<table>
<thead>
<tr>
<th>Date</th>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Nov/84</td>
<td>Memoir: Can one develop a noncommutative geometry for group theory?</td>
<td>P. Ribenboim F.R.S.C.</td>
</tr>
<tr>
<td>13 July/84</td>
<td>On the Congruences of Voronoi and Kummer for the Bernoulli numbers.</td>
<td>T. Agoh</td>
</tr>
<tr>
<td>27 Aug/84</td>
<td>Sur le radical de Jacobson dans les algèbres localement A-convexes</td>
<td>M. Oudadess</td>
</tr>
<tr>
<td>18 Oct/84</td>
<td>Ordinary arcs on convex bodies.</td>
<td>T. Biswarincky and P. Scherk</td>
</tr>
<tr>
<td>5 Nov/84</td>
<td>A remark about Vandiver’s Conjecture</td>
<td>I. Kersten and J. Michalicek</td>
</tr>
<tr>
<td>12 Nov/84</td>
<td>Orthogonal polynomials and transmutation</td>
<td>R. Carroll</td>
</tr>
<tr>
<td>28 Nov/84</td>
<td>On a functional equation connected to uniform non-additive information measures in an open domain.</td>
<td>P. Kannappan and P.K. Sahoo</td>
</tr>
<tr>
<td>29 Nov/84</td>
<td>Approximation Diophantienne par certains couples d’entiers.</td>
<td>F. Thurnheer</td>
</tr>
<tr>
<td>29 Nov/84</td>
<td>The set of exponents for which Fermat’s last theorem is true, has density one.</td>
<td>A. Granville</td>
</tr>
<tr>
<td>30 Nov/84</td>
<td>Groups with fixed-point-free automorphisms</td>
<td>I. Hughes</td>
</tr>
<tr>
<td>Date</td>
<td>Title</td>
<td>Authors</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>3 Dec/84</td>
<td>Détermination du groupe des automorphismes du p-groupe de Sylow du groupe symétrique de degré $p^n$ : l'idée de la méthode.</td>
<td>P. Lentoudis</td>
</tr>
<tr>
<td>5 Dec/84</td>
<td>Groups of projectivities of topological planes.</td>
<td>D. Betten and C. Weigand</td>
</tr>
<tr>
<td>5 Dec/84</td>
<td>Class multipliers for the orthogonal group over GF(2)</td>
<td>J.S. Frame</td>
</tr>
<tr>
<td>11 Dec/84</td>
<td>Sum form equations on an open domain I.</td>
<td>L. Losonci</td>
</tr>
<tr>
<td>17 Dec/84</td>
<td>Unités de certains sous-anneaux de corps de fonctions algébriques.</td>
<td>R. Paysant-le Roux, D.L. McQuillan, Y. Hellegouarch</td>
</tr>
<tr>
<td>2 Jan/85</td>
<td>The index of elliptic operators on a mapping torus.</td>
<td>B. Booss and K. Wojciechowski</td>
</tr>
</tbody>
</table>

Mailing Addresses 103
CAN ONE DEVELOP A NONCOMMUTATIVE GEOMETRY
FOR GROUP THEORY?

Paulo Ribenboim
F.R.S.C.

Dedicated to János Aczél on the occasion of his sixtieth birthday

The answer to this question is "maybe", and I wish to explain why I do not rule out immediately the possibility of developing a geometric language for group theory.

In (commutative) algebraic geometry, it is question of studying coordinate rings of varieties and their prime ideals. This leads to the concept of the spectrum of a commutative ring $A$. 
For the purpose of my discussion, I recall that Spec $A$ consists of a topological base space and a sheaf of local rings. The base space is the set of all prime ideals $p$ of $A$, with Zariski's topology. The sheaf of rings has stalk at $p$ equal to the localization of $A$ at $p$.

The fundamental theorem that justifies the consideration of the spectrum of $A$ states that $A$ is isomorphic to the ring of global sections of Spec $A$.

My aim is to indicate that a framework of a similar kind may be conceived in the study of groups — this involves of course nonabelian groups, finite or infinite, but also special classes of groups, like profinite groups. Specifically, the analogue of the spectrum of a ring should be proposed, including the base space; global sections and the process of localization.

1. How to introduce a "spectrum" for groups?

In commutative ring theory, the spectrum serves to analyze the ring, looking at every local piece, and the ring may be synthesized from the local data by forming the ring of global sections.

In group theory, a direct imitation of the construction for rings does not seem feasible. However, it is possible to grasp the spirit of the construction and do something analogue for groups. In the synthesis, it is essential to build the group from given data. Now the data consists of a given family of groups (analogous to the stalks), with appropriate homomorphisms (counterpart to the morphisms of localization). For groups there are also "twists", i.e. actions, which of course are trivial in a commutative situation.

So this comparison leads to the concept of an active family of groups as the data, and their active sum, as the analogue of the ring of global sections (see [8]).

Let $I$ be a partially ordered set — which is to be construed as the analogue of the partially ordered set of prime ideals of a ring. Actually, in order to cover a situation of interest just like in the theory of quivers, I may wish to take $I$ as a directed multigraph, however I shall abstain from doing it here.
Can one develop a noncommutative geometry for group theory?

Let \((G_i)_{i \in I}\) be a family of groups and, if \(i, j \in I\) and \(i \leq j\), let \(\phi_{ij}: G_i \to G_j\) be a homomorphism; moreover, \(\phi_{ii}\) is the identity and if \(i \leq j \leq k\) then \(\phi_{ik} = \phi_{jk} \circ \phi_{ij}\). Thus, \((G_i)_{i \in I}\) is a directed family of groups, indexed by \(I\).

Let \(G = \bigcup_{i \in I} G_i\) be the disjoint union of the groups \(G_i\) \((i \in I)\). Let \(\pi: G \to I\) be the map such that \(\pi(g) = i\) exactly when \(g \in G_i\).

Let \((G'_i)_{i \in I'}, \phi_{i'i'}, G'_i, \pi'\) be given similarly.

A map \(\mu: G \to G'\) is compatible when it satisfies:

1) if \(g, h \in G\) and \(\pi(g) = \pi(h)\) then \(\pi(\mu(g)) = \pi(\mu(h))\); thus \(\mu\) defines a map \(\mu: I \to I'\) such that the following diagram is commutative:

\[
\begin{array}{ccc}
G & \xrightarrow{\pi} & I \\
\downarrow \mu & & \downarrow \mu' \\
G' & \xrightarrow{\pi'} & I'
\end{array}
\]

2) \(\mu\) preserves the order.

If \(\mu: G \to G'\), \(\mu': G' \to G'\) are compatible, so is \(\mu' \circ \mu\) and \(\mu' \circ \mu = \mu' \circ \mu\).

A compatible map \(\mu: G \to G'\) is a homomorphism when it satisfies: if \(\pi(g) = \pi(h)\) then \(\mu(gh) = \mu(g)\mu(h)\).

If \(\mu: G \to G'\), \(\mu': G' \to G'\) are homomorphisms then so is \(\mu' \circ \mu\).

A trivial case is a family consisting of only one group \(A\) (i.e. \(I = \{0\}, G_0 = A\)), which we denote by \(A\) for simplicity. So a homomorphism \(\mu: G \to A\) is a mapping such that if \(\pi(g) = \pi(h)\) then \(\mu(gh) = \mu(g)\mu(h)\).

A homomorphism \(\mu: G \to G'\) is an isomorphism when it is bijective and \(\mu^{-1}\) is compatible. It follows that \(\mu\) is also bijective and for every \(i \in I\), \(\mu|_{G_i}: G_i \to G'_{\pi(i)}\) is an isomorphism.

If \(\mu: G \to G'\), \(\mu': G' \to G'\) are isomorphisms so are \(\mu' \circ \mu\) and the inverse map \(\mu^{-1}: G' \to G\).
A homomorphism $\mu: G \to G$ is called an endomorphism of $G$. An isomorphism from $G$ to $G$ is called an automorphism of $G$. Let $\text{Aut}(G)$ denote the group of automorphisms of $G$.

A mapping $\tau: G \to \text{Aut}(G)$ is called an action when it satisfies:

1. If $\tau(g) = \tau(h)$ then $\tau_{gh} = \tau_g \circ \tau_h$,
2. If $1_i$ is the unit element of $G_i$ then $\tau_{1_i}$ is the identity automorphism of $G$,
3. If $g \in G_i$ then $\tau_g| G_i$ is the inner automorphism of $G_i$ defined by $g$ (hence $\tau_g(i) = i$),
4. If $\pi(g) = i \leq j$ then $\tau_{\phi_{ij}(g)} = \tau_g$.

In particular, if the action is trivial, each $G_i$ is abelian. If $\tau_I$ is the identity map of $I$, for every $g \in G$, the action is called normal.

The data $((G_i)_{i \in I}, \tau)$ is called an active family of groups.

Before proceeding, I wish to give some examples.

**Example 1.** Let $G$ be a finite group, let $(G_i)_{i \in I}$ be a family of subgroups of $G$, partially ordered by inclusion; if $G_i \subseteq G_j$ (with $i, j \in I$) take $\phi_{ij}$ to be the inclusion map. Let $G = \coprod_{i \in I} G_i$. For each $i \in I$, $g \in G$ assume that there exists $j \in I$ (necessarily unique) such that $g^{-1}G_i g = G_j$. Let $\tau_i: I \to I$ be defined by $\tau_i(i) = j$ and let $\tau_g: G \to G$ be given by the conjugation by $g$, that is, if $h \in G_i$ then $\tau_g(h) = g^{-1}hg \in G_{\tau_i(i)}$ thus $\tau$ is an action and $((G_i)_{i \in I}, \tau)$ is an active family of subgroups of $G$.

In particular, $(G_i)_{i \in I}$ may be the family $P$ of all primary subgroups (i.e. having prime-power order); or the family $S$ of all Sylow subgroups; or the family $M$ of all monogenous normal subgroups of $G$, i.e. all subgroups generated by one element and its conjugates). I note that, if each $G_i$ is a normal subgroup, then for each $g \in G$ the mapping $\tau_g$ is the identity map of $I$, that is the action $\tau$ is normal.

It is useful to consider active families of profinite groups, the definition being just about the same as before, with the exclusive consideration of continuous homomorphisms of profinite groups. This is worthwhile, in view of the following example ([7]).
Example 2. Let $K \mid Q$ be a Galois extension, $G = \text{Gal}(K \mid Q)$. For each prime ideal $p$ of the ring of integers of $K$ let $D_p = \{ \sigma \in G \mid \sigma(p) = p \}$ be the corresponding decomposition group. Let $D = (D_p)_p$ and let the action be defined by conjugation, as before. An active family of groups may be viewed like a sheaf of groups, the action being the structure twists. In the presence of this data, the object is "to untwist the sheaf building the group of global sections". Precisely, this leads to a universal problem, which has a solution, as indicated in the following theorem:

Let $((G_i)_{i \in I}, \tau, \eta)$ be an active family of groups. Then there exists a unique group $A$ and a homomorphism $\rho: G \to A$ (considered as a family with only one group) such that:

1. If $i, j \in I, i \leq j$, if $g \in G_i$ then $\rho(\phi_{ij}(g)) = \rho(g)$,

2. For every $g \in G$ the following diagram is commutative:

$$
\begin{array}{ccc}
G & \to & G \\
\rho \uparrow & & \downarrow \rho \\
A & \to & A \\
\end{array}
$$

$[\iota_{\rho(g)}]$ denotes the inner automorphism of $A$ defined by $\rho(g)$.

Moreover, $A, \rho$ have the universal property that if $A', \rho'$ are like $A, \rho$ then there exist a unique homomorphism $\psi: A \to A'$ such that $\rho' = \psi \circ \rho$.

$A, \rho$ are unique up to a unique isomorphism; $A$ is called the active sum of the given active family of groups.

If the action $\tau$ is the identity then $A$ is the direct limit of the abelian groups $G_i$ ($i \in I$). If moreover, $I$ is trivially ordered then $A$ is the direct sum of the abelian group $G_i$ ($i \in I$). This suggests to use the notation $A = \bigoplus_{i \in I} G_i$ (which is however very incomplete).

Construction of the active sum: Let $F$ be the free product of the family $(G_i)_{i \in I}$, let $R$ be the normal subgroup generated by the elements of $F$ of the form
Paulo Ribenboim

\[
\begin{align*}
\left\{ [g]^{-1}A[g][g^{-1}A]^{-1}, & \quad \forall g, h \in G \\
\left\{ \phi_j(g)[g]^{-1}A \right\}, & \quad \forall g \in G_j, i \leq j
\end{align*}
\]

(here \([g]\) denotes the image of \(g \in G\) in \(F\)). Let \(A = F/R\), \(\gamma : F \rightarrow A\) (canonical homomorphism) and \(\rho(g) = \gamma([g])\). Then \((A, \rho)\) defines the active sum of \(((G_i)_{i \in I}, \gamma)\).

In more specific cases, like two groups with mutual actions, the construction gives a quotient of the semi-direct product. This may also be extended to finitely many groups: If \((G_i)_{i \in I}\) is an active family of finite groups and \(I\) is also finite, then \(A = \bigoplus G_i\) is a finite group with order at most \(\prod \#(G_i)\). Moreover if the action is normal then \(\#(A)\) divides \(\prod \#(G_i)\). So in this case, if \(p\) is a prime and each \(G_i\) is a \(p\)-group then \(A\) is a \(p\)-group.

If \(G\) is a group, if \((G_i)_{i \in I}\) is a family of subgroups as in Example 1, let \(\rho: G = \bigcap G_i \rightarrow A = \bigoplus G_i\) let \(\tau: G \rightarrow G\) be the homomorphism induced by the inclusions \(G_i \subseteq G\). By the universal property, there is a unique homomorphism \(\psi: A \rightarrow G\) such that \(\psi \circ \rho = \iota\). Then \(\psi\) is surjective if and only if \(\bigcup G_i\) generates \(G\).

Taking \(G\) to be a finite group and \((G_i)_{i \in I} = P\) (the family of primary subgroups of \(G\)), the following theorem holds:

The active sum of the active family of primary subgroups of \(G\) is naturally isomorphic to \(G = \bigoplus P \cdot G\).

This means that a finite group is completely determined by the knowledge of its primary subgroups and their mutual actions. The existence theorem also tells that however complicated be the given finite active family \(P\) of finite primary groups, there exists a finite group \(G\) with this family \(P\) of primary groups and action given by conjugation.

The preceding main theorem does not hold in general for the family \(S\) of Sylow subgroups. For example, if \(G = S_4\) (symmetric group in 4 letters), then \(\bigoplus S = G \times C_2\) where \(C_2\) is the group of order 2.

A group \(G\) is atomic if there exists \(g \in G\) such that \(G\) is generated by \(g\) and its conjugates. A group \(G\) is molecular if there exists a family \(A\) of atomic subgroups stable under conjugation such that the canonical homomorphism \(\psi: \bigoplus A \rightarrow G\) is an iso-
Can one develop a noncommutative geometry for group theory?

morphism. The following can be shown: Every finite group (resp. finite $p$-group) is the quotient of a finite group (resp. finite $p$-group) $M$ which is molecular, by a central normal subgroup $K$ (hence abelian).

Now concerning Example 2, where $D = (D_p)_p$ is the family of decomposition groups for a Galois extension $K \mid K_0$ ($K_0$ a number field), it follows from Čebotarev's density theorem that $\bigcap D_p = \{1\}$ and also that $\bigcup D_p$ is a dense subset of $G = \text{Gal}(K \mid K_0)$. Then $\psi: \bigoplus D \rightarrow G$ is surjective.

All the above concepts and results are fully explained and developed in the papers [8] and [7].

2. Another aspect of group theory which is parallel to a procedure in commutative ring theory concerns localization. As a matter of fact, this has been developed already long ago, in the work of the Russian school (Kontorović, Mal'cev, Kurosh, Černikov, etc.) and has also been extensively studied by Baumslag. A new impetus has been given by a problem in Algebraic Topology, more specifically homotopy theory. Here it is question of the localization of the fundamental group of a space — mostly 1-connected CW-complexes, but also CW-complexes having nilpotent fundamental groups with nilpotent action on the higher homotopy group; see for example the book of Hilton, Mislin and Roitberg [5] and the lecture notes of Hilton [4].

In my recent work, partly still unpublished, I have succeeded in extending the theory of localization to arbitrary groups, using a totally different method. It was essential to develop a theory of torsion also for nonabelian groups.

I wish now to indicate these concepts, methods and some of the main results.

In his classical paper, Baumslag [1] used the following terminology. Let $\Pi$ be any set of prime numbers, and let $G$ be a group.

1) $G$ is a $U\Pi$-group when the following property holds: if $g_1,g_2 \in G$, if $p \in \Pi$ and $g_1^p = g_2^p$, then $g_1 = g_2$ (property of uniqueness of $p$-th roots).
(2) $G$ is an $E_{\Pi}$-group when: if $g \in G$, $p \in \Pi$, then there exists $h \in G$ such that $h^p = g$ (property of existence of $p$-th roots).

(3) $G$ is a $D_{\Pi}$-group when it is a $U_{\Pi}$-group and a $E_{\Pi}$-group.

If $\Pi$ is the set of all prime numbers then $U_{\Pi}$-groups were called $R$-groups by Kontorović and $E_{\Pi}$-groups were called rational groups by Mal’cev.

In the above cases the question is to solve the equations $X^p g^{-1} = 1$ for $g \in G$, $p \in \Pi$.

More generally, let $W \subseteq F(Y_1, Y_n, X)$ (the free group in $n + 1$ indeterminates, $n \geq 1$); so $W$ is a given set of words in the indeterminates $Y_1, \ldots, Y_n, X$.

For every group $G$, consider the set

$$W_G = \{w(g_1, \ldots, g_n, X) \mid (g_1, \ldots, g_n) \in G^n, w \in W\}$$

of words in one indeterminate and coefficients in $G$; these are therefore elements of the free product $G*F(Y)$.

For example, let $S$ be a set of positive integers, let $W = \{X^m Y^{-1} \mid m \in S\}$. For every group $G$ then $W_G = \{X^m Y^{-1} \mid g \in G, m \in S\}$.

The problem is to solve, respectively to solve uniquely, all equations $w(X) = 1$ with $w(X) \in W_G$, for a group $G$.

There is a clear analogy with the theory of commutative fields. Cyclotomic field extensions, which are obtained by adjunction of $m$-th roots, correspond to the extension of groups so as to contain solutions to arbitrary algebraic extensions. I have introduced the following concepts. Let $W$ be a set of words in the indeterminates $Y_1, \ldots, Y_n, X$.

$G$ is $W$-complete if, for every $w(X) \in W_G$, there exists $g \in G$ such that $w(g) = 1$.

$G$ is $W$-perfect if, for every $w(X) \in W_G$, there exists a unique $g \in G$ such that $w(g) = 1$.

So, if $W = \{X^p Y^{-1} \mid p \in \Pi\}$, where $\Pi$ is any set of prime numbers, then $G$ is $W$-complete exactly if it is an $E_{\Pi}$-group and $G$ is $W$-perfect when it is a $D_{\Pi}$-group.
The main problem is to find out whether there exists a universal $W$-perfection for any group $G$. More precisely, given $W$ and a group $G$, a $W$-perfection of $G$ is a pair $(G^W, \phi^W)$ with

1. $G^W$ is a $W$-perfect group $\phi^W: G \to G^W$ is a homomorphism.

