) with (♣■) for $\mathbb{I} = -\hat{J} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, $\lim_{x\to-\infty} \exp(-ik\mathbb{I}x)\vec{f}_\ell(k,x) = \hat{f}_\ell(k,0) = \binom{1}{\mathring{R}_\ell}(1/\mathring{T})$, $\lim_{x\to\infty} \exp(-ik\mathbb{I}x)\vec{f}_r = \binom{\mathring{R}_r}{1}(1/\mathring{T})$, $\exp(-ik\mathbb{I}x)\vec{f}_r \to \binom{0}{1}$ as $x \to -\infty$, and as $x \to \infty$ $\exp(-ik\mathbb{I}x)\vec{f}_\ell \to \binom{1}{0}$. Then one can express the components $f_r^{1,2}$ and $f_\ell^{1,2}$ in terms of $\varphi_\lambda^{P,Q}$, $\theta_\lambda^{P,Q}$, and $\Phi_{\pm\lambda}^{P,Q}$ ($\lambda \sim k$ here for the second order equations) and in particular $\hat{V}_r = f_r^1 + f_r^2 = Z^{-1/2}[\varphi_\lambda^Q - i\lambda\theta_\lambda^Q]$ with $\hat{I}_r = f_r^1 - f_r^2 = Z^{1/2}[-\varphi_\lambda^P + i\lambda\theta_\lambda^P]$. Using

(■■) one finds also (♠▲) $\mathring{R}_r = (c_Q - \frac{1}{2}F_Q^-)/(c_Q^- + \frac{1}{2}F_Q)$, $(1/\mathring{T}) = c_Q^- + \frac{1}{2}F_Q = \frac{1}{2}F_P + c_P^-$, and $\mathring{R}_\ell = (\frac{1}{2}F_Q - c_Q^-)/(\frac{1}{2}F_Q + c_Q^-)$. An M type equation arises now from (♠■) $\vec{f}_r(-k,x) = \mathring{T}\Lambda\vec{f}_\ell(k,x) - \mathring{R}_\ell\Lambda\vec{f}_r(k,x)$ where $\Lambda = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in the form (★★) $\vec{A}(y,x) = \Sigma(x+y)\binom{0}{1} - \int_{-y}^{x} \Lambda\vec{A}(\xi,x)\Sigma(\xi+y)d\xi$ for $-x < y < x$ where $\Sigma(x) = (1/2\pi)\int_{-\infty}^{\infty} \mathring{R}_\ell(k)\exp(-ikx)dk$ ($\Sigma(x) = 0$ for $x < 0$) and (♠★) $\vec{f}_r(k,x) = \exp(-ikx)\binom{0}{1} - \int_{-x}^{x} \exp(-iky)\vec{A}(y,x)dy$ with $2A_1(y,y) = r(y)$. Thus

Theorem 4.1. Everything can be given a spectral version as before (cf. Theorem 3.1) and in particular one has $A_1(y,x) = -m_{21}(x,y)$ with $A_2(y,x) = -m_{11}(x,y)$.

REFERENCES

1. A. Bruckstein, T. Kailath, and B. Levy, SIAM J. Appl. Math., 45 (1985), 312-335
2. A. Bruckstein and T. Kailath, Inverse scattering for discrete transmission line models, SIAM Review, to appear
3. R. Burridge, Wave Motion, 2 (1980), 305-323
4. R. Carroll, Applicable Anal., 18 (1984), 39-54
5. R. Carroll, Transmutation, scattering theory, and special functions, North-Holland, Amsterdam, 1982
6. R. Carroll, Acta Applicandae Math., to appear
7. R. Carroll, Proc. Conf. Diff. Eqs., Univ. Bologna, July, 1985, to appear
8. R. Carroll, Transmutation theory and applications, North-Holland, 1985
9. R. Carroll, Rocky Mount. Jour. Math., 12 (1982), 393-427
10. R. Carroll, Some spectral formulas for systems and transmission lines, to appear
11. R. Carroll, Some comments on the integral equations of inverse scattering theory, to appear
12. R. Carroll and F. Santosa, Applicable Anal., 13 (1982), 271-277
13. R. Carroll and F. Santosa, Conf. Inverse Scattering, SIAM, 1983, pp. 230-244
14. R. Carroll and S. Dolzycki, Applicable Anal., 19 (1985), 189-200
15. H. Dym and A. Iacob, Topics Oper. Theory, Birkhauser, 1984, pp. 141-240
16. H. Dym and D. Alpay, Integ. Eqs. Oper. Theory, 7 (1984), 589-641 and 8 (1985), 145-180
17. L. Fadeev, Uspekhi Mat. Nauk, 14 (1959), 57-119
18. M. Howard, Geophysics, 48 (1983), 163-170
19. R. Newton, Conf. Inverse Scattering, SIAM, 1983, pp. 1-74
20. F. Santosa, Geophys. J. Roy. Astr. Soc., 70 (1982), 229-243

Mathematics Department
University of Illinois
Urbana, Illinois 61801
U.S.A.

Received 31 January, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 2, Apr. 1986 avr.

ON THE ZETA FUNCTION ATTACHED TO THE REDUCTIVE DUAL PAIR ($\underline{\underline{MO}}(p,q,\underline{\underline{R}}),\underline{\underline{Mp}}(1,\underline{\underline{R}})$) IN THE METAPLECTIC GROUP $\underline{\underline{Mp}}(p+q,\underline{\underline{R}})$

Walter Schempp

Presented by P.C. Greiner, F.R.S.C.

1. Introductory Remarks on the Restricted Metaplectic Representation

Let $p \geqq 0$ and $q \geqq 0$ denote integers having the sum $n=p+q \geqq 2$. Fix the standard non-degenerate $\underline{\underline{R}}$-bilinear form $(.|.)_{p,q}$ of signature (p,q) on the n-dimensional real vector space $\underline{\underline{R}}^n=\underline{\underline{R}}^p \oplus \underline{\underline{R}}^q$. Then we have the decomposition $(.|.)_{p,q}=(.|.)_{p,0}-(.|.)_{0,q}$ into a positive and a negative definite $\underline{\underline{R}}$-bilinear form on $\underline{\underline{R}}^p$ and $\underline{\underline{R}}^q$, respectively, by putting

$$(x|y)_{p,q}=\sum_{1\leqq j\leqq p} x_j y_j - \sum_{p+1\leqq j\leqq n} x_j y_j .$$

We shall adapt the complex Hilbert space $L^2(\underline{\underline{R}}^n)$ to this decomposition of $(.|.)_{p,q}$ by setting $L^2(\underline{\underline{R}}^n)=L^2(\underline{\underline{R}}^p)\otimes L^2(\underline{\underline{R}}^q)$. Let $\mathscr{S}(\underline{\underline{R}}^n)$ denote the complex Schwartz-Bruhat space on $\underline{\underline{R}}^n$. For any function $f \in \mathscr{S}(\underline{\underline{R}}^n)$ we will also adapt its Fourier transform to $(.|.)_{p,q}$ according to the rule

$$\mathscr{F}_{\underline{\underline{R}}^p \oplus \underline{\underline{R}}^q} f(y) = \int_{\underline{\underline{R}}^n} f(x) e^{-2\pi i (x|y)_{p,q}} dx \qquad (y \in \underline{\underline{R}}^n).$$