2. If $H$ is a $W$-perfect group and $\psi: G \to H$ is a homomorphism then there exists a unique homomorphism $\psi^W: G^W \to H$ such that $\psi^W \circ \phi^W = \psi$.

If a $W$-perfection exists, it must be unique up to a unique isomorphism.

The following special cases are important:

$$W = W_S = \{X^SY^{-1} \mid s \in S\} \quad \text{where} \quad S \subseteq \{1,2,3\},$$
or more particularly, $W = W_\Pi$ where $\Pi$ is a set of prime numbers.

If $\Pi'$ is the complement of $\Pi$ in the set of all prime numbers, then the $\Pi'$-perfection of $G$ has been called the $\Pi'$-localization of $G$, explicitly denoted by $(G_{\Pi'}, \phi_{\Pi'})$.

It has the following properties:

1. for every prime number $p \in \Pi$ and $g \in G_{\Pi}$ there exists a unique $h \in G_{\Pi}$ such that $h^p = g$, and $\phi_{\Pi}: G \to G_{\Pi}$ is a homomorphism.

2. the analogous universal property.

For example, if $\Pi = \emptyset$ then the $\Pi$-localization is the rationalization of Mal'cev.

The existence of $\Pi$-localization may be shown using arguments of category theory (see Warfield [9]) or universal algebra (following ideas of Birkhoff [2]).

I have given two proofs for the existence of the $W$-perfection of a group. The first one, which uses general algebra-categorical principles, is simple but does not allow to keep any control on the structure of the $W$-perfection.

The second proof is of a relatively concrete nature and I describe it here in the special case of the $\Pi$-perfection. The idea is to adjoin $p$-th roots of $g$ to $G$, for every $g \in G$ and $p \in \Pi$, then to amalgamate in order to guarantee that each $p$-th root is unique. The proof consists of successive steps and requires the concept of torsion closure of a subgroup.
First step: For every \( p \in \Pi, \varrho \in G \) let \( X_{\varrho,p} \) be a symbol, let \( F = F(X_{\varrho,p}) \) be the free group generated by these symbols and consider the free product \( G^{*}F(X_{\varrho,p})_{\varrho,p} \). Let \( R \) be the normal subgroup generated by all elements \( X_{\varrho,p}^{p-1} \). Thus in \( G^{*}F/R \) every \( g \in G \) has a \( p \)-th root in \( G^{*}F \), however it is not necessarily unique.

The \( \Pi \)-torsion closure \( T_{\Pi}(G^{*}F,R) \) of \( R \) in \( G^{*}F \) is introduced to guarantee the uniqueness of \( p \)-th roots. More generally, if \( K \) is any group, if \( H \) is a normal subgroup of \( K \) and \( \Pi \) is a set of prime numbers, an element \( y \in K \) is an element of torsion-type relative to \( H \) (and \( \Pi \)) if there exists elements \( h_{1}, h_{2} \in H, k_{1}, k_{2} \in K \) such that \( y = k_{1}k_{2}^{-1} \) and \( k_{1}h_{1} = h_{2}k_{2} \). Let \( T_{1}(H) \) be the set of finite products of elements of torsion-type as above; then \( T_{1}(H) \) is a normal subgroup of \( K \). Let \( T_{i+1} = T_{1}(T_{i}(H)) \) for every \( i \geq 1 \) and \( T_{\Pi}(K,H) = T(H) = \bigcup_{i=1}^{\infty} T_{i}(H) \). \( T_{\Pi}(K,H) \) is a normal subgroup of \( K \) called the \( \Pi \)-torsion closure of \( H \) in \( K \). A similar notion of \( W \)-torsion closure of \( H \) in \( K \) may be defined with respect to a set \( W \) of words.

This notion yields a good theory of torsion. \( K \) is \( \Pi \)-torsion free when \( T_{\Pi}(K,\{1\}) = \{1\} \). Thus, if \( H \) is a normal subgroup of \( K \), then \( K/T_{\Pi}(K,H) \) is \( \Pi \)-torsion free; etc.

Now, I return to the construction of the \( \Pi \)-perfection of \( G \). Taking the natural homomorphism \( \phi^{1}: G \to G^{1} = (G^{*}F)/T_{\Pi}(G^{*}F,R) \) the image \( \phi^{1}(g) \) of every element \( g \in G \) has unique \( p \)-th root in \( G^{1} \), for every \( p \in \Pi \).

Next steps: The above construction is iterated leading to new groups \( G^{i+1} = (G^{i})^{1} \) and homomorphisms \( \phi^{i+1}: G^{i} \to G^{i+1} \) such that the image \( \phi^{i+1}(g) \) of every element \( g \in G^{i} \) has unique \( p \)-th root in \( G^{i+1} \), for every \( p \in \Pi \). Finally, let \( G^{\Pi} = \lim G^{i} \), with obvious homomorphism \( \phi^{\Pi}: G \to G^{\Pi} \). This is the \( \Pi \)-perfection of \( G \).

The construction of the \( \Pi \)-perfection yields a right-exact, but generally not left-exact functor.

It is perhaps not superfluous to stress that the construction of the \( W \)-perfection is performed in the utmost generality; it consists of a succession of steps, all of the same kind so that it is possible to prove results about the perfection by investigating what happens in the typical step of the construction.
Fixing the attention on nilpotent groups and $\Pi$-localization, the theory has been developed (see for example Hilton, Mislin and Roitberg, Warfield) in a different way. If $N \in N_c$ (the class of nilpotent groups of class $c \geq 1$) then $N$ is a central extension $1 \to A \to N \to N' \to 1$, where $A$ is an abelian group and $N' \in N_{c-1}$. By induction on $c$, the $\Pi$-localizations $A_{\Pi}$, $N'_{\Pi}$ are known and $N_{\Pi}$ is obtained by taking the central extension defined by $A_{\Pi}$, $N'_{\Pi}$ and the cocycle which served to define $N$, so that the following diagram is commutative

$$
\begin{array}{c}
1 \to A \to N \to N' \to 1 \\
\downarrow & \downarrow & \downarrow \\
1 \to A_{\Pi} \to N \to N'_{\Pi} \to 1
\end{array}
$$

In my own construction, it follows from a theorem of Černikov that if $N \in N_c$ if $N'_{\Pi}$ is the $\Pi$-perfection of $N$, then in fact $N'_{\Pi} \in N_c$, and so $N_{\Pi}$ coincides with the above localization. The whole theory developed for example by Hilton may be easily inferred.

Another aspect of the proposed analogy between group theory and commutative ring theory concerns the local-global questions. For example, the integrally closed commutative domains are those which may be recovered from the valuation rings containing it. Similarly, it is natural to ask about the recovery of a group from localizations. In this respect, a natural concept is the following.

Let $(\Pi_i)_{i \in I}$ be a family of sets of prime numbers. The group $G$ is separable (with respect to this family) when $\bigcap_{i \in I} \ker(\phi^{\Pi_i}) = \{1\}$, where $\phi^{\Pi_i}: G \to G^{\Pi_i}$ is the $\Pi$-perfection; in other words, the canonical homomorphism $G \to \prod_{i \in I} G^{\Pi_i}$ is injective. The study of separable groups has been initiated in [8], but should be continued.

Lastly I would like to mention that the above ideas of localization may be applied in the category of profinite groups in which it becomes a powerful method of investigation (see [3]).

It is hoped that the rich developments in commutative ring theory, which were inspired by the geometric interpretation of rings, may induce by analogy a more systematic treatment of group theory, leading to interesting new problems and a better understanding of groups.
Bibliography


Department of Mathematics and Statistics
Queen's University
Kingston, Ontario, Canada
K7L 3N6

Received November 10, 1984.
ON THE CONGRUENCES OF VORONOI AND KUMMER
FOR THE BERNOULLI NUMBERS

T. AGOH

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

Abstract: The Bernoulli numbers $B_m (m \geq 2)$ are defined by the formal power series expansion $x/(e^x - 1) = 1 - (1/2)x + \sum_{m=2}^{\infty} B_m x^m/m!$. These numbers appear in many areas of mathematics, and have various fascinating properties. The purpose of this paper is to study the analog of Voronoi’s congruence and to discuss Kummer’s congruences under more general situation.

1. Introduction. Let $B_m$ be the $m$-th Bernoulli number in the even suffix notation, $\mathbb{Z}$ the ring of integers, and $\mathbb{Z}_n$ the ring of all rational numbers which are $n$-integral.

It is easy to show that if $m \geq 3$ is odd, then $B_m = 0$. And also, $B_m > 0$ if and only if $m/2$ is odd.

In the theory of Bernoulli numbers, we have the following important theorems, which tell us various arithmetical properties of these numbers (see e.g. [3, 4]):

Theorem A (von Staudt - Clausen). If $m \geq 2$ is even, then

$$B_m + \sum_{p-1|m}^{1} - \frac{1}{p} \in \mathbb{Z}.$$  

Letting $B_m = N_m/D_m$, $N_m, D_m (> 0) \in \mathbb{Z}$, $(N_m, D_m) = 1$, it follows that

Theorem B (Voronoi). Let $m \geq 2$ be even and $n \geq 1$. If $a$ is a positive integer with $(a, n) = 1$, then
\[(a^m - 1) N_m \equiv m^{a^m-1} D_m \sum_{j=1}^{n-1} j^{m-1}[ja/n] \pmod{n}, \quad (1)\]

where \([ja/n]\) means the greatest integer in \(ja/n\).

**Theorem C (Kummer).** Let \(p\) be an odd prime, \(e \geq 1\), \(m\) an even integer with \(m \geq e + 1\), and \(\beta_m = B_m / m\). If \(a\) is a positive integer with \((a, p) = 1\), then

\[\sum_{k=0}^{e} (-1)^k \binom{e}{k} (a^{m+k(p-1)} - 1) \beta_{m+k(p-1)} \equiv 0 \pmod{p^e}. \quad (2)\]

In particular, if \(p \nmid m\), then

\[\sum_{k=0}^{e} (-1)^k \binom{e}{k} \beta_{m+k(p-1)} \equiv 0 \pmod{p^e}. \quad (3)\]

**Theorem D (Adams - Sylvester).** Let \(m \geq 2\) be even and \(m = p^t m'\) (where \(p\) is an odd prime, \(t \geq 1\) and \((m', p) = 1\)). If \(p \nmid D_m\), then \(p^t \mid N_m\).

In the next section, we shall study the analog of the congruence (1), and extend the congruences (2) and (3) to more general situation.

2. **Some Results.** For a given prime \(p\), we define \(\text{ord}_p (r)\) to be the exponent of the highest power of \(p\) that divides the integer \(r\). Suppose that

\[n = \prod_{i=1}^{s} p_i^{e_i} (e_i \geq 1; p_i \neq p_j \text{ if } i \neq j)\]

is the decomposition of \(n > 0\) into the prime divisors. And, let

\[S(n) = \{p_1, p_2, \ldots, p_s\} \text{ and } u(m, n) = \prod_{i=1}^{s} p_i^{e_i+g_i},\]

where \(m \geq 2\) is even, \(f_i = \text{ord}_{p_i} (m)\) and \(g_i = \text{ord}_{p_i} (D_j) \quad (i = 1, 2, \ldots, s)\).

**Theorem 1.** Let \(m \geq 2\) be even, \(n \geq 1\), \(w\) an arbitrary positive integer with \(nu(m, n) \mid w\), and \(\beta_m = B_m / m\). If \(a\) is a positive integer with \((a, w) = 1\), then

\[\prod_{p \in S(n)} (1 - p^{m-1}) (a^m - 1) \beta_m \equiv a^{m-1} \sum_{j=1}^{w} j^{m-1} [ja/w] \pmod{n}. \quad (4)\]
Proof. Theorem A shows that $B_m \in \mathbb{Z}_p$ if and only if $p-1 \nmid m$. Consider the congruence (1), where $n$ is replaced by $w$. That is, if $(a, w) = (a, n) = 1$, then

$$
(a^m - 1) N_m \equiv m a^{m-1} D_m \sum_{j=1}^{w-1} j^{m-1} [ja/w] \pmod{w}.
$$

(5)

If $p^t \mid m$ and $p-1 \nmid m$, then $p^t \nmid D_m$, hence $p^t \mid N_m$ by Theorem D. Also, if $p^t \mid m$ and $p-1 \mid m$, then $p^{t+1} \mid a^m - 1$. In this case, we have $\text{ord}_p (D_m) = 1$. Therefore, we may divide the congruence (5) by $u(m, n)$. Since $(mD_m / u(m, n), n) = 1$, the following congruence can be deduced:

$$
(a^m - 1) \theta_m \equiv a^{m-1} \sum_{j=1}^{w-1} j^{m-1} [ja/w] \pmod{n}.
$$

(6)

Let $P(E)$ be the power set of $E = \{1, 2, \ldots, s\}$. For $I \in P(E)$, let

$$
\omega_I = w / \prod_{i \in I} p_i \quad \text{and} \quad T_I = (-1)^{\eta(I)-1} \prod_{i \in I} \{ \sum_{r=1}^{p_i-1} r^{m-1} [ra/w_I] \},
$$

where $\eta(I)$ is the number of elements of $I$. Then, the sum in the right hand side of (6) may be written as follows: If $P_k = \{ I \in P(E) \mid \eta(I) = k \}$, then

$$
\sum_{j=1}^{w-1} j^{m-1} [ja/w] = \sum_{1 \leq j \leq w-1} \sum_{(j,n)=1} j^{m-1} [ja/w] + \sum_{1 \leq j \leq w-1} \sum_{(j,n) \neq 1} j^{m-1} [ja/w] \equiv \sum_{1 \leq j \leq w-1} \sum_{(j,n)=1} j^{m-1} [ja/w] + \sum_{k=1}^{s} \sum_{I \in P_k} T_I.
$$

(7)

Let us now consider the congruence (6), where $n$ is replaced by $n_I = n / \prod_{i \in I} p_i$:

$$(a^m - 1) \theta_m \equiv a^{m-1} \sum_{j=1}^{w-1} j^{m-1} [ja/w_I] \pmod{n_I}.\n$$

(8)

Multiplying this by $(-1)^{\eta(I)-1} \prod_{i \in I} p_i^{m-1}$, we have

$$
(-1)^{\eta(I)-1} \prod_{i \in I} p_i^{m-1} (a^m - 1) \theta_m \equiv a^{m-1} T_I \pmod{n}.
$$

(8)
From (6), (7) and (8) we arrive at the following congruence:

\[
(1 + \sum_{k=1}^{S} (-1)^k \prod_{i \in P_k} p_i^{m-1})(a^m - 1) \beta_m
\]

\[
= \prod_{p \in S(n)} (1 - p^{m-1})(a^m - 1) \beta_m
\]

\[
= a^{m-1} \sum_{1 \leq j \leq \omega-1} j^{m-1} \left[ j/a \right] \pmod{n},
\]

which is the congruence indicated in the statement.

Next, we shall show the following result which is a generalization of Theorem C:

**Theorem 2.** Let \( n \geq 3, e \geq 1 \) and \( m, a, S(n), \beta_m \) be as in Theorem 1. And, let \( \phi(n) \) denote the Euler \( \phi \)-function of \( n \). Then,

\[
\sum_{k=0}^{e} (-1)^k \binom{e}{k} \prod_{p \in S(n)} (1 - p^{m-1+k\phi(n)})(a^{m+k\phi(n)} - 1) \beta_{m+k\phi(n)} \equiv 0 \pmod{n^e}.
\]

(9)

In particular, if \( p-1 \mid m \) for all \( p \in S(n) \), then

\[
\sum_{k=0}^{e} (-1)^k \binom{e}{k} \prod_{p \in S(n)} (1 - p^{m-1+k\phi(n)}) \beta_{m+k\phi(n)} \equiv 0 \pmod{n^e}.
\]

(10)

**Proof.** For brevity, we set

\[
A_m = \prod_{p \in S(n)} (1 - p^{m-1})(a^m - 1) \beta_m.
\]

Since \( n \geq 3, m + k\phi(n) \) \((k = 1, 2, \ldots, e)\) are always even. And also, since \( p-1 \mid \phi(n) \) for all \( p \in S(n) \), it follows that \( p-1 \mid m \) if and only if \( p-1 \mid m + k\phi(n) \). Hence, \( g_i = \text{ord}_{p_i} (D_m) = \text{ord}_{p_i} (D_{m+k\phi(n)}) \) for \( i = 1, 2, \ldots, s \). Now, let \( w' = n^e u'(m, n, e) \), where

\[
u'(m, n, e) = \prod_{i=1}^{S} \frac{f_i! \beta_{p_i}^*}{p_i^{\text{ord}_{p_i} (m + k\phi(n))}} \text{ and } \max_{0 \leq k \leq e} \frac{f_i!}{p_i^{\text{ord}_{p_i} (m + k\phi(n))}}.
\]

(T. Agoh)
Consider the congruence (4), where \(m, n\) and \(w\) are replaced by \(m + k \phi(n), n^e\) and \(w'\), respectively:

\[
A_{m+k\phi(n)} \equiv \sum_{\substack{1 \leq j \leq w'-1 \atop (j, n) = 1}} (a_j)^{m-1+k\phi(n)} \cdot [ja/w'] \pmod{n^e},
\]

(11)

which is valid for all \(k = 0, 1, \ldots, e\). From (11) it follows that

\[
\sum_{k=0}^{e} (-1)^k \binom{e}{k} A_{m+k\phi(n)} \equiv \sum_{\substack{1 \leq j \leq w'-1 \atop (j, n) = 1}} (a_j)^{m-1} \cdot [1 - (a_j)^{\phi(n)}] \cdot e \cdot [ja/w']
\]

\(\pmod{n^e} \).

In this congruence, \((a_j, n) = 1\), so that \(\{(a_j)^{\phi(n)} - 1\}^e \equiv 0 \pmod{n^e}\). Consequently, we obtain

\[
\sum_{k=0}^{e} (-1)^k \binom{e}{k} A_{m+k\phi(n)} \equiv 0 \pmod{n^e},
\]

which completes the proof of (9).

In particular, if \(p-1 \nmid m\) for all \(p \in S(n)\), then we can choose \(\alpha > 0\) such that \((\alpha, n) = 1, \alpha^{\phi(n)} \equiv 1 \pmod{n^e}\) and \((\alpha^m - 1, n) = (\alpha^{m+k\phi(n)} - 1, n) = 1\). Thus, by dividing (9) by \(\alpha^m - 1\), we can deduce the congruence (10).

If \(m-1 \geq e\), then the congruences (2) and (3) can be easily deduced from (9) and (10) respectively, by taking \(n = p \not\equiv 2\). Also, we note that Theorem 2 for the case \(n = p^r \not\equiv 1\) has been proved by Frobenius [1].

In this paper, we did not make use of the properties of p-adic L-functions (see e.g. Iwasawa [2]). We cannot say exactly now, but it seems that perhaps the congruences (1) and (4) are intimately connected with the construction of p-adic L-functions.

REFERENCES


Department of Mathematics
Science University of Tokyo
Noda, Chiba 278, Japan

Received July 13, 1984.
Abstract: We give a counter-example to an assertion of T. Husain and S.A. Warsi ([4], Theorem 2) on the expression of the spectrum (of an element) in A-convex algebras. The same counter-example also shows that in such algebras the radical (of Jacobson) need not be closed.