Let $\underline{\underline{O}}(p,q,\underline{\underline{R}})$ denote the isometry group of the quadratic form $\underline{\underline{R}}^n \ni x \longmapsto (x|x)_{p,q}$, i.e., the group of linear transformations preserving $(.|.)_{p,q}$. Then $\mathscr{F}_{\underline{\underline{R}}^p \oplus \underline{\underline{R}}^q}$ commutes with the action of the pseudo-orthogonal group $\underline{\underline{O}}(p,q,\underline{\underline{R}})$ on $\underline{\underline{R}}^n$. In the case $0<p<n$ the group $\underline{\underline{O}}(p,q,\underline{\underline{R}})$ acting on $\underline{\underline{R}}^n$ has four connected components each component containing one component of the maximal compact subgroup $\underline{\underline{O}}(p,0,\underline{\underline{R}}) \times \underline{\underline{O}}(0,q,\underline{\underline{R}})$. Klein's Vierergruppe transforms the connected component $\underline{\underline{SO}}(p,q,\underline{\underline{R}})$ of the identity in the pseudo-orthogonal group $\underline{\underline{O}}(p,q,\underline{\underline{R}})$ onto the whole group $\underline{\underline{O}}(p,q,\underline{\underline{R}})$. In the case $n=4$, $p=1$, $q=3$ the proper Lorentz group $\underline{\underline{SO}}(1,3,\underline{\underline{R}})$ in 4 variables arises.

Form the real metaplectic group $\underline{\underline{Mp}}(n,\underline{\underline{R}})$ which is a central exten-

---

Because of an unfortunate misunderstanding, a preliminary version of this paper was published in Math. Reports, Vol. VIII (1), 43-48. Here is the final improved version provided by the author.

sion of the real symplectic group $\underline{\underline{Sp}}(n,\underline{\underline{R}})$ by $\underline{\underline{Z}}/2\underline{\underline{Z}}$. Then each fiber of the covering homomorphism $\underline{\underline{Mp}}(n,\underline{\underline{R}}) \ni \tilde{\sigma} \longrightarrow \sigma \in \underline{\underline{Sp}}(n,\underline{\underline{R}})$ consists of two different points. Let $\underline{\underline{MO}}(p,q,\underline{\underline{R}})$ be the inverse image of $\underline{\underline{O}}(p,q,\underline{\underline{R}})$ in $\underline{\underline{Mp}}(n,\underline{\underline{R}})$. Then $(\underline{\underline{MO}}(p,q,\underline{\underline{R}}),\underline{\underline{Mp}}(1,\underline{\underline{R}}))$ forms a reductive dual pair in the real metaplectic group $\underline{\underline{Mp}}(n,\underline{\underline{R}})$. In order to explain some details of this notion, let $(\underline{\underline{R}}^2,b)$ denote the two-dimensional real symplectic vector space with the standard symplectic form given by

$$b:\ \underline{\underline{R}}^2 \times \underline{\underline{R}}^2 \ni ((u,u'),(v,v')) \longrightarrow \det\begin{pmatrix} u & u' \\ v & v' \end{pmatrix} \in \underline{\underline{R}}.$$

Then $\underline{\underline{Sp}}(\underline{\underline{R}},b)=\underline{\underline{Sp}}(1,\underline{\underline{R}})=\underline{\underline{SL}}(2,\underline{\underline{R}})$. Obviously the tensor product $B_{p,q}=(.|.)_{p,q} \otimes b$ represents a non-degenerate alternating $\underline{\underline{R}}$-bilinear form on $\underline{\underline{R}}^{2n} = \underline{\underline{R}}^{2p} \oplus \underline{\underline{R}}^{2q}$ and $(\underline{\underline{R}}^{2n},B_{p,q})$ forms a 2n-dimensional real symplectic vector space. Let $\tilde{A}(\underline{\underline{R}}^n)$ denote the (2n+1)-dimensional real Heisenberg nilpotent Lie group with underlying manifold $\underline{\underline{R}}^n \oplus \underline{\underline{R}}^n \oplus \underline{\underline{R}}$ and multiplicative group law

$$(x,y,z).(x',y',z') = (x+x',y+y',z+z'+\tfrac{1}{2}B_{p,q}((x,x'),(y,y'))).$$

Then $\tilde{A}(\underline{\underline{R}}^n)$ forms a central extension of $\underline{\underline{R}}^{2n}$ by $\underline{\underline{R}}$ and the real symplectic group $\underline{\underline{Sp}}(\underline{\underline{R}}^n,B_{p,q})$ acts as a group of automorphisms of $\tilde{A}(\underline{\underline{R}}^n)$ leaving the one-dimensional center $\underline{\underline{R}}$ of $\tilde{A}(\underline{\underline{R}}^n)$ fixed (cf.[7]). An application of the Stone-von Neumann-Mackey uniqueness theorem implies via the covariance identity for the linear Schrödinger representation of $\tilde{A}(\underline{\underline{R}}^n)$ the existence of the Segal-Shale-Weil metaplectic (or linear oscillator) representation $\underline{\underline{Mp}}(\underline{\underline{R}}^n,B_{p,q}) \ni \tilde{\sigma} \longrightarrow T_{\tilde{\sigma}} \in \underline{\underline{U}}(L^2(\underline{\underline{R}}^n))$ of the real metaplectic group $\underline{\underline{Mp}}(\underline{\underline{R}}^n,B_{p,q})$ in the complex Hilbert space $L^2(\underline{\underline{R}}^n)$. Since the direct product $\underline{\underline{MO}}(p,q,\underline{\underline{R}}) \times \underline{\underline{Mp}}(1,\underline{\underline{R}})$ is naturally embedded into $\underline{\underline{Mp}}(\underline{\underline{R}}^n,B_{p,q})$, we may consider the restriction $T^{p,q} = T\,|(\underline{\underline{MO}}(p,q,\underline{\underline{R}}) \times \underline{\underline{Mp}}(1,\underline{\underline{R}}))$ of the metaplectic representation $(T,L^2(\underline{\underline{R}}^n))$ of $\underline{\underline{Mp}}(\underline{\underline{R}}^n,B_{p,q})$. $(T^{p,q},L^2(\underline{\underline{R}}^n))$ is called to be the restricted metaplectic representation attached to the reductive dual pair $(\underline{\underline{MO}}(p,q,\underline{\underline{R}}),\underline{\underline{Mp}}(1,\underline{\underline{R}}))$ in the metaplectic group $\underline{\underline{Mp}}(n,\underline{\underline{R}})$; cf. Gelbart [2]. The images of $\underline{\underline{MO}}(p,q,\underline{\underline{R}})$ and $\underline{\underline{Mp}}(1,\underline{\underline{R}})$ in the unitary group $\underline{\underline{U}}(L^2(\underline{\underline{R}}^n))$ form the centralizer of the other, whence the name. A calculation of the 2-cocycle of the projective linear representation $\underline{\underline{O}}(p,q,\underline{\underline{R}}) \times \underline{\underline{Sp}}(1,\underline{\underline{R}}) \ni \sigma \longrightarrow T^{p,q}_{\sigma} \in \underline{\underline{U}}(L^2(\underline{\underline{R}}^n))$ associated with the restricted metaplectic representation

$(T^{p,q}, L^2(\mathbb{R}^n))$ shows that it is isomorphic to an ordinary unitary linear representation of $\mathbb{O}(p,q,\mathbb{R}) \times \mathbb{Sp}(1,\mathbb{R})$ in a complex Hilbert space if and only if $n \geq 2$ is an even integer.

Suppose $p>1$ and $q>1$. For each pair $(k,l) \in \mathbb{N} \times \mathbb{N}$ of integers ≥ 0 let $H_k(\mathbb{R}^p)$ and $H_l(\mathbb{R}^q)$ denote the complex vector spaces of solid spherical harmonic functions of degree k on $\mathbb{R}^p$ and degree l on $\mathbb{R}^q$, respectively. It is the purpose of this note to attach to every function $f \in \mathcal{S}(\mathbb{R}^n)$ and every pair $(P_k, Q_l) \in H_k(\mathbb{R}^p) \times H_l(\mathbb{R}^q)$ a bivariate zeta function $(s,t) \longrightarrow \zeta(f;P_k,Q_l;s,t)$. We will establish a functional equation and the holomorphic continuation of the zeta function $\zeta(f;P_k,Q_l;.,.)$ by means of the restricted metaplectic representation $(T^{p,q}, L^2(\mathbb{R}^n))$ attached to the dual reductive pair $(\mathbb{MO}(p,q,\mathbb{R}), \mathbb{Mp}(1,\mathbb{R}))$ in the metaplectic group $\mathbb{Mp}(n,\mathbb{R})$. Finally we compare our results with the investigations recently done in this field by Neil Ormerod.