I. Introduction. T. Husain et S.A. Warsi affirment ([4], Theorem 2) que si E est une a.l. A-convexe commutative complète, alors elle vérifie la propriété

\[(P): \forall x \in E, \text{Sp}(x) = \{\chi(x) \mid \chi \in M\},\]

où Sp(x) est le spectre de x et M l'espace des caractères continus (non nuls) de E. Nous exhibons une classe d'a.l.u. A-convexes (et non seulement A-convexes) ne vérifiant pas (P).

La propriété (P) implique que le radical de E, Rad E, est fermé. Comme elle n'est pas vérifiée, on peut se demander si, quand même, le radical est fermé. Le même contre-exemple montre que la réponse à cette question est aussi négative.

II. Définitions. Soient \((E,\tau)\) un espace localement convexe et \((p_{\lambda})_{\lambda}\) une famille de semi-normes définissant sa topologie \(\tau\). Si E est munie d'une structure d'algèbre telle que la multiplication soit séparément continue, on dit que \((E,\tau)\) est une algèbre
localement convexe (a.l.c.).

Une a.l.c. est dite A-convexe (a.l. A-convexe) si, pour tout \( \lambda \) et tout \( x \), il existe \( M(\lambda, x) > 0 \) et \( N(\lambda, x) > 0 \) tels que:

\[
p_{\lambda}(x \cdot y) \leq M(\lambda, x) \cdot p_{\lambda}(y) \quad \text{et} \quad p_{\lambda}(y \cdot x) \leq N(\lambda, x) \cdot p_{\lambda}(y), \quad \forall y.
\]

Elle est dite uniformément A-convexe (a.l.u. A-convexe) si pour tout \( x \), il existe \( M(x) > 0 \) et \( N(x) > 0 \) tels que:

\[
\forall \lambda: p_{\lambda}(x \cdot y) \leq M(x) \cdot p_{\lambda}(y) \quad \text{et} \quad p_{\lambda}(y \cdot x) \leq N(x) \cdot p_{\lambda}(y), \quad \forall y.
\]

Elle est dite localement multiplicativement convexe (a.l.m.c.) si

\[
p_{\lambda}(x \cdot y) \leq p_{\lambda}(x) \cdot p_{\lambda}(y), \quad \text{pour tout} \ \lambda \ \text{et tous} \ x, y.
\]

Toute a.l.m.c. et toute a.l.u. A-convexe est une a.l.A-convexe mais une a.l.m.c. n'est pas toujours une a.l.u. A-convexe. De même une a.l.u. A-convexe n'est pas toujours une a.l.m.c. ([2]).

Nous ne considérons que des algèbres complexes et unitaires. Si \((E, \tau)\) est une a.l.c. on désigne par \( \mathcal{M}^* \) l'ensemble des caractères (algébriques) non nuls de \( E \).

Pour les exemples se reporter à ([1], [2], [3], [8]).

III. Sur une expression du spectre. Nous avons, dans [7] (Remarque 4), donné un exemple d'a.l.u. A-convexe unitaire commutative complète pour laquelle les caractères ne sont pas tous continues i.e. \( M \neq \mathcal{M}^* \).

Nous allons maintenant décrire une situation où non seulement \( M \neq \mathcal{M}^* \) mais \( \mathcal{M} = \emptyset \).

**Contre-exemple III.1:** Soit \( E \) une algèbre de Banach commutative, intègre radicale et à unité approchée bornée. Considérons l'algèbre \( \mathcal{M}(E) \), des multiplicateurs \( T \) de \( E \), munie de la topologie stricte \( \beta \) définie par la famille de semi-normes \( (p_x) \), \( x \in E \), où \( p_x(T) = \|T(x)\| \). C'est une a.l.u. A-convexe commutative, uni-
taire et complète (c.f. [5] ou [9]).

On a $M^* = 0$, et l'on sait que tout $x \in M^*$ est $\beta$-borné ([7] ou [8]). Par ailleurs $E$ est $\beta$-dense dans $M(E)$ ([9], theorem 2.4, p. 1134); et comme $E$ n'admet aucun caractère (non nul), $M(E)$ n'admet aucun caractère (non nul) $\beta$-continu. Ainsi $M(M(E)) = 0$. Et donc $M(E)$ ne vérifie pas (P).

IV. Radical de Jacobson. Comme, dans le cas des a.l.m.c. ([10]), on montre la proposition suivante:

Proposition IV.1. Soit $E$ une a.l. A-convexe commutative, unitaire complète et vérifiant (P). Alors $\text{Rad} E = \cap \{\ker x | x \in M\}$; et donc $\text{Rad} E$ est fermé.

Dans le contre-exemple III.1, $\text{Rad} M(E)$ n'est pas égale à $\cap \{\ker x | x \in M\}$. Nous allons voir qu'il n'est pas fermé.

Contre-exemple IV.2. Reprenons l'algèbre $M(E)$ du contre-exemple III.1. On sait que $M(E)$ peut être munie d'une norme d'algèbre de Banach ([5] ou [9]), donc

$$\text{Rad}(M(E)) = \{T \in M(E) | \rho(T) = 0\},$$

où $\rho(T)$ est le rayon spectral de $T$.

Pour tout $x \in E$, on considère le multiplicateur $T_x$ défini par $T_x(y) = x \cdot y$. L'application $x \rightarrow T_x$, de $E$ dans $M(E)$ est injective et on a $||T_x|| \leq ||x||$. Identifions $x$ avec $T_x$ et posons $||T_x|| = ||x||'$; On a $||x||' \leq ||x||$. Et comme $E$ est radicale on a $E \subseteq \text{Rad}(M(E))$. Mais l'on sait que $E$ est $\beta$-dense dans $M(E)$ ([9], theorem 2.4, p. 1134). Alors $\text{Rad}(M(E))$ n'est pas $\beta$-fermé car
sinon il serait égale à $M(E)$ car $E$ est un espace unitaire.

**Remarque IV.3.** Comme $M(M(E)) = \emptyset$, la topologie d'a.l.m.c. $m(M(E))$ de Cochran ([3]) n'est pas complète.

**Remarque IV.4.** Il serait intéressant de regarder les a.l. A-convexes unitaires commutatives complètes qui vérifient la propriété $(P)$, avec $M$ non vide, ou dont le radical est fermé.

**Remerciements.** L'auteur remercie M. le Pr. Ngô Van Quê pour son invitation, ainsi que MM les Pr. J. I. Nieto, P. Gauthier et A. Giroux pour leur aide, et le D. M. S. de l'Université de Montréal pour son hospitalité.

**REFERENCES.**


Ecole Normale Supérieure Takaddoum
Avenue Oued Akreuch
B. P. 5118, Rabat (MAROC)

Received August 27, 1984.
ORDINARY ARCS ON CONVEX BODIES

T. Bisztriczky and P. Scherk, F.R.S.C.

The classical four-vertex theorem of plane differential geometry has been extended to various closed and simple skew curves. Such a four-vertex theorem has been proved in particular within the framework of the geometry of orders and thus purely synthetically in [1]. The curves were assumed to satisfy certain smoothness conditions and to be convex; that is, they lie on the boundary of their convex hull and they meet no line in more than two points. The first convexity condition implies that their tangents do not meet the interior of the convex hull.

So far, no \((n + 1)\)-vertex theorem is known for curves in \(n\)-space. The smoothness conditions are readily generalized but it is not clear what convexity assumptions are required. In this note, we compare two such assumptions dealing not with closed curves but only with certain subarcs. The results depend on the parity of the space.

1. Let \(I = (r, s, \ldots)\) be an open interval in \(R\), and let \(R_n\) denote a real affine \(n\)-space; \(n \geq 2\). An arc in \(R_n\) is a continuous map \(\Gamma: I \to R_n\). We identify \(I\) with \(\Gamma(I)\) and note that the topology of \(I\) defines open neighbourhoods on \(\Gamma\).

The arc \(\Gamma\) shall be differentiable in the following sense. For every \(s \in I\), let \(\Gamma_{-1}(s) = \phi\) and \(\Gamma_0(s) = \Gamma(s)\). If \(\Gamma_{k-1}(s)\) is already defined and its existence postulated then we require that for \(t \in I \setminus \{s\}\) sufficiently close to \(s\), the flat \(\langle \Gamma_{k-1}(s), \Gamma(t) \rangle\) spanned by \(\Gamma_{k-1}(s)\) and \(\Gamma(t)\) has dimension \(k\) and it converges as \(t\) tends to \(s\). Its limit is the osculating \(k\)-flat \(\Gamma_k(s)\); \(k = 1, 2, \ldots, n\).
Let $t \in I$. If $U(t)$ is a neighbourhood of $t$ in $I$, we write $U'(t) = U(t) \setminus \{t\}$, $U^-(t) = \{s \in U(t) : s < t\}$ and $U^+(t) = \{s \in U(t) : t < s\}$. Obviously, there are $(n-1)$-flats meeting $\Gamma(U(t))$ in $n$ or more points. If no $(n-1)$-flat meets $\Gamma(U(t))$ in more than $n$ points, we say that $\Gamma(U(t))$ is of order $n$

$\text{(ord } \Gamma(U(t)) = n)$. and $\Gamma(t)$ is ordinary.

An $(n-1)$-flat $R_{n-1}$ supports [cuts] $\Gamma$ at $t$ if there is a $U(t)$ such that $\Gamma(U^-(t))$ and $\Gamma(U^+(t))$ lie on one side [on opposite sides] of $R_{n-1}$. If $\Gamma(t)$ is ordinary and

$$R_{n-1} \cap \Gamma_{k+1}(t) = \Gamma_k(t),$$

then $R_{n-1}$ supports [cuts] $\Gamma$ at $t$ if $k$ is odd [even]; $0 \leq k \leq n-1$; cf. [3], p. 168.

From now on, we assume that $\Gamma$ is elementary. This means, to every $t \in I$ there is a $U(t)$ such that

$$\text{ord } \Gamma(U^-(t)) = \text{ord } \Gamma(U^+(t)) = n.$$

Then $\Gamma_k(t), 0 \leq k \leq n-1$, depends continuously on $t$. Furthermore,

1. $\Gamma$ is dually differentiable; that is,

$$\Gamma_k(s) = \lim_{s \to t} \Gamma_{k+1}(s) \cap R_{n-1}(t)$$

for $s \in I$ and $-1 \leq k \leq n-1$; cf. [2], p. 116. This readily implies

2. given a point $p \in R_n$ and $t \in I$, there is a $U(t)$ such that

$$p \notin \Gamma_{n-1}(s) \text{ for all } s \in U'(t).$$

2. Let $C$ be a convex body in $R_n$ and let $\Gamma(I) \subset C$. We introduce the following statements for $0 \leq k \leq n-1$:

A($k$): $\Gamma_{n-1}(r) \cap \Gamma_k(s) \cap \text{int } C = \emptyset$ for all $r \neq s$ in $I$.

B($k$): $\Gamma_k(s) \cap \text{int } C = \emptyset$ for all $s \in I$. 


(Thus $B(k)$ implies that $\Gamma(I)$ lies on the boundary of $C$).

1. Remarks. (i) By (1), $B(k)$ is equivalent to

$$\Gamma_{n-1}(t) \cap \Gamma_{k+1}(s) \cap \text{int } C = \emptyset$$

for every $s \in I$ and all $t$ in some $U'(s)$; $0 \leq k \leq n - 1$.

(ii) Obviously, $B(k)$ implies $A(k)$ for $0 \leq k \leq n - 1$.

(iii) By (1), $A(k)$ implies $B(k - 1)$ for $1 \leq k \leq n - 1$.

(iv) If $k$ is odd, then $B(k - 1)$ implies $B(k)$ for $1 \leq k \leq n - 1$.

In order to prove (iv), we assume first that $\Gamma(s)$ is ordinary. By $B(k - 1)$, there is an $(n - 1)$-flat $R_{n-1}$ through $\Gamma_{k-1}(s)$ supporting $C$ and thus $\Gamma$ at $\Gamma(s)$. Since $k - 1$ is even, $R_{n-1}$ must contain $\Gamma_{k}(s)$. This yields $B(k)$ for the ordinary points $\Gamma(s)$ in $\Gamma$. As $\Gamma_k(s)$ depends continuously on $s$ and $\Gamma$ is elementary, (iv) follows.

2. From now on, we assume that $\Gamma(I) \subset C$ and that $\Gamma$ is an ordinary arc; that is, $\Gamma(t)$ is ordinary for each $t \in I$. Hence for each $t \in I$, there is a $U(t)$ such that

$$\Gamma_{n-1}(t) \cap \Gamma(U'(t)) = \emptyset; \text{ cf. [3], p. 174}$$

Let $C_t^-[C_t^+]$ denote the component of $C\setminus\Gamma_{n-1}(t)$ which contains $\Gamma(U^-(t)) [\Gamma(U^+(t))]$. As $\Gamma_{n-1}(t)$ cuts $\Gamma$ at $t$, we have

$$C_t^- \cap C_t^+ = \emptyset \text{ and } C\setminus\Gamma_{n-1}(t) = C_t^- \cup C_t^+.$$

For every $p \in R_n$, we put

$$I_p^o = \{s \in I | p \in \Gamma_{n-1}(s)\} \text{ and } I_p^z = \{s \in I | I_p^o \cap I_p^z\} \in C_g^z.$$

From (2), we readily obtain
2. Lemma. (i) \( I^s_p \) is closed in \( I \),
(ii) \( I^-_p \) and \( I^+_p \) are open in \( I \),
and (iii) if \( p \notin \Gamma_{n-1}(t) \) for \( t \in (r,s) \subseteq I \), then either \((r,s) \subseteq I^-_p\) or \((r,s) \subseteq I^+_p\).

Our goal is the following

Theorem. Let \( n \) be odd. Then \( B(n-2) \) implies \( A(n-1) \).

We first show that this theorem follows from

3. Lemma. Let \( n \) be odd. Let \( t \in I \) and \( c \in \Gamma_{n-1}(t) \cap \text{int} \ C \). Then
\( U(t) \subseteq I^+_c \) and \( I^+(t) \subseteq I^-_c \) for some \( U(t) \).

Suppose there are \( r \) and \( s \) in \( I \), \( r < s \), and a point
\( c \in \Gamma_{n-1}(r) \cap \Gamma_{n-1}(s) \cap \text{int} \ C \). By (2), we may assume that \( c \notin \Gamma_{n-1}(t) \) for \( t \in (r,s) \). Thus either \((r,s) \subseteq I^-_c\) or \((r,s) \subseteq I^+_c\) by Lemma 2(iii). But this
contradicts Lemma 3.

\( \Delta \). We prove Lemma 3. Since \( \Gamma \) is ordinary, there is a \( U(t) \) such that
(a) neither \( \Gamma(t) \) nor \( c \) lie in \( \Gamma_{n-1}(s) \) for \( s \in U'(t) \)
and
(b) \( \text{ord} \ \Gamma(U(t)) = n \).
Let $\Gamma^c$ denote the projection of $\Gamma$ from $c$ onto an $(n-1)$-flat $R_{n-1}$ not through $c$. By [2], p. 113, $\Gamma^c$ is an elementary arc in $R_{n-1}$ with the osculating flats

$$\Gamma^c_k(s) = \begin{cases} \langle \Gamma_k(s), c \rangle \cap R_{n-1} & \text{if } c \not\in \Gamma_k(s) \\ \Gamma_k(s) \cap R_{n-1} & \text{if } c \in \Gamma_k(s) \end{cases}; \ s \in I, -1 \leq k \leq n-1.$$

Since $\Gamma^c$ is elementary, we may assume

(c) $\text{ord } \Gamma^c(\mathcal{U}^-) = \text{ord } \Gamma^c(\mathcal{U}^+) = n-1$.

By symmetry, it suffices to deal with $\mathcal{U}^-$. Let $s \in \mathcal{U}^- = (r,t)$.

Then (b) implies $\Gamma_{n-1}(s) \cap \Gamma(r,t) = \{\Gamma(s)\}$ and therefore by (a),

$$\Gamma_{n-1}(s) \cap \Gamma(r,t) = \{\Gamma(s)\},$$

where

$$\Gamma(r,s) \subset C^0_{\mathcal{s}}, \Gamma(s,t) \subset C^+_{\mathcal{s}} \text{ and } s \in \mathcal{I}^+_{\Gamma(t)}.$$

Thus $(r,t) \subset \mathcal{I}^+_{\Gamma(t)}$ and we may assume that $c \not\in \Gamma(t)$.

By (a), $A(s) = \langle c, \Gamma_{n-2}(s) \rangle$ is an $(n-1)$-flat distinct from

$\Gamma_{n-1}(s)$ and thus $\Gamma^c_{n-2}(s) = A(s) \cap R_{n-1}$. We note that $A(s)$ supports $\Gamma$ at $s$.

By (c), $\Gamma^c_{n-2}(s) \cap \Gamma^c(r,t) = \{\Gamma^c(s)\}$. Hence

$$A(s) \cap \Gamma(r,t) = \{\Gamma(s)\}.$$

Let $\mathcal{C}_s$ denote the component of $C \setminus A(s)$ containing $\Gamma(r,t) \setminus \{\Gamma(s)\}$. Thus

(d) $\Gamma(r,s) \subset C^0_{\mathcal{s}} \cap \mathcal{C}_s$ and $\Gamma(s,t) \subset C^+_{\mathcal{s}} \cap \mathcal{C}_s$.

By $B(n-2)$, there is a supporting $(n-1)$-flat $\pi(s)$ of $C$ through $\Gamma_{n-2}(s)$. Since $c \in \text{int } C$ and $\Gamma_{n-1}(s)$ cuts $\Gamma$ at $s$, we obtain that $\Gamma_{n-1}(s)$, $A(s)$ and $\pi(s)$ are mutually distinct $(n-1)$-flats through $\Gamma_{n-2}(s)$.

Let $\Gamma^o_{n-1}(s) [A^o(s)]$ denote the intersection of $\Gamma_{n-1}(s) [A(s)]$ with the closed half-space bounded by $\pi(s)$ and containing $C$. By (d),

(e) $C^o_s \cap \Gamma(r,t) \setminus \{\Gamma(s)\}$ and thus $\Gamma^o_{n-1}(s)$ lie in the same closed quadrant bounded by $A(s)$ and $\pi(s)$

and

(f) $C^+_s$ lies in the closed quadrant bounded by $\pi(s)$

and $\Gamma^o_{n-1}(s)$ containing $\Gamma(s,t)$. 
Obviously, $\Gamma_{n-1}(a)$ and $a^*(a)$ depend continuously on $s$. Since $c \in \Gamma_{n-1}(t)$, both $a_{n-1}(a)$ and $a^*(a)$ converge to $\Gamma_{n-1}(t)$ as $s$ tends to $t$. Let $s$ be sufficiently close to $t$. Then $\Gamma(r,s)$ must lie outside the quadrant bounded by $\Gamma_{n-1}(s)$ and $a^*(a)$. As $\Gamma_{n-1}(s)$ cuts $\Gamma$ at $s$, $\Gamma(s,t)$ must therefore lie in this quadrant. Hence $a^*(a)$ meets $C^+_g$ (cf. (f)) and in particular, $c \in C^+_g$, $s \in I_c^+$ and $U^-(t) = (r,t) \subset I_c^+$.

4. Remarks. (1) If $k$ is odd then

$$A(k) = B(k - 1) = B(k) = A(k)$$

by I. (iii), (iv) and (ii). Thus in particular, if $n$ is even and $c \subset C$ is elementary then $A(n - 1) = B(n - 1)$

(ii) We note that Lemma 3 is still valid for $c \in \Gamma_{n-1}(t) \cap \phi$. The only use of $c \subset \text{int } C$ is to show that $a(s) \neq \pi(s)$; but since $\Gamma_{n-1}(t) \cap \text{int } C \neq \phi$ for an ordinary $\Gamma(t)$, $a(s) \cap \text{int } C \neq \phi$ and hence $a(s) \neq \pi(s)$ for $s$ in a suitable $U'(t)$. The strengthened Lemma 3 and $B(n - 2)$ now imply

$$A'(n - 1): \Gamma_{n-1}(r) \cap \Gamma_{n-1}(s) \cap C = \phi$$

for all $r \neq s$ in $I$.

In comparison to the preceding, we then have if $n$ is odd and $C \subset C$ is ordinary then

$$A(n - 1) = B(n - 2) = A'(n - 1) = A(n - 1).$$

REFERENCES


University of Calgary
Calgary, Alberta
Canada T2N 1N4

University of Toronto, Toronto, Ontario
Canada M5S 1A1

Received October 18, 1984.
A REMARK ABOUT VANDIVER'S CONJECTURE
I. Kersten and J. Michaliček

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

Let $K$ denote the field

$$K = \mathbb{Q}(\zeta + \zeta^{-1})$$

where $\zeta = \zeta_p$ is a primitive $p$-th root of unity and $p > 2$ is a prime.

Vandiver's conjecture states that $p$ does not divide the class number $h(K)$ of $K$. By class field theory this conjecture is equivalent to the following statement: There is no unramified Galois field extension of degree $p$ over $K$.

Let $R_F$ be the ring of integers of any number field $F$.

Given two number fields $F \subset L$ where $L$ is a Galois extension over $F$ with group $G$ then $L$ is unramified over $F$ if and only if the ring $R_L$ is a Galois extension with group $G$ over the ring $R_F$ (see i.e. [2], Chap. III, Cor. 4.5).

The aim of this paper is the proof of the following Proposition 1.

**Proposition 1.** Let $G = (\sigma_i)_{i=0,1,\ldots,p-1}$ be a group of order $p$ and let $L$ be an unramified Galois field extension with group $G$ over $K$. Then the ring $R_L[p^{-1}]$ is a Galois extension with group $G$ over $R_K[p^{-1}]$ without normal basis. In particular, $R_L$ has no normal basis over $R_K$.

By Proposition 1 Vandiver's conjecture is true if each
unramified Galois field extension $L$ over $K$ of degree $p$ has a normal basis which is also a normal basis of $R_L[p^{-1}]$ over $R_K[p^{-1}]$.

Proof of Proposition 1: Suppose that $R_L[p^{-1}]$ has a normal basis $(X_i = \sigma^i(X_0) | i = 0, 1, \ldots, p-1)$ over $R_K[p^{-1}]$. We consider in the group ring $R_L[p^{-1}][G]$ the element

$$X = \sum_{i=0}^{p-1} X_i \sigma^{-i}.$$ 

By Satz 1 of [1] we may assume that $X$ is a unit in $R_L[p^{-1}][G]$ with inverse

$$(1) \quad X^{-1} = \sum_{i=0}^{p-1} X_i \sigma^i.$$ 

We define for $k = 0, 1, \ldots, p-1$ the $L$-algebra homomorphism

$$x_k : L[G] \rightarrow L(\zeta) \text{ via } x_k(\sigma) = \zeta^k.$$ 

Let $\overline{x}$ denote the conjugate complex number of $x \in L(\zeta)$. Since $L$ is totally real and $X_i \in L$ it follows that $\overline{x_k(x)} = \sum_{i=0}^{p-1} \overline{X_i} \overline{\zeta^{-i}} = \sum_{i=0}^{p-1} X_i \zeta^{ik} = x_k(x)^{-1}$ by (1).

Thus $\hat{x}_k := x_k(X)$ is a unit in $R_L(\zeta)[p^{-1}]$ and

$$(2) \quad \hat{x}_k \hat{x}_k = 1 \text{ for all } k = 0, 1, \ldots, p-1.$$ 

We now consider for $k = 0, 1, \ldots, p-1$ the fraction ideal

$$\hat{x}_k R_L(\zeta) = \prod_{\gamma \in \mathbb{Z}} \mathcal{F}_{\gamma}^{\alpha(\gamma)}, \text{ where } \alpha(\gamma) \in \mathbb{Z} \text{ and }$$
\( \alpha(\mathfrak{p}) = 0 \) for almost all prime ideals \( \mathfrak{p} \) in \( R_L(\zeta) \). If \( \alpha(\mathfrak{p}) = 0 \) for all \( \mathfrak{p} \) then \( \hat{X}_k \) is a unit in \( R_L(\zeta) \). If \( \alpha(\mathfrak{p}) \neq 0 \) for some \( \mathfrak{p} \) then all prime ideals \( \mathfrak{p}_i \) in \( R_L(\zeta) \), which occur in the unique prime ideal decomposition

\[
(3) \quad \hat{X}_k R_L(\zeta) = \prod_{i \in I} \mathfrak{p}_i^{\alpha_i}, \quad I \text{ finite set}, \quad \alpha_i \neq 0 \forall i \in I,
\]

where \( \mathfrak{p}_i \neq \mathfrak{p}_j \) for \( i \neq j \), lie above \( p \), since \( \hat{X}_k \) is a unit in \( R_L(\zeta)[p^{-1}] \). We now replace \( X \) by \( Y = X^2 \). The equation (2) implies

\[
\hat{Y}_k := X_k(Y) = \frac{\hat{X}_k}{\hat{X}_k},
\]

therefore (3) implies

\[
\hat{Y}_k R_L(\zeta) = \frac{\prod_{i} \mathfrak{p}_i^{\alpha_i}}{\prod_{j} \mathfrak{p}_j^{\alpha_i}}.
\]

Since there is only one prime ideal above \( p \) in \( R_K(\zeta) \) we have \( \mathfrak{p} = \mathfrak{p}_0 \) for all prime ideals \( \mathfrak{p} | p \) in \( R_L(\zeta) \) and so \( \hat{Y}_k R_L(\zeta) = R_L(\zeta) \). We have proved that \( \hat{Y}_k \) is a unit in \( R_L(\zeta) \) of absolute value 1 for all \( k = 0,1,\ldots,p-1 \). Thus \( \hat{Y}_k \) is a root of unity for all \( k \) \[3\], Chap. 9B.

We now prove that

\[
(4) \quad L(\zeta) = K(\zeta)(\sqrt[p]{\zeta}).
\]
If there is $k \in \{0, 1, \ldots, p-1\}$ such that $L(\zeta) = K(\zeta)(\hat{Y}_k)$ then

$\hat{Y}_k^p = \zeta^j$ for some $j \in \{1, \ldots, p-1\}$ since $X^p \in K[G]$ and so

$\hat{Y}_k^p \in K(\zeta)$. This shows

$\hat{Y}_k \in K(\zeta)(\sqrt[p]{\zeta})$ for all $k = 0, 1, \ldots, p-1$.

If we write $Y = \sum_{i=0}^{p-1} Y_i \sigma^{-i}$ in $L[G]$ we check for $i=0, 1, \ldots, p-1$:

$\sum_{i=0}^{p-1} Y_i \zeta^i k = \sum_{k=0}^{p-1} X_k(Y) \zeta^i k = \sum_{k=0}^{p-1} \left( \sum_{m=0}^{\infty} Y_m \zeta^{-m} k \right) \zeta^i k = p Y_i$, hence

$Y_i \in K(\zeta)(\sqrt[p]{\zeta})$ for all $i = 0, 1, \ldots, p-1$.

Showing that $Y_0, \ldots, Y_{p-1}$ are $K$-linear independent in $L$ will thus prove (4).

If $m = \frac{p+1}{2}$ and $\tau = \sigma^m$ we have

$\sum_{i=0}^{p-1} \tau(Y_i) \sigma^{-i} = (\sigma^m \cdot X)^2 = \sigma \cdot Y = \sum_{i=0}^{p-1} Y_i \sigma^{-i+1} = \sum_{i=0}^{p-1} Y_{i+1} \sigma^{-i}$,

hence $\tau(Y_i) = Y_{i+1}$ for all $i = 0, \ldots, p-1$, where $Y_p = Y_0$.

Let $\sum_{i=0}^{p-1} \alpha_i Y_i = 0$ with $\alpha_i \in K$, then

$0 = \tau \left( \sum_{i=0}^{p-1} \alpha_i Y_i \right) = \sum_{i=0}^{p-1} \alpha_i Y_{i+j} \mod p$ for all $j = 0, \ldots, p-1$.

Writing $\alpha = \sum_{i=0}^{p-1} \alpha_i \sigma^i$ this implies $\alpha \cdot Y = 0$ and hence $\alpha = 0$. 

because $Y$ is a unit in $L[G]$. Thus $a_i = 0$ for all $i$ and $Y_0, \ldots, Y_{p-1}$ are $K$-linear independent in $L$. Let $\eta$ be a primitive $p^2$-th root of unity then (4) implies that $L(\zeta) = Q(\eta)$, but $Q(\eta)$ is totally ramified in $p$. It follows that the prime ideal $q | p$ of $R_K$ is ramified in $R_L$, which is a contradiction.

References


I. Kersten
NWF-I Mathematik
Universitätstr. 31
D-8400 Regensburg
W.-Germany

J. Michaliček
Mathematisches Seminar
Bundesstr. 55
D-2000 Hamburg 13
W.-Germany

Received November 5, 1984.
ORTHOGONAL POLYNOMIALS
AND TRANSMUTATION

Robert Carroll

Presented by F.V. Atkinson, F.R.S.C.

Abstract. It is shown how transmutation methods can be used to construct orthogonal functions relative to a suitable measure of polynomial growth on [0,∞). Gelfand-Levitan (G-L) methods are used in which the symmetric kernel arises from a moment functional via generalized translation.

1. Basic constructions. Suppose given a measure $d\sigma$ on [0,∞) of the form $d\omega = (2/\pi)d\lambda + d\sigma$ for suitable bounded $d\sigma$ and consider "polynomials" (*) $\pi(\lambda,t) = \cos\lambda \tau + \int_0^t c(t,s)\cos\lambda s ds$ (i.e. even entire functions of exponential type $t$). These will correspond to extensions of real Krein functions (continuous analogues of orthogonal polynomials - cf. [1;11;12;14-17]). Define a "moment functional" $L(\cos\lambda t) = \int_0^\infty \cos\lambda t d\omega(\lambda) = g(t) = 1 + g_r(t)$ where $g_r(t) = \int_0^\infty \cos\lambda t d\sigma(\lambda)$ (this will be characterized below in terms of generalized translation). One wants to construct orthogonal "polynomials" (relative to $d\omega$) of the form (*)

$(1.1) \quad f(\lambda,t) = \cos\lambda t + \int_0^t K(t,s)\cos\lambda s ds$

Thus one wants (*) $\int_0^\infty f(\lambda,t)f(\lambda,s)d\omega(\lambda) = \delta(t-s)$. Analogous to the theory of orthogonal polynomials (cf. [13]) let us require

$(1.2) \quad \int_0^\infty \cos\lambda sf(\lambda,t)d\omega(\lambda) = \tilde{g}(t,s) = 0$

for $t > s$. Then write

$(1.3) \quad A(t,s) = \langle \cos\lambda t, \cos\lambda s \rangle_\omega = \delta(t-s) + \Omega(t,s)$
(1.4) \( \Omega(t,s) = \int_0^\infty \cos \lambda t \cos \lambda s d\sigma = \frac{1}{2} [g_p(t+s) + g_p(|t-s|)] \)

One obtains immediately from (1.1)-(1.2) a G-L equation

(1.5) \( \Omega(t,s) + K(t,s) + \int_0^t K(t,\tau)\Omega(\tau,s) d\tau = 0 \)

for \( s < t \) which can be assumed to have a unique solution. Then

Theorem 1. Let \( K \) be the (unique) solution of (1.5) and construct \( f(\lambda,t) \)

as in (1.1). Then the \( f \) satisfy the orthogonality condition (\( \rom{\ast} \)). Conversely
if \( f \) of the form (1.1) are orthogonal then one obtains (1.2) and thence the G-L

equation (1.5).

Theorem 2. If \( \Omega \) is twice differentiable and \( f \) is of the form (1.1) with \( K \)

the unique solution of (1.5) then \( K \) satisfies a Goursat problem

(1.6) \( Q(D_t)K(t,\tau) = D_t^2 K(t,\tau); \quad Q(D_t) = D_t^2 - q; \quad q(t) = 2D_tK(t,t); \quad K(t,0) = 0 \)

while \( f \) satisfies \( Q(D_t)f = -\lambda^2 f; \quad f(\lambda,0) = 1; \quad f'(\lambda,0) = -g_p(0) \).

Remark 3. One can also give a number of approximation results based on

the minimization techniques of [5-8;10] which deal with the approximation of

more general functions \( \pi \) by orthogonal "polynomials" \( f \) relative to various mea­
sures. The G-L equation arises again intrinsically relative to \( d\omega \) as well as as a
certain generalized Bessel inequality relative to \( d\omega = (2/\pi)d\lambda \). We refer to


2. Singular cases. Take now a measure \( d\omega = (1 + \sigma(\lambda))d\nu \) where \( d\nu = c_m^2 \lambda^{2m+1} \)

has prototypical polynomial growth on \([0,\infty)\) and \( \sigma(\lambda) \) is "suitable". We associa­
te with \( d\nu \) the differential operator \( Q_m \) Relative to \( d\nu \) given as the spherical func­tion solutions of \( Pu = -\lambda^2 u (\varphi_\lambda^p(0) = 1; \quad D_t \varphi_\lambda^p(0) = 0); \quad explicitly \( \varphi_\lambda^p(t) = (1/c_m) \)

\( J_m(\lambda t)/(\lambda t)^m \) where \( c_m = 1/2^{m+1} \). The object now is to discover orthogonal
functions \( \varphi^Q_\lambda \) relative to \( \omega \) by showing that in suitable circumstances one can construct a singular differential operator \( Q \) and a transmutation \( B: P \to Q \) so that the spherical functions \( \varphi^Q_\lambda(t) \sim f(\lambda,t) \) can be obtained via \( B \) from \( \varphi^P_\lambda \). We refer to [2;4;9] for general transmutation theory and simply remark here that the idea is to connect \( P \) and \( Q \) via a formula

\[
(2.1) \quad f(\lambda,t) = A(t)\varphi^P_\lambda(t) + \int_0^t K(t,\tau)\varphi^P_\lambda(\tau)d\tau
\]

for suitable \( A \) and \( K \) (so that \( f \sim \varphi^Q_\lambda \)). Here as it turns out one can work typically with operators \( Qu = (\Delta_Q u')'/\Delta_Q + qu = Q_0 u + qu \) where \( \Delta_Q = A_Q A_P \) and \( A(t) = A^Q_\lambda(t) \) in (2.1) (cf. [2;9]). Relative to such \( P \) and \( Q \) one has transmutations \( B \) and \( B = (B^{-1})^* \) with kernels \( \beta(y,x) = \Delta^Q_\lambda(y)\delta(x-y) + K(y,x) \) (cf. (2.1)) and \( \tilde{\beta}(y,x) = \Delta^Q_\lambda(y)\delta(x-y) + \tilde{K}(y,x) \) where \( K(y,x) \) is causal and \( \tilde{K}(y,x) \) is anticausal. They are connected by a G-L equation \( \tilde{\beta}(y,x) = (\beta(y,\xi),A(\xi,x)) \) where \( A(\xi,x) = \delta(x-\xi) + \Omega(\xi,x)\Delta_p(x) \) has the form \( A(\xi,x) = \langle \varphi^P_\lambda(\xi),\varphi^P_\lambda(x) \rangle \Delta_p(x) \) with

\[
(2.2) \quad \Omega(\xi,x) = \int_0^\infty \varphi^P_\lambda(\xi)\varphi^P_\lambda(x)\sigma(\lambda)d\nu = \langle \varphi^P_\lambda(\xi),\varphi^P_\lambda(x)\rangle \sigma(\lambda),\nu
\]

Let us give a canonical expression for \( \Omega \) in terms of the "moment functional"

\[
g(t) = L[\varphi^P_\lambda(t)] = \int_0^\infty \varphi^P_\lambda(t)\sigma(\lambda)d\nu = \delta(t) + \sigma(\lambda)\Delta_p(t) (\varphi^P_\lambda = \Delta_p \varphi^P_\lambda). \quad \text{Thus}
\]

\[
(2.3) \quad \Omega(t,s) = T_s^t \Sigma(s); \quad \Sigma(s) = \int_0^\infty \sigma(\lambda)\varphi^P_\lambda(s)d\nu
\]

Here \( T_s^t \) denotes a certain generalized translation associated with \( P \) (cf. [2;3]) and it is represented by (2.2). The condition (1.2) is analogous here to (\#)

\[
\tilde{\beta}(t,s) = \Delta_p(s)\langle f(\lambda,t),\varphi^P_\lambda(s) \rangle \omega = 0 \quad \text{for } s < t.
\]

**Theorem 4.** Given (2.1) with (\#) and \( A(\xi,x) = \delta(x-\xi) + \Omega(\xi,x)\Delta_p(x) \) determined via the moment functional as above (cf. (2.3)) it follows that \( K \) satisfies a G-L equation for \( s < t \) of the form (\#)

\[
0 = A(t)\Omega(t,s)\Delta_p(s) + K(t,s) + \int_0^t K(t,\tau)\Omega(\tau,s)\Delta_p(s)d\tau.
\]
Remark 5. When \( f(\lambda, y) = \psi^Q(\lambda, y) \) the form of \( \tilde{B} \) in (\( \ast \)) plus the G-L representation \( \tilde{B}(y, x) = \left( \beta(y, x) t \right) \tilde{B}(\xi) \Delta_p(x), \tilde{B}(t) \Delta_p(t) = \sigma(t) + \Sigma(t) \Delta_p(t) \), lead one to deduce the triangularity of \( \tilde{B}(y, x) \) as an impulse response in a hyperbolic equation.

Now the G-L equation (\( \ast \)) in Theorem 4 contains two unknowns \( A \) and \( K \) so we write \( A(t)\mathfrak{K}(t, s) = K(t, s) \) and \( \Delta_p(s)\Omega(t, s) = \hat{\Omega}(t, s) \) with \( f(\lambda, t) = A(t)\mathfrak{f}(\lambda, t) \) so that \( \mathfrak{f}(\lambda, t) = \psi^P(\lambda, t) + \int_0^t \hat{k}(t, \tau)\psi^P(\tau) d\tau \) and (\( \ast \)) \( 0 = \tilde{\Omega}(t, s) + \hat{k}(t, s) + \int_0^t \hat{k}(t, \tau) \hat{\Omega}(s, \tau) d\tau \) for \( s < t \).