2. The Decomposition of $L^2(\mathbb{R}^n)$ According to the Action of $T^{p,q}$

Suppose $p>1$ and $q>1$. Let $\Delta_{p,q}$ denote the Laplacian operator corresponding to the standard quadratic form $x \longrightarrow (x|x)_{p,q}$ of signature (p,q) on $\mathbb{R}^n$. Recall that the elements of the complex vector spaces $H_k(\mathbb{R}^p), k \in \mathbb{N}$, and $H_l(\mathbb{R}^q), l \in \mathbb{N}$, respectively, are the homogeneous polynomials P (resp. Q) with complex coefficients of degree k (resp. l) in p (resp. q) real variables such that $\Delta_{p,0}P = 0$ (resp. $\Delta_{0,q}Q = 0$). It is well known (cf. [1,8]) that the natural action of the compact orthogonal group $\mathbb{O}(p,0,\mathbb{R})$ on $H_k(\mathbb{R}^p)$ defines a finite dimensional, irreducible, linear representation $(D_{k,p}, H_k(\mathbb{R}^p))$ of $\mathbb{O}(p,0,\mathbb{R})$. Similarly $H_l(\mathbb{R}^q)$ may be considered as $\mathbb{O}(0,q,\mathbb{R})$-module under the action of the irreducible linear representation $(D_{l,q}, H_l(\mathbb{R}^q))$ of the compact orthogonal group $\mathbb{O}(0,q,\mathbb{R})$.

If $P \in H_k(\mathbb{R}^p)$ then $\mathbb{R}^p \ni \xi \longrightarrow P(\xi)e^{-\pi(\xi|\xi)_{p,0}} \in \mathbb{C}$ forms a lowest weight vector for the representation $(T^{p,0}, L^2(\mathbb{R}^p))$ of weight $k+\frac{1}{2}p$. Let $\mathbb{C}_+ = \{ z=x+iy \mid x \in \mathbb{R}, y \in \mathbb{R}, y>0 \}$ denote the open upper half-plane and for any positive integer or half integer m let $H_m(\mathbb{C}_+)$ denote the complex vector space of all holomorphic functions on $\mathbb{C}_+$ such that $\lim_{z \in \mathbb{C}_+, |z| \to \infty} |\varphi(z)| = 0$ and $\int_{\mathbb{C}_+} |\varphi'|^2 y^m dx dy < \infty$.

If $(D_m, H_m(\mathbb{C}_+))$ denotes the holomorphic series of unitary linear representations of $\underline{\underline{Mp}}(1,\underline{\underline{R}})$ with lowest weight m and similarly $(\bar{D}_m, \bar{H}_m(\mathbb{C}_+))$ denotes the antiholomorphic series of unitary linear representations of $\underline{\underline{Mp}}(1,\underline{\underline{R}})$ with lowest weight m then these representations belong to the holomorphic resp. antiholomorphic discrete series (cf. Lang [3]) for m>1.

Theorem 1. Let p>1 and q>1. The restriction $T_o^{p,q} = T^{p,q}|(\underline{\underline{O}}(p,q,\underline{\underline{R}}) \times \underline{\underline{Mp}}(1,\underline{\underline{R}}))$ of the restricted metaplectic representation $(T^{p,q}, L^2(\underline{\underline{R}}^n))$ attached to the reductive dual pair $(\underline{\underline{MO}}(p,q,\underline{\underline{R}}), \underline{\underline{Mp}}(1,\underline{\underline{R}}))$ in the metaplectic group $\underline{\underline{Mp}}(n,\underline{\underline{R}})$ admits the decomposition