Theorem 6. Assume (\( \ast \)) has unique solutions (\( \tilde{\Omega} \) being known via the moment functional) and define \( \hat{q}(t) = 2D_t K(t, t) \). Then \( \hat{K} \) satisfies a Goursat type problem \( \hat{Q}(D_t)^2 K(t, s) = [P(D_t) - \hat{q}(t)]\hat{K}(t, s) = P^*(D_s) K(t, s); \hat{K}(t, 0) = 0; 2D_t \hat{K}(t, t) = \hat{q}(t); \) and \( D_t [\hat{K}(t, t) / \Delta_p(t)](t, 0) = 0 \). Further \( \mathfrak{f} \) given via (2.1) satisfies \( Q(D_t)^2 \mathfrak{f} = -\lambda^2 \mathfrak{f} \).

One shows next that if \( f(\lambda, t) \sim \psi^Q(\lambda, t) \) with \( \psi^Q(\lambda, t) = -\lambda^2 \psi^Q(\lambda, t) \), \( Q = Q_0 + qu \), then, with \( K \) as in (2.1) and \( A = A_0^{-1} \), one obtains \( \hat{q}(y) = 2D_y K(y, y) = -q + q_0 \) where \( q_0 = \lambda(A_0'' / A_0') + (A_0'' / A_0')[(m+\lambda)] / y - \lambda(A_0'' / A_0')^2 \). Further \( A_0^{-1} p^F = (Q_0 + q_0) f \). Hence from Theorem 6, \( Q_0 f + q f = A_0^{-1} q f + (q - q_0) f = -\lambda^2 f + (q + q - q_0) f \). We have now \( q \) and \( A_0 \) at our disposal and for simplicity take \( q = 0 \) (other situations are possible but we omit any discussion here). Then

Theorem 7. Our connection (2.1) with \( A = A_0^{-1} \) will arise from an underlying operator \( Q = Q_0 \) with \( B: \psi^P + f \) in (2.1) representing a transmutation provided \( A_0 \) can be found satisfying \( C = A_0 C'' + [(2m+1) / y] C' - \lambda C = 0 \) where \( \hat{q} \) is known from solving (\( \ast \)). The resulting \( f \) are then orthogonal relative to \( d\omega \).

REFERENCES

2. R. Carroll, Transmutation, scattering theory, and special functions, North-Holland, Amsterdam, 1982


5. R. Carroll and F. Santosa, Impedance profile recovery from transmission data, Jour. Acous. Soc. Amer., to appear


9. R. Carroll, Some remarks on orthogonal polynomials and transmutation methods, to appear


Received November 12, 1984.
On a Functional Equation Connected to Sum Form

Nonadditive Information Measures on an Open Domain

Pl. Kannappan and P.K. Sahoo

Abstract. Shannon's entropy is additive. However, there are information measures such as the entropies of degree $\beta$ which are nonadditive. The sum form representation of these measures along with additivity and specific nonadditivity properties yield many interesting functional equations for instance (5) and (4). In this short communication, we find the measurable solutions of the functional equation (4) on an open domain.

1. Introduction

Let

$$\Gamma_n = \{ P = (p_1, p_2, \ldots, p_n) \mid p_k \geq 0, \sum_{i=1}^{n} p_i = 1 \}$$

be the set of all finite complete discrete probability distributions and

$$\Gamma_n^0 = \{ P = (p_1, p_2, \ldots, p_n) \mid 0 < p_i < 1, \sum_{i=1}^{n} p_i = 1 \}.$$

In analyzing the additivity and sum property of Shannon's entropy, one comes across the following functional equation

Research partially supported by an NSERC of Canada grant.
where $P \in \Gamma_n$ and $Q \in \Gamma_m$. The entropies of degree $\beta$

$$H_\beta^P(P) = \frac{\sum_p p^\beta - 1}{2^{1-\beta} - 1} \quad (\beta \neq 1)$$

proposed by Havrda and Charvat [4] are nonadditive. If we write

$$f(p) = \frac{p^\beta - p}{2^{1-\beta} - 1},$$

then the entropies of degree $\beta$ take the form

$$H_\beta^P(P) = \sum_{i=1}^n f(p_i).$$

The function $f$ in (3) is called the generating function. The generating function given by (2) satisfies the functional equation

$$\sum_{i=1}^n \sum_{j=1}^m f(p_i q_j) = \sum_{i=1}^n f(p_i) + \sum_{j=1}^m f(q_j) + \lambda \sum_{i=1}^n \sum_{j=1}^m f(p_i) f(q_j),$$

where $P \in \Gamma_n$, $Q \in \Gamma_m$, and $\lambda = (2^{1-\beta} - 1)$. The functional equation (4) was solved in [3,5,6,9] under various regularity conditions and in [10] without regularity condition. In all these papers [3,5,6,9,10], the functional equation was solved with the use of 0-probability and 1-probability along with the corresponding regularity conditions on $f$.

The use of these extreme values of the probabilities makes the functional equation easily solvable. However, the use of these requires definitions like $0^\beta = 0$, $0 \log 0 = 0$. It is also a priori quite possible that there may exist solutions other than those on $[0,1]$ restricted to $]0,1[$ as shown in [2] for a fundamental equation of information. In this short communication, in line with results obtained on open domains for similar equations [1,7,11,12], we report some results of our recent investigation on the functional equation (4) on open domain. The details of the proofs (see [8]) will appear elsewhere.

In order to solve (4) we make use of the following results.

**Result 1** [11]. Let $f: ]0,1[ \rightarrow \mathbb{R}$ (reals) and satisfy the functional equation

$$\sum_{i=1}^n \sum_{j=1}^m f(p_i q_j) = \sum_{i=1}^n f(p_i) + \sum_{j=1}^m f(q_j) + \lambda \sum_{i=1}^n \sum_{j=1}^m f(p_i) f(q_j),$$

where $P \in \Gamma_n$ and $Q \in \Gamma_m$. The entropies of degree $\beta$
for arbitrary (but fixed) \( n \geq 3 \) and at least one of the \( f_i \)'s be measurable. Then the \( f_i \)'s are given by

\[
f_i(p) = ap + b_i,
\]

where \( a \) and the \( b_i \)'s are arbitrary constants satisfying

\[
a + \sum_{i=1}^{n} b_i = 0.
\]

**Result 2 (J. Aczél).** Let \( \Phi, \Psi : [0,1] \rightarrow \mathbb{R} \) be real valued functions. They satisfy the functional equation

\[
g\Phi(p) - p\Phi(q) = \Psi(q) - \Psi(p)
\]

for all \( p \) and \( q \) in \([0,1]\) if, and only if,

\[
\Phi(p) = ap + b, \quad \Psi(p) = bp + c,
\]

where \( a,b,c \) are arbitrary constants.

**Proof.** Writing

\[
g(p) = \Psi(p) - \Psi(\delta),
\]

where \( \delta \) is a fixed real number in \([0,1]\) and putting (11) into (8), we get

\[
g\Phi(p) - p\Phi(q) = g(q) - g(p),
\]

and

\[
g(\delta) = 0.
\]

Now we put \( p = \delta \) in (12) and use (13) to obtain
\( g(q) = \alpha q - \delta \Phi(q) \).  

(14)

Putting this back into (12), we get

\( q \Phi(p) - p \Phi(q) = \alpha q - \delta \Phi(q) - \alpha p + \delta \Phi(p) \).  

(15)

Writing

\( h(p) = \Phi(p) - \alpha \)  

(16)

in (15), we obtain

\( (q - \delta)h(p) = (p - \delta)h(q) \).  

(17)

Let us substitute a fixed value \( q = q_0 \) (\( q \neq \delta \)) and get

\( h(p) = \alpha(p - \delta) \).  

(18)

Hence from (16) and (18), we get

\( \Phi(p) = ap + b \),  

(19)

where \( b = \alpha - a\delta \). Use of (19) and (14) in (11) yields

\( \psi(p) = \alpha p - a\delta p - \delta b + \psi(\delta) = bp + c \).  

(20)

The if part of the result is trivial.

The following lemma [8] plays an important role in the solution of (4).

**Lemma 3.** Let \( f : ]0,1[ \rightarrow R \) be measurable and satisfy the functional equation

\[ \sum_{i=1}^{n} \sum_{j=1}^{m} f(p_i q_j) = \sum_{i=1}^{n} f(p_i) \sum_{j=1}^{m} f(q_j), \]  

(21)

for a fixed pair of positive integers \( n,m \) (\( \geq 3 \)) and for all \( P \in \Gamma_n \) and \( Q \in \Gamma_m \). Then

\( f(p) = p^\beta, \quad p \in ]0,1[ \),  

(22)

or

\( f(p) = Ap + B, \quad p \in ]0,1[ \)  

(23)

where \( \beta \) is an arbitrary constant and \( A,B \) are constants satisfying
\[(A + mnB) = (A + nB)(A + mB). \quad (24)\]

Results 1 and 2 are used to prove this lemma. Using this lemma we have proved the following theorem in [8].

**Theorem.** Suppose that \( f: [0,1] \rightarrow \mathbb{R} \) is measurable and satisfies the functional equation (4) for a fixed pair \( m \geq 3, \ n \geq 3 \) for a constant \( \lambda \neq 0 \) and for all \( (p_1, p_2, \ldots, p_n) \in \Gamma_\lambda^0, (q_1, q_2, \ldots, q_m) \in \Gamma_\lambda^0 \). Then the function \( f \) is given by

\[
f(p) = \frac{(a-1)}{\lambda} p + \frac{b}{\lambda} \quad (25)
\]

or

\[
f(p) = \frac{p^\beta - 1}{\lambda}, \quad (26)
\]

where \( \beta \) is an arbitrary constant while the constants \( a, b \) satisfy the equation

\[
(a + mnB) = (a + nB)(a + mB). \quad (27)
\]

**Acknowledgement.** The proof of Result 2 is due to Professor J. Aczél. The authors are thankful to J. Aczél and to the referee for their comments and suggestions.

**References**


Faculty of Mathematics
University of Waterloo
Waterloo, Ontario, Canada
N2L 3G1

Received November 28, 1984.
RESUME. Soient $\alpha,\beta$ réels. D'après un théorème de Dirichlet il existe une infinité de points entiers $x=(a,b)\in\mathbb{Z}^2$, avec
$$\|a\alpha+b\beta\|^2 \leq (\max(|a|,|b|))^2,$$
on
où $\|\|$ désigne la distance à l'entier le plus proche. On peut montrer que cet énoncé reste vrai si on restreint le choix des points approximants $x=(a,b)$ à certains sous-ensembles de $\mathbb{R}^2$. De plus on peut étudier l'approximation diophantienne de $\alpha,\beta$ par des points entiers $x$ dans un domaine angulaire.

RESULTATS. Soit
$$\Psi_0 = \{(\xi_1,\xi_2)\in\mathbb{R}^2 \mid |\xi_1|^{1/3} < |\xi_2| < |\xi_1|^{7/4} \text{ ou } |\xi_1| < 1 \text{ ou } |\xi_2| < 1\},$$

et soit $A$ une transformation linéaire régulière. On note $\Psi$ et $\Phi$ les images de $\Psi_0$, respectivement de $\Phi_0$ par $A$. Par $\|\|$ on désigne la distance à l'entier le plus proche et pour $x=(a,b)\in\mathbb{R}^2$ soit $\langle x \rangle = \max(|a|,|b|)$.

THEORÈME 1. Pour tout couple $\alpha,\beta$ de nombres réels il existe une infinité de points entiers $x=(a,b)\in\mathbb{Z}^2$ avec
$$x \in \Psi \text{ et } \|a\alpha+b\beta\|^2 \leq c_1 \langle x \rangle^2,$$

où $c_1$ dépend tout au plus de $\alpha,\beta$ et $A$.

Remarquons que le même énoncé est vrai avec $c_1=c_1(A)$ indépendant de $\alpha,\beta$ si dans la définition de $\Psi$ on remplace l'ensemble $\Psi_0$ par $\Psi_1 = \{(\xi_1,\xi_2)\in\mathbb{R}^2 \mid |\xi_2| < |\xi_1|^{\kappa} \text{ ou } |\xi_1| < 1\}$, avec $\kappa > 7/4$. Le théorème 1 raffine un résultat dans [6].
THEOREME 2. Soient $\alpha, \beta$ réels avec $1, \alpha, \beta \not\propto$-linéairement indépendants. Soit $1/2 \leq n < 1$. On suppose qu'avec $c_2(\alpha, \beta, n) > 0$ on a
$$\max(\|a_q\|, \|b_q\|) \geq c_2 |q|^{-n}$$
(1)

pour tout $q \in \mathbb{Z}$, $q \neq 0$.

Alors il existe une infinité de points entiers $x = (a, b) \in \mathbb{Z}^2$, tels que
$$x \in \phi \quad \text{et} \quad \|a\alpha + b\beta\| \leq c_3^{-h(n)} \cdot$$
avec
$$h(n) = \frac{1}{4n} \left[1 + n + \sqrt{1 + 2n + 17n^2}\right],$$
on où $c_3$ dépend tout au plus de $\alpha, \beta, \Lambda$ et $n$.

On a $h(1/2) = 2$ et $h(1) = (1 + \sqrt{5})/2$. Pour $n = 1$ la condition (1) est sans objet. Dans ce cas le théorème 2, avec $c_3$ arbitraire positif, a été démontré [3] par W.M. Schmidt, qui a suggéré aussi l'hypothèse (1). Un exemple dans [3] montre qu'une hypothèse du type "$1, \alpha, \beta \not\propto$-linéairement indépendants" est indispensable.

Presque tous les couples $\alpha, \beta$ de nombre réels - au sens de la mesure de Lebesgue dans $\mathbb{R}$ - vérifient la condition (1) avec $n = \frac{1}{2} + \delta$, pour tout $\delta > 0$ ([2]). De plus l'ensemble des $(\alpha, \beta) \in \mathbb{R}^2$ avec $1, \alpha, \beta \not\propto$-linéairement dépendants est de mesure zéro. Le théorème 2 contient donc le

COROLLAIRE. Soit $\epsilon > 0$. Pour presque tous les couples $\alpha, \beta$ de nombres réels il existe une infinité de points entiers $x = (a, b) \in \mathbb{Z}^2$ avec
$$x \in \phi \quad \text{et} \quad \|a\alpha + b\beta\| \leq <x>^{-2+\epsilon}.$$

Ce corollaire démontre pour presque tous les couples $\alpha, \beta$ une conjecture générale de W.M. Schmidt [4].

Les démonstrations des théorèmes 1 et 2, données en détail dans [5], sont basées sur la méthode introduite dans [3], qui repose sur la géométrie des nombres. Pour la preuve du théorème 2 on
fait appel en plus au principe de Khintchine.

**REMARQUE.** Soit \( k \) entier, \( k \geq 2 \) et \( \epsilon > 0 \). On pose

\[
R = R(k) = \begin{cases} 2^{1-k} & , 2 \leq k \leq 11. \\ 2/(9k^2\log k + 4), & k \geq 12. \end{cases}
\]

Alors d’après un théorème de R.J. Cook [1] il existe une infinie- 
té de points entiers \( x = (a,b) \in \mathbb{Z}^2 \), avec \( \| a^k + b^k \| < \epsilon \), où \( c \) 
ne dépend que de \( k \) et \( \epsilon \). Cet énoncé peut être démontré à l’aide 
d’une méthode basée sur des estimations de sommes exponentielles. 
La même méthode permet de démontrer le résultat suivant:

Soient \( a, b \) réels et irrationnels, \( k \) entier, \( k \geq 2 \) et \( 0 < \epsilon < R/4 \).
Alors il existe une infinité de points entiers \( x = (a,b) \in \mathbb{Z}^2 \), 
tels que

\[
x \in \Phi \text{ et } \| a^k + b^k \| < \epsilon, \quad \text{avec}
\]

\[
r = r(k) = \begin{cases} (k + R - \sqrt{(k+R)^2 - 2R})/2, & 2 \leq k \leq 11. \\ 0, & k \geq 12. \end{cases}
\]

De plus, si

\[
\| aw \| > w^{-(k+R-1)/(1-\epsilon/2R)}
\]

pour tout \( w \in \mathbb{Z} \), \( w > w_0(k,a) \), alors on peut choisir \( r(k) = 0 \).

On a \( r < R/2 \sqrt{(k+R)^2 - 2R} < R/2k \).

**REFERENCES.**


[2] W.M. Schmidt: Approximation to algebraic numbers. L'enseign-


[5] P. Thurnheer: Approximation diophantienne par certains coup-

[6] P. Thurnheer: Zur diophantischen Approximation von zwei re-

Englischviertelstr. 17 8032 Zürich, Suisse.

Received November 29, 1984.
THE SET OF EXPONENTS, FOR WHICH FERMAT'S LAST THEOREM IS TRUE, HAS DENSITY ONE

Andrew Granville

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

ABSTRACT. We use Filaseta's theorem, which is a corollary of Faltings' theorem, to establish the proposition in the title.

1. In this paper we shall examine Fermat's equation

\[(1) \quad x^n + y^n = z^n\]

with positive integer exponents \(n > 2\).

Faltings [2] has established that for every exponent \(n > 3\), \(1_n\) has only finitely many solutions in pairwise coprime integers \(x, y, z\). Filaseta [3] has used Faltings' theorem to show that, for each integer \(r \geq 3\), there exists an integer \(N(r)\), such that if \(m > N(r)\) and \(n = mr\) then \(1_n\) has only trivial solutions. We note that \(N(r)\) is not effectively computable.

We will use Filaseta's theorem and an elementary lemma on set densities to establish that

\[
\lim_{N \to \infty} \frac{\# \{n \leq N \mid 1 \leq n \leq N \text{ and } (1_n \text{ has only trivial solutions})\}}{N} = 1.
\]

This improves on the result of Ankeny and Erdős [1] who established this theorem, though with the extra condition that \(n\) is coprime to \(x, y,\) and \(z\).
Finally, we shall note that our theorem holds true for any Fermat curve \( aX^n + bY^n = cZ^n \), with \( a, b, c \) non-zero integers, where, for the case \( a \pm b = c \) we define \((\pm 1, \pm 1, 1)\) to also be a 'trivial' solution.

2. For completeness, we present the proof of Filaseta's theorem.

**Theorem 1.** If \( r \geq 3 \) then there exists a positive integer \( N(r) \) such that if \( m > N(r) \) then the equation \( X^{mr} + Y^{mr} = Z^{mr} \) has only the trivial solution \((x,y,z)\) with \( xyz = 0 \).

**Proof:** If \( r = 3 \) the equation has only the trivial solution, as was shown by Euler. If \( r > 3 \), then by Faltings' theorem, there exists only finitely many triples of non-zero coprime integers \((x,y,z)\) such that \( x^r + y^r = z^r \); we note that \( |z| = \max\{|x|, |y|, |z|\} > 1 \). So there exists a positive integer \( L(r) \) such that \( |z| < L(r) \) for all solutions \((x,y,z)\) as above.

If \( m > N(r) = \left\lfloor \frac{\log L(r)}{\log 3} \right\rfloor + 1 \) and if \((a,b,c)\) is a non-trivial solution in coprime integers of \( X^{mr} + Y^{mr} = Z^{mr} \) then \( |c| \geq 2 \), \((a^m, b^m, c^m)\) is a non-trivial solution in coprime integers of \( x^r + y^r = z^r \), hence \( |c^m| \geq 2^m > L(r) > |c^m| \), which is a contradiction.

Now we prove a lemma about densities. Let \( P \) be a set of \((k \geq 1)\) prime numbers, let \( N \) be a positive integer and \( S_{p,N} = \{n \in \mathbb{N} \mid 1 \leq n \leq N \text{ and there exists } p \in P \text{ such that } p|n\} \).

**Lemma.** With the above notation

\[
\frac{\theta(S_{p,N})}{N} \geq 1 - \prod_{p \in P} \left(1 - \frac{1}{p}\right) - \frac{2^k}{N}
\]
Proof: Let \( Q = \prod_{p \in \mathbb{P}} p \). Then
\[
\theta(S_{p,n}) = \sum_{P \in \mathbb{P}} \left[ \frac{N}{P} \right] - \sum_{P_1 \neq P_2 \in P} \left[ \frac{N}{P_1 P_2} \right] + \ldots + (-1)^{k+1} \left[ \frac{N}{Q} \right].
\]
But
\[
\sum_{d|Q} \mu(d) \left[ \frac{N}{d} \right] = N - \sum_{d|Q} \mu(d) \left[ \frac{N}{d} \right].
\]
Then
\[
\frac{\theta(S_{p,n})}{N} \geq 1 - \prod_{p \in \mathbb{P}} \left( 1 - \frac{1}{p} \right) - \frac{2^k}{N}.
\]

Now we shall indicate the main result. Let \( p_1 = 2 < p_2 = 3 < p_3 < \ldots \) be the sequence of prime numbers, for each \( k \geq 2 \) let \( P_k = \{ p_2, p_3, \ldots, p_k \} \). For each prime \( p_j \) let \( N(p_j) \) be the integer considered in Filaseta's theorem and for each \( k \geq 2 \) let \( N_k = \max \{ p_j N(p_j) \} \). For each integer \( N \geq 1 \) we also consider the sets
\[
S_{p_k,N}^* = \{ n \in \mathbb{N} \mid N_k < n \leq N \text{ and there exists } p_j \in \mathbb{P} \text{ such that } p_j \mid n \}
\]
and \( F_N = \{ n \in \mathbb{N} \mid 3 \leq n \leq N \text{ such that equation (1) has only trivial solutions} \} \).
We note that $S'_{p_k} \leq \sum_{n \leq N'} \leq S'_{p_k} \cup \{1, 2, \ldots, n_k\}$

With above notations, we have:

**Theorem 2.** 
\[
\lim_{N \to \infty} \frac{\theta(F_N)}{N} = 1
\]

**Proof:** Let $\epsilon > 0$. Since 
\[
\prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right) = \frac{1}{\prod_{n=1}^{\infty} \frac{1}{n^2}} = 0
\]

there exists $k \geq 2$ such that 
\[
2 \prod_{j=1}^{2k} \left(1 - \frac{1}{p_j}\right) + \frac{1}{p_k} < \epsilon.
\]

Let $N' = (2^{k-1} + n_k) n_k$ and $N > N'$. By Filaseta's theorem, 

$S'_{p_k} \subseteq F_{n'}$, because if $n \notin S'_{p_k} \subseteq F_{n'}$ then $N_k < n \leq N$ and there exists 

$p_j \in P_k$ such that $p_j \mid n$; so $n = p_j \cdot m > N_k \geq p_j N(p_j)$ hence $m > N(p_j)$

and therefore $n = p_j \cdot m \notin F_{n'}$.

As $\theta(S'_{p_k} \cdot N) - N_k \leq \theta(S'_{p_k} \cdot N)$ it follows that 

\[
\frac{\theta(S'_{p_k} \cdot N)}{N} - \frac{N_k}{N} \leq \frac{\theta(S'_{p_k} \cdot N)}{N} \leq \frac{F_{n'}}{N} \leq 1
\]
On the other hand, by the lemma,

\[
\frac{\varphi(S_{p_k^kN})}{N} \geq 1 - \prod_{j=2}^{k} \left(1 - \frac{1}{p_j}\right) - \frac{2^{k-1}}{N} = \\
1 - 2 \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) - \frac{2^{k-1}}{N}.
\]

Thus

\[
1 - 2 \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) - \frac{2^{k-1} + N_k}{N} \leq \frac{\varphi(N)}{N} \leq 1
\]

hence if \( N \geq N' \geq N_k \geq p_k \) then

\[
1 - \varepsilon \leq \frac{\varphi(N)}{N} \leq 1. \text{ This shows that } \lim_{N \to \infty} \frac{\varphi(N)}{N} = 1,
\]

which completes the proof of the theorem.

3. A final remark concerns the equations

\[
(2)_n \quad aX^n + bY^n = cZ^n
\]

where \( a, b, c \) are non-zero integers, and solutions with \((X,Y,Z) \not\in (-1,0,1)\) are considered trivial.

For \( n > 3 \) the genus of \((2)_n\) is still greater than one, and a non-trivial soln of \((2)_n\) has at least one of \(|X|, |Y|, |Z| > 1|\).

Hence the proof of Filaseta's theorem as well as the proof of theorem 2 still hold true for this equation and we conclude that the density of exponents \( n \), for which \((2)_n\) has no solution \((x,y,z)\) with \(xyz \neq 0\), \(\gcd(x,y,z) = 1\), is equal to 1.
REFERENCES


Department of Mathematics and Statistics
Queen's University
Kingston, Ontario, K7L 3N6

Received November 29, 1984.
GROUPS WITH FIXED-POINT-FREE AUTOMORPHISMS
Ian Hughes

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

Using Graham Higman's reduction of the problem to the analogous one for Lie Rings, we show that if a finite group G has a fixed-point-free automorphism of order 7 then G is nilpotent of class at most 12.

1. Introduction

Graham Higman ([2] Theorem 1, p. 322) proved that to each prime $p$ corresponds an integer $k(p)$ such that if a Lie ring $L$ has an automorphism $\alpha$ of order $p$ which leaves fixed no element except zero, then $L$ is nilpotent of class at most $k(p)$. Later Krenkin and Kostrikin [3] (see Blackburn and Huppert [1], p. 361) proved that $k(p)$ is at most $\frac{(p-2)^{p-1}-1}{p-2}$ and Meixner [4] has improved this bound to $(p-1)^{2^{p-1}}$.

It is easy to see that $k(2) = 1$, and that $k(3) = 2$. Higman ([2] p. 331-334) showed that $k(5) = 6$ and for any odd prime $p$ that $k(p)$ is at least $\frac{2^{2^{p-1}}}{4}$. Using a computer, Scimemi [5] showed that $k(7) = 12$. We give an alternate proof that $k(5) = 6$ and outline a proof without computer of Scimemi's result.

2. Preliminaries

For $a_i$ in a Lie ring ($1 \leq i \leq n$) we denote by $a_1a_2a_3...a_n$ the left-ordered monomial $[[...[[a_1a_2]a_3]...a_n]$. 
By Higman ([2] p. 327) we may assume that L (in the Introduction) is a Lie ring over $\mathbb{Z}[\omega]$ where $\omega$ is a primitive $p$th root of unity and that $L$ is generated by $G = \langle G_i \rangle$ where $G_i = \{ a \in L \mid a(a) = \omega^i a \}$, the elements of $L$ of weight $i$. We think of these weights as being in $\mathbb{Z}_p$, the field of order $p$. Since $a$ leaves fixed only zero, $G_0 = \{ 0 \}$.

Let $a_i$ in $L$ have weight $w_i$ ($1 \leq i \leq n$). We denote by $x^i$ the sum $w_1 + w_2 + \ldots + w_i$ in $\mathbb{Z}_p$. We call the word $x_1x_2\ldots x_n$ the accumulative weight sequence of the left-normed monomial $a_1a_2\ldots a_n$.

We say that a word $x$ in elements of $\mathbb{Z}_p$ is zero if every left-normed monomial in elements of $G$ with $x$ as accumulative weight sequence is zero. Thus to prove that $L$ is nilpotent of class $c$ (say), it is sufficient to show that every word of length $c+1$ in elements of $\mathbb{Z}_p$ is zero.

Let $x_1x_2\ldots x_n$ be a word in elements of $\mathbb{Z}_p$. Then it is clear that this word is zero if either (1) $x_i = x_{i+1}$ for some $i$ or (2) $x_ix_{i+1}\ldots x_j$ is zero for some $i, j$; in particular for $i = j$, that is for $x_i = 0$. We use (1) and (2) repeatedly, without mention.

For $x_1x_2\ldots x_n$ a word in elements of $\mathbb{Z}_p$, we denote by $\rho(x_1x_2\ldots x_n)$ its reverse, that is the word $x_nx_{n-1}\ldots x_2x_1$.

Let $a_i \in G (1 \leq i \leq n)$, and suppose that the monomial $a_1a_2\ldots a_n$ has accumulative weight sequence $x_1x_2\ldots x_n$. By the Jacobi identity

$$a_1a_2\ldots a_{i-1}a_ia_{i+1}\ldots a_n = a_1a_2\ldots a_{i-1}[a_ia_{i+1}]a_{i+2}\ldots a_n + a_1a_2\ldots a_{i-1}a_{i+1}a_ia_{i+2}\ldots a_n.$$
The accumulative weight sequence of the first term on the right is \( x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n \) and that of the second term is
\[
x_1 x_2 \ldots x_{i-1} (x_{i-1} - x_i + x_{i+1}) x_i x_{i+1} \ldots x_n.
\]
We abuse notation and write
\[
x_1 x_2 \ldots x_n = x_1 x_2 \ldots x_{i-1} \ldots x_i x_{i+1} x_i \ldots x_n + x_1 x_2 \ldots x_{i-1} (x_{i-1} - x_i + x_{i+1}) x_i x_{i+1} \ldots x_n.
\]
We denote the "sum" on the right by \( x_1 x_2 \ldots x_{i-1} x_i x_{i+1} \ldots x_n \).
This identity will be used repeatedly, without mention, in the following way. Both terms on the right and their reverses having previously been proved to be zero, we conclude that the term on the left and its reverse is zero.

Almost every argument in the rest of this article uses only what has been already proved up to that point, and the identity above. We thus have the **Symmetry Principle**: If a word \( w \) in elements of \( Z_p \) is zero then so also is \( \sigma(w) \).

Suppose \( w, u, v \) are words in elements of \( Z_p \) and \( w = u + v \) and \( v \) is zero. We then write \( w = u \).

(A) By replacing \( a \) by \( a^k \) (\( 1 \leq k < p \)) it is not difficult to see that if the word \( x_1 x_2 \ldots x_n \) is zero (with the \( x_i 's \) in \( Z_p \)) then so is \( (kx_1)(kx_2)\ldots(bx_n) \). We denote the latter by \( k(x_1 \ldots x_n) \).

3. \( k(5) = 6 \)

For the rest of this article we will be concerned with accumulated weight sequences as words in elements of \( Z_p \).
In this section we state a lemma for arbitrary \( p \) and, in passing, obtain a tidy proof of Graham Higman's result that \( k(5) = 6 \).

\[\begin{array}{l}
\text{1. Hughes} \\
\text{63}
\end{array}\]
As usual we denote the elements of $\mathbb{Z}_p$ by $0, 1, 2, \ldots, p-1$. For $x$ in $\mathbb{Z}_p$ we denote by $xl$ the word $123\ldots x$. For $x$ in $\mathbb{Z}_p$ we denote the element $p - x$ in $\mathbb{Z}_p$ by $\bar{x}$.

**Lemma 1:** $\bar{yzt} = 0$ for all $y, z, t$ in $\mathbb{Z}_p$.


**Proof:** We must show that every word of length seven in elements of $\mathbb{Z}_5$ is zero. Let $w$ be a non-zero word of length seven. By (A) at the end of section 2, we may assume that the middle digit of $w$ is 2. By lemma 1 and the Symmetry Principle, the middle three digits of $w$ cannot be $12x$ nor $x21$ for all $x$ in $\mathbb{Z}_5$. Also $(\frac{1}{2})323(\frac{1}{2}) = 0$ and $3234 = 3434 = 0$. Thus,

$$a323b = 0 \text{ for all } a, b \text{ in } \mathbb{Z}_5 \quad (***)$$

and so the middle three digits of $w$ cannot be 323. Next $3(3241) = 4123$. Also, $4123(\frac{1}{2}) = 0$ and $4(41234) = 14321 = 0$ by the Symmetry Principle. We conclude that $3241a = 0$ for all $a$ in $\mathbb{Z}_5$. Also $3242 = 0$. Now $3243 = 323 + 3213$, and so $a3243b = 0$ for all $a, b$ by (***) except $43243b = 4343b = 0$.

We conclude that the middle three digits of $w$ cannot be 324 (or 423 by symmetry). Finally $2(424) = 2(414) = 323$ and so by (***) the middle three digits of $w$ cannot be 424. This completes the proof.
4. $k(7) = 12$

In this section we give a very condensed outline of the proof that $k(7) = 12$. We begin by stating a series of results, the first of which is an extension of Lemma 1, and each of the other uses the ones coming before it. We use the convention that the statement, for example $123abcd = 0$ means $123abcd = 0$ for all $a,b,c,d$ in $Z_7$ and also its reverse, that is, $dcba321 = 0$.

1. (a) $123abcd = 0$ except $123546(\frac{1}{5})$, $123561(\frac{2}{6})$, $123564(\frac{5}{6})$
   (b) $123abcde = 0$.

2. (a) $abc323def = 0$ unless $cda$ or $def$ is $62(\frac{4}{5})$ or $65(\frac{1}{4})$.
   (b) $abcd323efgh = 0$.

3. $abcdef123ghkm = 0$.

4. (a) $abcd124efgh = 0$ unless $efgh$ is $365(\frac{1}{4})$, $163(\frac{1}{2})$,
   $165(\frac{2}{3})$, $512(\frac{4}{5})$ or $513(\frac{6}{5})$.
   (b) $abc124defgh = 0$.

5. (a) $abcdef324efgh = 0$ with exceptions, namely the same for $efgh$ as in 4(a).
   (b) $abcd324efghk = 0$.

Next we deal with the exceptions in 4(a) and 5(a).

6. (a) $abcde124fghk = 0$ unless $e = 3$.
   (b) $abcdef124ghkm = 0$.

7. (a) $abcde324fghk = 0$ unless $e = 1$ and $fghk$ is $365(\frac{1}{4})$.
   (b) $abcdef324ghkm = 0$ and $abcd632416gh = 0$. 
We now consider words of length 13 and show that each is zero. By (A) at the end of section 2 we need only consider words with middle digit 2. Let \( w \) be a word of length 13 with middle digit 2 which is not zero. Then by 1(b), 2(b), 4(b) and 5(b) its middle three digits are restricted. We then consider all possible middle 5 digits, and using 1 to 7 above are left with eleven possible middle five digits for \( w \). We conclude by considering each of these individually.

References


5. SCIMEMI, B.: Unpublished.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
K7L 3N6

Received November 30, 1984.
DETERMINATION DU GROUPE DES AUTOMORPHISMES DU p-GROUPE DE SYLOW DU GROUPE SYMETRIQUE DE DEGRE p^m: L'IDEE DE LA METHODE

PAUL LENTOUDIS

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

Outline: We give in this note the idea of the method, which permitted us to determine and to describe the group of automorphisms Aut(P^m) of p-Sylow subgroup P_m of the symmetric group of degree p^m (where p is prime). The group P_m is (to isomorphy) the wreath product of m cyclic groups of order p, considered as permutation groups by identification with their regular representations (see [1], 5.9 and [3], 1)

On va présenter dans cette note la méthode, qui nous a permis de construire le groupe des automorphismes du p-groupe de Sylow du groupe symétrique S_p^m de degré p^m (p premier positif). Ce groupe de Sylow est à l'isomorphy près le produit d'entrelacement (wreath product) de m groupes cycliques d'ordre p, noté P_m, tel qu'il a été défini par L. Kaloujnine dans sa thèse [1].

On va donner d'abord la définition générale du produit d'entrelacement des groupes abstraits et quelques unes de ses propriétés indispensables pour notre propos.

Soient \(\Gamma_1, \Gamma_2, \ldots, \Gamma_m\) des groupes abstraits quelconques considérés comme groupes de permutation réguliers, dont les unités soient \(e_1, e_2, \ldots, e_m\). On pose

\[ e(s) = (e_1, e_2, \ldots, e_m) \quad (s \geq 0) \quad \text{et} \quad e = e^{(m)}. \]

Soit, pour \(0 \leq s \leq m\), \(E_s = \Gamma_1 \times \Gamma_2 \times \cdots \times \Gamma_s\) le produit direct des groupes \(\Gamma_1, \Gamma_2, \ldots, \Gamma_s\) (donc \(E_0 = \{e^{(0)}\}\); on pose en plus \(E = E_m\).

Soit \(a_s : E_{s-1} \rightarrow \Gamma_s\) une application de \(E_{s-1}\) dans \(\Gamma_s\) (en particulier \(a_1 : E_0 \rightarrow \Gamma_1\) est une constante \(e^{(1)}\)). Aussi \(a_s\) sera écrit \(a_s(x_1, \ldots, x_{s-1})\). On représente par le tableau

\[ A = \begin{bmatrix} a_1, a_2(x_1), \ldots, a_m(x_1, \ldots, x_{m-1}) \end{bmatrix} \]

la permutation de l'ensemble \(E,\)
définie par la correspondance

t=(t_1,t_2,...,t_m) \rightarrow t^*=(t_1'=a_1t_1,t_2'=a_2(t_2),...,t_m'=a_m(t_1,...,t_{m-1})t_m).

Quand les a_s (1\leq s \leq m) parcourent indépendamment, pour chaque s, l'ensemble des fonctions de E_{s-1} dans T_s, ces permutations forment un groupe, qu'on note G=\Gamma_1 \circ \Gamma_2 \circ \cdots \circ \Gamma_m et qu'on appelle _produit d'entrecacement_ des groupes abstraits \Gamma_1,\Gamma_2,...,\Gamma_m. La fonction 
a_s(x_1,...,x_{s-1}) sera appelée s-ième coordonnée de A et notée [A]_s.

Si \Gamma_i=F_p (1\leq i \leq m) (où F_p est le groupe cyclique d'ordre p, c'est-à-dire le groupe additif du corps de p éléments), alors le groupe 
F_p \circ F_p \circ \cdots \circ F_p est précisément le groupe P_m mentionné, qui est en fait un p-groupe de Sylow de S_{pm} [2]. Les fonctions a_s(x_1,x_2,...,x_{s-1}),
qui figurent comme coordonnées des tableaux de P_m (1\leq s \leq m), peuvent être et seront représentées par des polynômes x_1,x_2,...,x_{s-1} et à coefficients dans F_p, dans lesquels les exposants de chaque x_i ne sont pas supérieurs à p-1.

Soient z=(z_1,z_2,...,z_n) un vecteur de n variables z_1, z_2, ..., z_n et 
i=(i_1,i_2,...,i_n) un vecteur de n entiers. Alors on notera z^i le monôme 
z_1^{i_1}z_2^{i_2}\cdots z_n^{i_n}.
En particulier, si on adopte les variables x_1,x_2,...,x_{m-1}, on va poser, pour m-1 \leq \lambda \leq \lambda+1, x_{\mu,\lambda}=(x_{\mu},...,x_{\lambda+1}) et i_{\mu,\lambda}=(i_{\mu},...,i_{\lambda+1}). Si q est un entier, i_{\mu,\lambda} sera noté (q), s'il est de la forme (q,q,...,q). Ainsi
(x_{\mu,\lambda}^q=x_{\mu,\lambda}).
On écrit également x=x_{m-1,0}=(x_{m-1},...,x_1) et i=i_{m-1,0}=(i_{m-1},...,i_2,i_1). Si 
z=(x_{\mu,\lambda})^i_{\mu,\lambda},
on appelle hauteur de z l'entier
h(z)=i_{\mu}p^{\mu-1}+i_{\mu-1}p^{\mu-2}+\cdots+i_{\lambda+1}p^{\lambda+1}.