$$(T_o^{p,q}, L^2(\underline{\underline{R}}^n)) = \widehat{\bigoplus_{(k,l) \in \underline{\underline{N}} \times \underline{\underline{N}}}} ((D_{k,p}, H_k(\underline{\underline{R}}^p)) \underset{\mathbb{C}}{\otimes} (D_{l,q}, H_l(\underline{\underline{R}}^q)) \underset{\mathbb{C}}{\otimes} (D_{k+\frac{1}{2}p}, H_{k+\frac{1}{2}p}(\mathbb{C}_+)) \underset{\mathbb{C}}{\otimes} (\bar{D}_{l+\frac{1}{2}q}, \bar{H}_{l+\frac{1}{2}q}(\mathbb{C}_+)))$$

3. The Zeta Function $\zeta(f;P_k,Q_l;.,.)$

The compact unit spheres in $\underline{\underline{R}}^p$ (p>1) and $\underline{\underline{R}}^q$ (q>1) are given by $\underline{\underline{S}}_{p-1} = \underline{\underline{O}}(p,0,\underline{\underline{R}})/\underline{\underline{O}}(p-1,0,\underline{\underline{R}})$ and $\underline{\underline{S}}_{q-1} = \underline{\underline{O}}(0,q,\underline{\underline{R}})/\underline{\underline{O}}(0,q-1,\underline{\underline{R}})$, respectively. If $d\sigma_p$ resp. $d\sigma_q$ denote the normalized Haar measures of the compact orthogonal groups $\underline{\underline{O}}(p,0,\underline{\underline{R}})$ and $\underline{\underline{O}}(0,q,\underline{\underline{R}})$, respectively, then the surface measures $d\omega_{p-1} = d\sigma_p/d\sigma_{p-1}$ and $d\omega_{q-1} = d\sigma_q/d\sigma_{q-1}$ of $\underline{\underline{S}}_{p-1}$ and $\underline{\underline{S}}_{q-1}$, respectively, give rise to the following decomposition of the Lebesgue measure of $\underline{\underline{R}}^n$:

$$dx = \mathrm{vol}(\underline{\underline{S}}_{p-1}) r_1^{p-1} dr_1 \otimes d\omega_{p-1} \otimes \mathrm{vol}(\underline{\underline{S}}_{q-1}) r_2^{q-1} dr_2 \otimes d\omega_{q-1}$$

Let $(P_k, Q_l) \in H_k(\underline{\underline{R}}^p) \times H_l(\underline{\underline{R}}^q)$ be an arbitrary pair of solid spherical harmonic functions of degree $k \geq 0$ resp. $l \geq 0$ on $\underline{\underline{R}}^p$ resp. $\underline{\underline{R}}^q$. Define the bivariate zeta function $\zeta(f;P_k,Q_l;.,.)$ attached to $f \in \mathcal{S}(\underline{\underline{R}}^n)$ and the pair $(P_k,Q_l) \in H_k(\underline{\underline{R}}^p) \times H_l(\underline{\underline{R}}^q)$ according to the prescription

$$\zeta(f;P_k,Q_l;s,t) = \int_{\underline{\underline{R}}^n} f(x)\bar{P}_k(\xi)\bar{Q}_l(\eta) r_1^{s-k-p/2} r_2^{t-l-q/2} dx$$

where $\underline{\underline{R}}^n \ni x = (\xi,\eta) \in \underline{\underline{R}}^p \oplus \underline{\underline{R}}^q$, $r_1^2 = (\xi|\xi)_{p,0}$, and $r_2^2 = (\eta|\eta)_{0,q}$.