Soit g un sous-groupe de G=\Gamma_1 \circ \Gamma_2 \circ \cdots \circ \Gamma_m. On désigne par g_i les permutations de g, qui conservent les i premières coordonnées de e \in E: autrement dit, si j\neq i, a_j(e_1,...,e_{j-1})=e_j. On obtient ainsi 
suite de sous-groupes de g

g=g_0 \circ g_1 \circ g_2 \circ \cdots \circ g_m (s),
dont chacun est invariant dans le précédent. Cette suite s'appelle
la suite canonique de $g$. L'application $\phi_i : A_g \to a_i(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{i-1})$, où $A \in g_{i-1}$, est un isomorphisme, dit canonique, de $g_{i-1}/g_i$ dans $T_i$. Si $g$ est transitif, tous les $g_{i-1}/g_i$ le sont aussi, donc $\phi_i(g_{i-1}/g_i) = T_i$ et $g_m$, comme groupe de stabilité de l'élément $\varepsilon$ du support $E$, est anti-invariant dans $G$, c'est-à-dire il ne contient aucun sous-groupe (autre que l'unité) invariant dans $g$.

**Théorème d'immersion** [3]. Soit $h$ un groupe possédant une suite de sous-groupes

$$h = h_0 \supset h_1 \supset h_2 \supset \cdots \supset h_m \ (s')$$

telle que a) le quotient $h_{i-1}/h_i$ est isomorphe au groupe $T_i$ ($1 \leq i \leq m$) et, pour chaque $i=1, \ldots, m$, un isomorphisme $\psi_i$ de $h_{i-1}/h_i$ sur $T_i$ est donné b) $h_m$ est anti-invariant dans $H$. Alors, il existe un isomorphisme $\eta$ de $h$ sur un sous-groupe transitif $g$ de $G = T_1 \circ T_2 \circ \cdots \circ T_m$ vérifiant les propriétés suivantes: 1) $\eta(h_i) = g_i$ ; 2) $\psi_i = \phi_i \eta$, où on désigne aussi par $\eta$, comme il est habituel, l'homomorphisme induit par $\eta$ sur $h_{i-1}/h_i$ (pour quelque $i$). Un tel isomorphisme $\eta$ sera appelé un $(T_1, \ldots, T_m)$-isomorphisme (relativement à $(s')$, $(T_1, \ldots, T_m)$). En plus, à partir d'un choix arbitraire de représentants des classes (mod $h_i$) dans $h_{i-1}$, on peut construire effectivement, d'une certaine manière, un tel $\eta$.

**Théorème de transformation** [3]. Soit $\eta$ un $(T_1, \ldots, T_m)$-isomorphisme de $h$ (avec les $\psi_i$ fixés) dans $G$. Alors, si $\text{Int}_m(G)$ est le groupe des automorphismes intérieurs $\omega_\lambda$ de $G$ induits par les $\lambda \in G_m$, l'ensemble des $(T_1, \ldots, T_m)$-isomorphismes de $h$ dans $G$ est $\text{Int}_m(G)$. En particulier les $(T_1, T_2, \ldots, T_m)$-automorphismes de $G$ forment un groupe

$$\text{Aut}(T_1, \ldots, T_m)(G) = \text{Int}_m(G)$$

En posant $h=G$, les théorèmes précédents permettent de trouver $\text{Aut}(G)$, si on connaît a) les images de la suite canonique $(s)$ de $G$ par les éléments de $\text{Aut}(G)$ ainsi que b) l'ensemble $\text{Aut}(G, s)$ des automorphismes de $G$, qui stabilisent la suite $(s)$ en induisant n'importe quels automorphismes sur les facteurs de $(s)$. 

Soient \( \omega_1, \omega_2, \ldots, \omega_m \) des automorphismes quelconques des
\( \Gamma_1, \Gamma_2, \ldots, \Gamma_m \) respectivement. Soit alors \( \omega=(\omega_1, \omega_2, \ldots, \omega_m) \) l'automorphisme de \( G \), qui applique
\[ A=[a_1, a_2(x_1), \ldots, a_i(x_1, \ldots, x_{i-1}), \ldots] \]
\[ A'=[\omega_1 a_1, \omega_2 a_2(\omega_1^{-1} a_1), \ldots, \omega_i a_i(\omega_1^{-1} a_1, \ldots, \omega_{i-1}^{-1} x_{i-1}), \ldots] \](\( )\).

Cet automorphisme stabilise la suite \( (s) \) et induit, au sens évident, l'automorphisme \( \omega \) sur le groupe correspondant \( \Gamma_i \). Ces automorphismes \( \omega \) forment un groupe \( \Omega(\Gamma_1, \ldots, \Gamma_m) \) isomorphe à
\[ \text{Aut}(\Gamma_1) \otimes \ldots \otimes \text{Aut}(\Gamma_m) . \]
Il est visible que
\[ \text{Aut}(G, s)=\Omega_m(\Gamma_1, \ldots, \Gamma_m) \text{Aut}(\Gamma_1, \ldots, \Gamma_m)(G) . \]

Dans le cas où \( \Gamma=F \), \( \text{Aut}(\Gamma) \) est le groupe des multiplications des
\( x \in F \) par les \( w \in F \) non nuls. Si \( \Gamma_1=\Gamma_2=\ldots=\Gamma_m=F_p \) on va noter
\( w=(w_1, \ldots, w_m) \) l'automorphisme, qui applique
\[ A=[a_1, a_2(x_1), \ldots, a_m(x_1, \ldots, x_{m-1})] \]
\[ A'=[\omega_1 a_1, \omega_2 a_2(\omega_1^{-1} x_1), \ldots, \omega_m a_m(\omega_1^{-1} x_1, \ldots, \omega_{m-1}^{-1} x_{m-1})] \]
\[ \text{et on va noter } \Omega_m \text{ le groupe } \Omega_m(F_p, \ldots, F_p) . \]

La correspondance \( A \rightarrow \bar{A} \), où \( A \in P_m \) et \( \bar{A} \in P_{m-1} \), telle que \( [\bar{A}]_s=[A]_s \)
\[ \text{pour } 1 \leq s \leq m-1, \text{ est un homomorphisme de } P_m \text{ sur } P_{m-1}, \text{ appelé } (m-1)-\text{projection et noté } \text{pr}_{m-1}, \text{ dont le noyau est un sous-groupe caractéristique de } P_m \text{, noté } \Delta_{m-1} . \]
Si \( g \) est un sous-groupe de \( P_m \), son image
\[ \bar{g}=\text{pr}_{m-1}(g) \]
\[ \text{par } \text{pr}_{m-1} \text{ est appelée tête de } g \text{ et } \bar{g}=g \cap \Delta_{m-1} \text{ est appelé } \]
\[ \text{sous-groupe de fond de } g . \]

La correspondance \( \phi \rightarrow \bar{\phi} \), où \( A \in P_m \) et \( \bar{A} \in P_{m-1} \), telle que \( [\bar{A}]_s=[A]_s \)
\[ \text{pour } 1 \leq s \leq m-1, \text{ est un homomorphisme de } P_m \text{ sur } P_{m-1}, \text{ appelé } (m-1)-\text{projection et noté } \text{pr}_{m-1}, \text{ dont le noyau est un sous-groupe caractéristique de } P_m \text{, noté } \Delta_{m-1} . \]
Si \( g \) est un sous-groupe de \( P_m \), son image
\[ \bar{g}=\text{pr}_{m-1}(g) \]
\[ \text{par } \text{pr}_{m-1} \text{ est appelée tête de } g \text{ et } \bar{g}=g \cap \Delta_{m-1} \text{ est appelé } \]
\[ \text{sous-groupe de fond de } g \text{. } \]

La correspondance \( \phi \rightarrow \bar{\phi} \), où \( A \in P_m \) et \( \bar{A} \in P_{m-1} \), telle que \( [\bar{A}]_s=[A]_s \)
\[ \text{pour } 1 \leq s \leq m-1, \text{ est un homomorphisme de } P_m \text{ sur } P_{m-1}, \text{ appelé } (m-1)-\text{projection et noté } \text{pr}_{m-1}, \text{ dont le noyau est un sous-groupe caractéristique de } P_m \text{, noté } \Delta_{m-1} . \]
Si \( g \) est un sous-groupe de \( P_m \), son image
\[ \bar{g}=\text{pr}_{m-1}(g) \]
\[ \text{par } \text{pr}_{m-1} \text{ est appelée tête de } g \text{ et } \bar{g}=g \cap \Delta_{m-1} \text{ est appelé } \]
\[ \text{sous-groupe de fond de } g \text{. } \]

(\( )\) \text{Étant donnée une application } \( f:A \rightarrow B \text{ et } x \in A \), on note aussi
\( f \times x \) l'image de \( x \) par \( f \) et ce sera le seul emploi du point en tant que signe mathématique.
image Im(ϕ) et d'un certain sous-groupe Im*(ϕ) de Aut(Pm), tel que ϕ(Im*(ϕ)) = Im(ϕ), permet de présenter Aut(Pm) sous la forme: 
Aut(Pm) = Im*(ϕ)N(ϕ). La détermination de N(ϕ) et de Im*(ϕ) se fait 
de manière que la structure du groupe Aut(Pm) devient parfaitement 
claire. On va exposer ces résultats ultérieurement.

BIBLIOGRAPHIE


Paul Lentoudis
Université de Patras
Département de Mathématiques
Patras - GRECE

Received December 3, 1984.
GROUPS OF PROJECTIVITIES OF TOPOLOGICAL PLANES

Dieter Betten and Carsten Weigand

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

Abstract: The groups of projectivities of the Moulton planes, certain classes of topological translation planes and a class of topological Möbius planes are described in the article.

1. Introduction

We study groups of projectivities of topological projective planes, that is to say planes whose point and line sets are provided each with a non-discrete Hausdorff-topology, such that join and intersection are continuous. Perspectivities and therefore projectivities are homeomorphisms. All considered projective planes are compact and locally connected. The groups of projectivities provided with the compact-open topology then are topological transformation groups [1].

The classical examples: Let $\mathcal{P}_2 \mathbb{F}$ be the projective plane over $\mathbb{F} = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$, the classical fields of real and complex numbers and the quaternions and let $L$ be a line, then the group $\Pi = \Pi_L$ of projectivities is the Lie group $\text{PGL}_2(\mathbb{F})$ acting on $L = \mathcal{P}_2 \mathbb{F}$ in the usual way.

Let $\mathcal{P}_2 \mathbb{O}$ be the projective plane over the alternative division algebra of octonions over $\mathbb{R}$, then the action of $\Pi$ on $L$ is equivalent to the action of the 45-dimensional Lie group $\text{PSO}_{10}(\mathbb{R},1)$ on the 8-sphere of points in $\mathcal{P}_9 \mathbb{O}$ which are isotropic with respect to a quadratic form of index 1.

Let $\mathcal{A}_2 \mathbb{F}$ be the affine plane over $\mathbb{F} = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$, then the group of affine projectivities is $\Pi^\text{aff} = \{ x \rightarrow ax + b ; a, b \in \mathbb{F}, a \neq 0 \}$ and for $\mathcal{A}_2 \mathbb{O}$, $\Pi^\text{aff}$ is the group $\mathbb{R}^8 \rtimes \text{GO}_8^+(\mathbb{R})$ of similitudes of $\mathbb{R}^8$ of positive determinant.
2. The group of projectivities of the Moulton planes and a class of topological Möbius planes

With regard to their automorphism groups the projective Moulton planes are related closest to the real projective plane [11, 5.6.]. Nevertheless they have an extremely large group of projectivities.

The affine Moulton planes $M_k$ ($1 < k \in \mathbb{R}$) are obtained from the real affine plane by replacing the lines of negative slope $s$ by lines which have slope $s$ in the left half-plane and slope $ks$ in the right half-plane. Two such planes $M_k$ and $M_{k'}$ are isomorphic if $k = k'[11]$.

**Definition:** A bijection $\sigma$ of the projective line $P_1^R$ is called piecewise projective, if there exists a subdivision $P_1^R = I_1 \cup \ldots \cup I_n$ into closed intervals, such that on each $I_j$, the map $\sigma$ coincides with some element of $PGL_2(\mathbb{R})$.

In [3] it was shown that the set of all piecewise projective mappings forms a group $\Sigma$ by composition, acting as transformation group $(\Sigma, P_1^R)$ on the real projective line.

**Theorem:** [3] Let $L$ be a line of a projective Moulton plane $M_k$ and $\Pi$ the group of projectivities. Then there exists an isomorphism of transformation groups: $(\Pi, L) \cong (\Sigma, P_1^R)$.

**Remarks:**

a) $\Sigma$ contains the group $PGL_2(\mathbb{R})$ and all semi-dilatations $x \mapsto \begin{cases} x & \text{if } x \geq 0, \quad 0 < a \in \mathbb{R} \quad \text{Let } H_1 \text{ be the group of all semi-dilatations, then in [3] was shown: } \Sigma = \langle PGL_2(\mathbb{R}), H_1 \rangle.$

b) All Moulton planes $M_k$ ($1 < k \in \mathbb{R}$) have the same group of projectivities.

c) $\Sigma$ acts transitively on the oriented $n$-tuples of points of
for each nonnegative integer n [3].

d) There are elements different from identity, which fix elementwise a whole interval, e.g. the (proper) semi-dilatations.

e) The structure of $\Sigma$ is known [3;5]: $\Sigma$ possesses the commutator series $\Sigma = \Sigma' = \Sigma''$ with $\Sigma' \cong \mathbb{Z}_2$, $\Sigma' = (\mathbb{R}, +)$, $\Sigma'$ is a simple group and $\Sigma = \langle \text{PSL}_2(\mathbb{R}), H_1 \rangle$, the group of orientation preserving elements of $\Sigma$.

The group of projectivities of the classical miquelian Möbius plane is the group $\text{PGL}_2(\mathbb{R})$ (for a definition of projectivities of Möbius planes see e.g. [7, §1]). In [6, §4] G. Ewald described a class of 2-dimensional Möbius planes as follows: A great circle $C$ of a sphere in $\mathbb{R}^3$ defines two half-spheres. Replace one half-sphere by an ellipsoid, such that a surface $F$ which is differentiable everywhere results. The plane intersections of $F$ define the circles of a non-miquelian Möbius plane $M$. The planes are of Hering-type IV 1 [10] and all derived affine planes are arguesian.

Theorem: Let $\Pi$ be the group of projectivities of $M$, then $\Pi = \Sigma$.

Proof: a) $\Pi \leq \Sigma$ is easily verified (cp. [7, pp. 130-132]).

b) $\text{PGL}_2(\mathbb{R}) \leq \Pi$, see [7, 1.5].

c) To show $H_1 \leq \Pi$, map $F$ onto $\{(x, y) ; x, y \in \mathbb{R} \cup \{\infty\}\}$ by a stereographic projection, such that $C$ is projected onto the y-axis. Some circle of $M$ is projected onto the curve $K$, which is obtained from a usual circle of $\mathbb{R}^2$ with centre $(0,0)$ and radius 1 by replacing the part in the half-plane $x>0$ by some ellipse. Then $X := \{(x,0) ; x \in \mathbb{R}\}$ $\cup \{\infty\}$ is the symmetry axis of $K$. Let $\varphi_1$ ($\varphi_2$) be the perspectivity from $X$ to $K$ (from $K$ to $X$) with centres $\infty$ and $(x,\eta) \in K$, $\eta \neq \pm 1$ (with centres $\infty$ and $(0,-1) \in K$). Then $\varphi_2 \circ \varphi_1$ is a projectivity from $X$ onto itself. By combining $\varphi_2 \circ \varphi_1$ with a suitable element of $\text{PGL}_2(\mathbb{R})$ one
obtains on $X$ a proper semi-dilatation. By variation of $(\xi, \eta) \in K$, inversion and iteration one gets on $X$ all semi-dilatations.

3. The groups of projectivities of certain classes of topological translation planes

A connected compact translation plane $P$ is coordinizable over a locally compact topological quasifield $Q$, whose additive group is a vector group $\mathbb{R}^n$ ($n = 1, 2, 4, 8$). The lines of $P$ are homeomorphic to the $n$-sphere $S^n$ and the affine lines through the origin are linear subspaces of $Q \times Q$ of real dimension $n$ over the kernel of $Q$. The remaining affine lines are the images of the lines through the origin under the translation group $\mathbb{R}^{2n}$ [11, §7].

Now consider $\mathbb{R}^8$ with usual addition and multiplication $\odot$ defined by $(\mathbf{x} = (x_1, \ldots, x_8), \mathbf{a} = (a_1, \ldots, a_8), x_i, a_1 \in \mathbb{R})$:

$$x \odot a = (x_1, \ldots, x_8) \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 \\ -a_2 & r[a_1] & a_4 & -a_3 & a_6 & -a_5 & -a_8 & a_7 \\ -a_3 & -a_4 & r[a_1] & a_2 & a_7 & a_8 & a_5 & -a_6 \\ -a_4 & a_3 & -a_2 & r[a_1] & a_8 & a_7 & a_6 & -a_5 \\ -a_5 & -a_6 & -a_7 & -a_8 & r[a_1] & a_2 & a_3 & a_4 \\ -a_6 & a_5 & -a_8 & a_7 & -a_2 & r[a_1] & -a_4 & a_3 \\ -a_7 & -a_8 & a_5 & -a_6 & -a_3 & a_4 & r[a_1] & -a_2 \\ -a_8 & -a_7 & a_6 & a_5 & -a_4 & -a_3 & a_2 & r[a_1] \end{pmatrix}$$

where $1 < r \in \mathbb{R}$ and $r[t] = \begin{cases} t & \text{if } t \geq 0 \\ rt & \text{if } t \leq 0 \end{cases}$. Denote this structure by $(\mathbb{F}_r, +, \odot)$ (if $r=1$ one gets the multiplication of the octonions).

Using [8, 2.3.] one shows:

$(\mathbb{F}_r, +, \odot)$ is an 8-dimensional topological quasifield with kernel $\mathbb{F} \cong \{(x_1, 0, \ldots, 0) ; x_1 \in \mathbb{R}\}$ for all $r > 1$.

Let $Q_r := \{(x_1, x_2, 0, \ldots, 0) ; x_1 \in \mathbb{R}\} \subseteq \mathbb{F}_r$ and $D_r := \{(x_1, \ldots, x_4, 0, \ldots, 0) ; x_1 \in \mathbb{R}\} \subseteq \mathbb{F}_r$, then $Q_r$ ($D_r$) with the induced addition and multiplication is a 2-dimensional (4-dimensional) sub-quasifield of $\mathbb{F}_r$ and $Q_1 \cong \mathbb{I}$, $D_1 \cong \mathbb{H}$. The 4-dimensional trans-
lation planes over $Q_r (r > 1)$ are isomorphic to the planes [2, Satz 5].