For any function $f \in \mathscr{S}(\underline{\underline{R}}^n)$ belonging to an isotypic component of the action of $\underline{\underline{O}}(p,0,\underline{\underline{R}}) \times \underline{\underline{O}}(0,q,\underline{\underline{R}})$ on $L^2(\underline{\underline{R}}^n)$ there is a decomposition

$$f(x) = P_k(\xi)Q_l(\eta)g(r_1,r_2) \qquad (x \in \underline{\underline{R}}^n)$$

and in this case we get $\zeta(f;P_k,Q_l;.,.)$ as the Mellin transform

$$\zeta(f;P_k,Q_l;s,t) = \int_{\underline{\underline{S}}_{p-1}} |P_k|^2 \, d\omega_{p-1} \int_{\underline{\underline{S}}_{q-1}} |Q_l|^2 d\omega_{q-1} \cdot$$

$$\int_{\underline{\underline{R}}_+}\int_{\underline{\underline{R}}_+} g(r_1,r_2) r_1^{s+k+p/2-1} \, r_2^{t+l+q/2-1} dr_1 dr_2 .$$

Now we are in a position to establish a functional equation for the zeta function $\zeta(f;P_k,Q_l;.,.)$ and, at the same time, we may study the holomorphic continuation of this bivariate function.

Theorem 2. Suppose $p>1$ and $q>1$. For every function $f \in \mathscr{S}(\underline{\underline{R}}^n)$ and all pairs $(P_k,Q_l) \in H_k(\underline{\underline{R}}^p) \times H_l(\underline{\underline{R}}^q)$ of solid spherical harmonic functions of degree $k \geq 0$ resp. $l \geq 0$ on $\underline{\underline{R}}^p$ resp. $\underline{\underline{R}}^q$, the bivariate zeta function $\zeta(f;P_k,Q_l;.,.)$ admits a holomorphic continuation for all pairs $(s,t) \in \mathbb{C}^2$ such that $s+k+\frac{1}{2}p \notin -2\underline{\underline{N}}$ and $t+l+\frac{1}{2}q \notin -2\underline{\underline{N}}$ and satisfies the functional equation

$$\zeta(f;P_k,Q_l;s,t) = i^{k+l} \pi^{-(s+t)} \frac{\Gamma(\frac{1}{2}(s+k+\frac{1}{2}p))\,\Gamma(\frac{1}{2}(t+l+\frac{1}{2}q))}{\Gamma(\frac{1}{2}(-s+k+\frac{1}{2}p))\,\Gamma(\frac{1}{2}(-t+l+\frac{1}{2}q))} \cdot$$

$$\zeta(\mathscr{F}_{\underline{\underline{R}}^p \oplus \underline{\underline{R}}^q} f;P_k,Q_l;-s,-t) .$$

Proof (Sketch). Look at the decomposition $f = P_k \otimes Q_l \otimes g$ as before. Consider the Weyl element

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

of $\underline{\underline{SL}}(2,\underline{\underline{R}})$ and evaluate $T_0^{p,q}(u)f$ at the element $u = \mathrm{id}_{\underline{\underline{R}}^p \oplus \underline{\underline{R}}^q} \otimes \tilde{w}$ of $\underline{\underline{O}}(p,q,\underline{\underline{R}}) \times \underline{\underline{Mp}}(1,\underline{\underline{R}})$. Then we obtain the identity

$$i^{(p-q)/2} \mathscr{F}_{\underline{\underline{R}}^p \oplus \underline{\underline{R}}^q} f = P_k \otimes Q_l \otimes D_{k+\frac{1}{2}p} \otimes \bar{D}_{l+\frac{1}{2}q}(\tilde{w})g .$$

Since $D_{k+\frac{1}{2}p} \otimes \bar{D}_{l+\frac{1}{2}q}(\tilde{W})g$ is a Hankel transform of g of order $k+\frac{1}{2}p-1$ in the first variable and a Hankel transform of order $l+\frac{1}{2}q-1$ in the second variable, the result follows by taking the Mellin transforms (cf.[6]) of both sides. -

4. Concluding Remarks

Theorem 2 generalizes a result of Ormerod [5] (also see [4]) who considered the case q=0. This author, however, applies harmonic analysis only of the compact orthogonal group $\underline{O}(p,0,\underline{R})$ by appealing to the Funk-Hecke Theorem (cf. Coifman-Weiss [1]) and does not refer explicitly to the less classical "dual part" in the reductive dual pair $(\underline{MO}(p,0,\underline{R}),\underline{Mp}(1,\underline{R}))$ in the metaplectic group $\underline{Mp}(p,\underline{R})$.

Acknowledgments. The present paper includes some parts of a research work done when the author visited the Seoul National University in Korea, the Academia Sinica, and the Peking University in the People's Republic of China. The author is grateful to these institutions for their kind hospitality extended to him.

References

1. Coifman, R.R., Weiss, G.: Representations of compact groups and spherical harmonics. Enseignement math. 14 (1968), 121-173.
2. Gelbart, S.: Examples of dual reductive pairs. In: Automorphic forms, representations and L-functions. Proc. of Symposia in Pure Math., Vol. 33 (1979), Part 1, pp. 287-296.
3. Lang, S.: $SL_2(\underline{R})$. Reading, MA: Addison-Wesley 1975.
4. Ormerod, N.: A theorem on Fourier transforms of radial functions. J. Math. Anal. Appl. 69 (1979), 559-562.
5. Ormerod, N.: Fourier transforms and harmonic functions. J. Austral. Math. Soc. (Ser. A) 36 (1984), 187-193.
6. Schempp, W.: Complex contour integral representation of cardinal spline functions. Providence, RI: Amer. Math. Soc. 1982.
7. Schempp, W.: Harmonic analysis on the Heisenberg nilpotent Lie group, with applications to signal theory. London: Pitman (in print).
8. Schempp, W., Dreseler, B.: Einführung in die harmonische Analyse. Stuttgart: Teubner 1980.

Lehrstuhl fuer Mathematik I
University of Siegen
D-5900 Siegen
Federal Republic of Germany

Received 4 February, 1986

Mailing Addresses

1. R. Carroll — Department of Mathematics
University of Illinois
Urbana, Illinois 61801, U.S.A.

2. M. Csörgő — Department of Mathematics
and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6

3. E.G. Goodaire — Department of Mathematics
and Statistics
Memorial University of Newfoundland
St. John's, Newfoundland, Canada
A1C 5S7

4. I. Halperin — Department of Mathematics
University of Toronto
Toronto, Ontario, Canada M5S 1A1

5. Y. Hellegouarch — Département de Mathématiques
et de Mécanique
Université de Caen
14032 Caen Cedex, France

6. L. Horváth — Bolyai Institute, Szeged University
Aradi Vértanúk Tere 1
H-6720 Szeged, Hungary

7. C.U. Jensen — Matematisk Institut
Universitetsparken 5
2100 Copenhagen Ø, Denmark

8. AR. Meenakshi — Department of Mathematics
Annamalai University
Annamalainagar - 608002
India

9. J. Mináč — Department of Mathematics
and Statistics
Queen's University
Kingston, Ontario, Canada K7L 3N6

10. D.S. Mitrinović — Faculty of Electrical Engineering
University of Belgrade
Yugoslavia

11. R.A. Mollin — Department of Mathematics
University of Calgary
Calgary, Alberta, Canada T2N 1N4

12. M.M. Parmenter — Department of Mathematics
and Statistics
Memorial University of Newfoundland
St. John's, Newfoundland, Canada
A1C 5S7

13. J.E. Pěcarié — Faculty of Electrical Engineering
University of Belgrade
Yugoslavia

14. W. Schempp — Lehrstuhl fuer Mathematik I
University of Siegen, D-5900 Siegen
Federal Republic of Germany

15. R.A.G. Seely — Department of Mathematics
John Abbott College, C.P. 2000
Ste. Anne de Bellvue, Quebec, Canada
H9X 3L9

16. J. Steinabach — Fachbereich Mathematik
Universitat Marburg
Hans-Meerwein-Strasse, D-3550 Marburg
West Germany

17. L. Székelyhidi — Department of Mathematics
L. Kossuth University
H-4010 Debrecen, Pf.12, Hungary

18. P.G. Walsh — Department of Mathematics
University of Calgary
Calgary, Alberta, Canada T2N 1N4