The quasifields $D_r$ and their correlated 8-dimensional translation planes were described in [9, 3.3]. Two such planes over $Q_r$ and $Q_{r'}$ ($D_r$ and $D_{r'}$) are isomorphic iff $r = r'$.

**Definition:** Bijections of $\mathbb{R}^n$, defined by

$$(x_1, \ldots, x_n) \mapsto \begin{cases} (x_1, \ldots, x_n) & \text{if } x_1 > 0 \\ (x_1, \ldots, x_n) (c_1, c_2, \ldots, c_n) & \text{if } x_1 \leq 0 \end{cases}$$

where $c_i \in \mathbb{R}, c_i > 0$ are called semi-affinities of $\mathbb{R}^n$.

Let $H_n$ denote the group of all semi-affinities of $\mathbb{R}^n$. $H_n$ acts on $\mathbb{R}^n \cup \{0\}$ by mapping $\infty$ onto itself. $H_1$ is the group of semi-dilatations.

In the following, let $\Pi(Q) (\Pi_{\text{aff}}(Q))$ be the group of (affine) projectivities of the projective (affine) plane over the $n$-dimensional quasifield $Q$ and let $\Pi_{\text{aff}}(Q)$ denote the stabilizer of $\Pi_{\text{aff}}(Q)$ on $0 \in \mathbb{R}^n$.

**Theorem:** Let $r > 1$, then we have

a) [4, 1.1., p. 29] $\Pi_{\text{aff}}(Q_r) = GL_2(\mathbb{R})^1$, $\Pi_{\text{aff}}(Q_r) = H_2$.

b) $\Pi (Q_r) \cong (\text{PGL}_2(\mathbb{R}), H_6)$.

c) $\Pi (Q_r) \cong (\text{PGL}_2(\mathbb{R}), H_6)$.

**Remarks:** As $\text{PGL}_2(\mathbb{R}) \cong \text{PSO}_4(\mathbb{R}, 1)$ and $\text{PGL}_2(\mathbb{R}) \cong \text{PSO}_6(\mathbb{R}, 1)$ [12], the groups $<\text{PGL}_2(\mathbb{R}), H_6>$ and $<\text{PGL}_2(\mathbb{R}), H_6>$ belong to the family $G_n := <\text{PSO}_{n+2}(\mathbb{R}, 1), H_n>$, $n \geq 2$. We have for all $n \geq 2$:

a) The groups $G_n$ are simple [4, 2.6.; 13, 2.5.].
b) The transformation groups \((G_n, S^n)\) are \(k\)-transitive for all nonnegative \(k \in \{4, 2, 7, 13, 2, 6\}\).

References

CLASS MULTIPLIERS FOR THE ORTHOGONAL GROUPS OVER GF(2)

J. S. Frame

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

Abstract. Generic formulas are found for the class multipliers of all irreducible complex characters of the orthogonal groups \( O_n(2) \) on eight classes besides the two already known.

1. Introduction. The absolutely irreducible complex (AIC) characters \( \chi^\sigma \) of the orthogonal group \( G_n = O_{2n+1}(2) \) or \( \chi^\sigma \) of its maximal subgroup \( G^\sigma_n = O_{2n+2}^\sigma(2) \), with \( \sigma = \pm \) (or \( \pm 1 \)), have values \( \chi \alpha \) or \( \chi \lambda \) on class \( C^\alpha \) of size \( \alpha C \alpha \) or \( \alpha C \lambda \). Their class multipliers are

\[
\omega^\chi = \alpha C \lambda \chi \lambda / \chi \lambda
\]

For eight classes \( C \alpha \) besides the classes \( C_1 \) and \( C_t \) for which they are already known, this report derives generic formulas for the class multipliers \( \omega^\chi \) (or \( \omega^\chi \) ) of each AIC character \( \chi \) of \( G_n \) (or \( \chi^\sigma \) of \( G^\sigma_n \)) as polynomials in \( N = 2^n \) with coefficients determined by \( \chi \) (or \( \chi^\sigma \)). Thus \( \chi \lambda \) (or \( \chi \lambda^\sigma \)) can be found explicitly for each of ten classes corresponding to classes of \( S_8 \) as follows:

\[
\begin{align*}
C_1 &= 1^8, \\
C_2 &= 1^3 2^5, \\
C_3 &= 1^3 5, \\
C_4 &= 1^4 2^2, \\
C_5 &= 2^4.
\end{align*}
\]

If \( \chi \) has level \( L = 2^k \), and its "parent" character \( \phi \) (see \([1]\) ) in \( G^\sigma_8 \) (or \( G_8 \)) has codegree \( d \) (= group order/\( \phi_1 \) ), then the degree \( \chi_1 \) (or \( \chi^\sigma_1 \)) is expressible as a polynomial in \( N \).

\[
\chi_1 d = \prod_{i=1}^{2^k} (N - r_i) = N^{2^k} (1 - a_1/N + a_2/N^2 - a_3/N^3 + \cdots)
\]

where the \( 2^k \) roots \( r_i \) are distinct factors of \( N^2 \) having the elementary symmetric functions \( a_i \). As before, we denote the monic
polynomial (1.3) by a code word whose $v^{th}$ letter is $h$, $k$, $g$, or $i$ according as $N-2v-1$, $N+2v-1$, both or neither are factors. Thus the character of $G^+_n$ denoted $h_{gk}/72$ has degree $(N-1)(N^2-4)(N+4)/72 = 15(252)20/72 = 1050$, and $k_{ih}/6 = (N+1)(N-4)/6$. This symbolism, with powers of $N$ adjoined where needed, describes the sizes of pertinent conjugacy classes in $G_n$ and $G^+_n$ as follows:

<table>
<thead>
<tr>
<th>$C_A$</th>
<th>$C_3$</th>
<th>$C_5$</th>
<th>$C_S$</th>
<th>$C_R$</th>
<th>$C_t$</th>
<th>$C_3t$</th>
<th>$C_{st}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0C_A$</td>
<td>$gN^2/6$</td>
<td>$gN^4/2^5$</td>
<td>$g/2^2$</td>
<td>$g/2^2$</td>
<td>$gN^2/2^3$</td>
<td>$gN^2/2^3$</td>
<td></td>
</tr>
<tr>
<td>$0C_A$</td>
<td>$hNh^2/24$, $hNh^2/2^10$, $hNh^2/2^5$, $hNh^2/2^3$, $hNh^2/2^3$, $hNh^2/2^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Also $0C_{4-} = 0C_{4+} = gN^2/2^5$, $0C_{4-} = gNh^2/2^8$, and $0C_{4+} = gNh^2/2^8$.

Character and class size formulas for $G^-_n$ can all be obtained from those of $G^+_n$ by either changing $f(N)$ to $f(-N)$ or replacing $h$'s by $k$'s and $k$'s by $h$'s, and $r_1$ by $-r_1$, thus changing signs of $a_1, a_2, \ldots$

Hence we may restrict attention to formulas for $G_n$ and $G^+_n$.

Class multipliers for class $C_t$ were already found [1] to be:

$\omega_t = 0C_t \lambda_t/\lambda_1 = T(N+a_1)^{-1}$, $\omega_t^\sigma = (T/2)(N+a_1-\sigma)$ (1.5)

where $T$ is the sign of $\lambda_t$ and $T = T/N$.

Letting the class symbol $C_A$ denote also the sum of its elements in the group ring, we note the four product formulas

$$C_t^2 = m_{t1}C_1 + 3C_3 + 2C_s, \quad m_{t1} = N(N-\sigma)/(1+\sigma^2)-1+\sigma^2$$

$$C_3C_t = m_{3t}C_t + C_{3t} + 4C_{4-}, \quad m_{3t} = N(3N-\sigma)/(1+\sigma^2)$$

$$C_RC_t = m_{rs}C_s + C_{st} + 2C_{4+}, \quad m_{rs} = 1 - \sigma^2$$

$$C_SC_t = m_{st}C_t + 3m_{rs}C_R + 3C_{3t} + 3C_{st} + 2C_{4-}$$

(1.6a, b, c)

where $m_{st} = (\frac{1}{N^2-2})/(1+\sigma^2)$, $\sigma$ is 0 for $G^-_n$, +1 for $G^+_n$, and $m_{R\mu}$ are the multiplicities of elements of $C_\mu$ in $C_\mu C_t$. Formulas (1.6) and (1.7a, b, c) yield similar formulas for class multipliers $\omega_A$ or $\omega_A^\sigma$, and supply four of the eight pairs of relations we require.
In Section 2 we derive formulas for $\omega_3$, $\omega_3^+$, $\omega_5$, and $\omega_5^+$, and find $\omega_s$, $\omega_s^+$ from (1.6). In Section 3 we evaluate the functions

$$\omega_x = \omega_3 - 2\omega_r, \quad \omega_y = 4(\omega_{4+} - \omega_{4-})$$

for $G_n$ and $\omega_x^+$ and $\omega_y^+$ for $G_n^+$. Then, applying (1.7a,b,c) we get

$$\begin{bmatrix} 4 \omega_{3t} \\ 8 \omega_{st} \\ 16 \omega_{4-} \end{bmatrix} = \begin{bmatrix} 1 & 1 & -3 \\ -3 & 1 & 5 \\ 3 & -1 & 3 \end{bmatrix} \begin{bmatrix} (\omega_3 - m_{3t}) \omega_t \\ (\omega_s - m_{st}) \omega_t - 3m_{rs} \omega_r \\ \omega_r \omega_s^+ - m_{rs} \omega_s + \omega_y/2 \end{bmatrix}$$

with corresponding formulas for $G_n^+$. Thus the ten character values can be computed explicitly for each AIC character $\lambda$ of $G_n$ or $G_n^+$. Other values may then be obtained either by congruence relations or by additional product formulas analogous to (1.7a,b,c).

2. Basic and extended characters. The parent character $\phi$ in $G$ for $\lambda$ of level $\ell$ in $G_n$ (or in $G_n^+$ for $\lambda^+$ in $G_n^+$) generates an extended level $\ell$ character $\Phi$ that contains $\lambda$ (or $\lambda^+$) and possibly other AIC characters of lower level. For example, the characters $\phi = (1,1)$ and $(1,-1)$ of $G_1$ of codegree 2 generate the extended $G_n$-characters $\Phi = (\alpha + \beta)/2 = \lambda + 1$ and $(\alpha - \beta)/2 = \lambda - 1$ that are induced in $G_n$ by $G_n^+$ and $u_n^-$. These include the 1-character of level 0 with the level 1 AIC characters $Y$ or $X$ that have sign $e^+=1$ on class $C_+$. The extended character $\Phi$ multiplied by the codegree $d$ of $\phi$ is a linear combination of basic characters $b_{\lambda}$, one for each class $C_{\mu}$ of $G_\lambda$ (or $G_\lambda^+$), with coefficients $w_{\mu}$ that are the class multipliers of $\phi$ for $C_{\mu}$. The $b_{\lambda}$ have values $b_{\lambda}$ on each class $C_{\lambda}$ of $G_n$ (or $G_n^+$) that are $\pm$ a power of 2 or 0. Thus we write

$$\Phi d = \sum_{\mu} w_{\mu} b_{\lambda}$$

$$\Phi d/\alpha^2 = 1 + W_t(\beta/\alpha) + W_3(Y/\alpha) + W_2(\beta/\alpha)^2 + W_r(\alpha_2/\alpha^2)$$

$$+ W_3t(\beta Y/\alpha^2) + W_{st}(\beta/\alpha)^3 + W_4(\delta/\alpha^2) + W_4(\beta_2/\alpha^2) + W_5(\varepsilon/\alpha^2) + \cdots$$
Values of the basic characters $\alpha, \beta, \ldots$ on four classes $C^4$ are

<table>
<thead>
<tr>
<th>$C_i$</th>
<th>$\alpha$</th>
<th>$\alpha^*$</th>
<th>$\beta$</th>
<th>$\beta^*$</th>
<th>$\gamma$</th>
<th>$\epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1$</td>
<td>$N^2$</td>
<td>$N^2$</td>
<td>$N$</td>
<td>$N$</td>
<td>$1$</td>
<td>$1$</td>
</tr>
<tr>
<td>$C_3$</td>
<td>$N^2/4$</td>
<td>$N^2/4$</td>
<td>$-N/2$</td>
<td>$-N/2$</td>
<td>$1$</td>
<td></td>
</tr>
<tr>
<td>$C_5$</td>
<td>$N^2/16$</td>
<td>$N^2/16$</td>
<td>$-N/4$</td>
<td>$-N/4$</td>
<td>$1$</td>
<td>$-4$</td>
</tr>
<tr>
<td>$C_t$</td>
<td>$N^2/2$</td>
<td>$N^2$</td>
<td>$0$</td>
<td>$N$</td>
<td>$-N$</td>
<td>$-1$</td>
</tr>
</tbody>
</table>

Applying (2.2) and (2.3) for classes $C_1, C_3$ and $C_5$ and letting $D_1$ denote a sum of codegrees $d/d_1$ to account for any level $k$ characters that may be included in $\Phi$, we have

\begin{align*}
\lambda_1 d/N^{2l} &= 1 + W_1 t/N + (W_3 + W_2 + W_4 - D_1)/(N^2 + (W_3 t + W_3 + W_4 - D_1)N)/N^3 + \ldots \quad (2.4a) \\
\lambda_3 d/(4/N^2)^l &= 1 - 2W_1 t/N + (W_3 + W_2 + W_4 - D_1)/N^2 - (3W_3 t + a_3)8/N^3 + \ldots \quad (2.4b) \\
\lambda_5 d/(16/N^2)^l &= 1 - 4W_1 t/N + (W_3 + W_2 + W_4 - D_1)16/N^2 + 64a_3/N^3 + (a_4 - 5W_5)4/N^4 + \ldots \quad (2.4c)
\end{align*}

Noting the $a_i$ in (1.3) and inverting (2.4a), we next obtain

\begin{align*}
(\lambda_1 d/N^{2l})^{-1} &= 1 + a_1/N + (a_1^2 - a_2)/N^2 + (a_1^3 - 2a_1 a_2 + a_3)/N^3 + \ldots \quad (2.5) \\
L^2 \lambda_3 d/N^{2l} &= 1 + 2a_1/N + 4(a_2 - 3W_3)/N^2 + 8(a_3 - 3W_3)/N^3 + \ldots \quad (2.6) \\
L^4 \lambda_5 d/N^{2l} &= 1 + 4a_1/N + 16a_2/N^2 + 64a_3/N^3 + 64(a_4 - 5W_5)/N^4 + \ldots \quad (2.7)
\end{align*}

We now subtract (1.3) from (2.6) and (2.7) and multiply the remainders by (2.5) to obtain the character/degree formulas

\begin{align*}
L^2 \lambda_3/\lambda_1 &= 1 + 3a_1/N + 3(a_1^2 + 2a_2 - 4W_3)/N^2 + 3(a_1^3 + 3a_2^2 - 4a_1 W_3 - 8W_3)/N^3 + \ldots \quad (2.8) \\
L^4 \lambda_5/\lambda_1 &= 1 + 5a_1/N + 5(a_1^2 + 3a_2)/N^2 + 5(a_1^3 + 2a_1 a_2 + 13a_3)/N^3 + 5(a_1^4 + a_1^2 a_2 - 3a_2^2 + 14a_1 a_3 + 5a_4 - 256W_5)/N^4 + \ldots \quad (2.9)
\end{align*}

**Theorem 2.1.** The class multipliers for $\lambda$ and $\lambda^+$ on class $C_3$ are

\begin{align*}
\omega_3 &= (T^2/2)((N^2 - 1)/3 + a_1(N + a_1) + a_2 - 4W_3) \quad (2.10a) \\
\omega_3^+ &= (T^2/8)((N - 1)(N - 2)/3 + a_1(N + a_1 - 3) + a_2 - 4W_3) \quad (2.10b)
\end{align*}

**Proof:** We multiply (2.8) by $c_3^0/L^2$ and $c_3^+L^2$ from (1.4), and discard all terms in $N^1, N^2, \ldots$. These coefficients must vanish since $\omega_3$ and $\omega_3^+$ are algebraic integers for all $N$ and $T = \tau N/L$. 


Theorem 2.2. The class multipliers for $\tilde{\chi}$ and $\chi^+$ on class $C_2$ are

\[ \omega_\ast = \frac{\left( T^2/4 \right) (N^2+1+a_1 (N-a_1) - 3a_2 + 12w^2) - T(N+a_1) + 1 - N/2}{J} \]  

(2.11a) \[ \omega^+ = \frac{\left( T^2/16 \right) (N^2-N+a_1 (N-a_1)+5) - 3a_2 + 12w^2) - N(N-1)/4}{J} \]  

(2.11b)

Proof: These formulas follow from Theorem 2.1 and (1.6).

Theorem 2.3. The class multipliers for $\tilde{\chi}$ and $\chi^+$ on class $C_5$ are

\[ \omega_5 = \frac{\left( T^2/2^6 \right) \left[ N^4+5a_1 N^3+5(a_1^2+3a_2-1)N^2 + 5(a_1^3-5a_1+2a_1 a_2+13a_3)N \right.}{+ 5(a_1^4-5a_1^2 a_2-3a_2^2-15a_2+14a_1 a_3+51a_4-2^8 w^5)} \]  

(2.12) \[ \omega^+_5 = \frac{\left( T^2/2^10 \right) \left[ N^4+5a_1(N-1)N^3+5(a_1^2-5a_1+3a_2)N^2 + 5(a_1^3-5a_1^2+42a_2)N \right]}{- 16 - 2^8(5w^5)} \]  

(2.13)

Proof: Using (2.9) and (1.4) we mimic the proof of Theorem 2.1.

3. Formulas generated by level $n$ characters. Next let $\lambda$ in $G_n$ be the parent of a level $n$ character $\tilde{\chi}^+$ in $C_2$ whose roots $R_j$ are $R_j: 1, z^2, z^4, \ldots, z^{2^n}$, and $\bar{R}_j: -1, z^2, z^4, \ldots, z^{2^n}$, with all roots $R_j$ of $\tilde{\chi}$ and all roots $\bar{R}_j$ of $\chi^+$.

The elementary symmetric functions $A_i$ of $R_j$ and $\bar{A}_i$ of $\bar{R}_j$ are

\[ -A_1 = \omega_1 = T(N+a_1) - 1, \quad A_2-A_1 = T^2(a_1 a_2) - (T^2-1)/3 \]  

(3.2a) \[ -\bar{A}_1 = \omega^+_1 = (T/2)(N+a_1-1), \quad \bar{A}_2 = (T/2)^2((N-1)(a_1-1)+a_2)-(T^2-1)/3 \]  

(3.2b) \[ A_3-A_2-A_1 = T^3(Na_1(N+a_1)+a_1 a_2) \quad \text{for } G_n \]  

(3.3a) \[ \bar{A}_3-\bar{A}_2 \bar{A}_1 = (T/2)^3((N-1)(a_1-1)(N+a_1)+a_1 a_2 a_3) \quad \text{for } G_n^* \]  

(3.3b)

Formulas analogous to (1.3) and (2.4) for classes $C_1$ and $C_2$ are

\[ f_1^+d/z^{2n} = 1 + \omega_1/z + (\omega_1^+ + \omega_1^+ + \omega_1^+)z + (\omega_2^+ + \omega_1^+ + \omega_1^+)z^2 + \cdots \]  

(3.4)

\[ f_2^+d(2/z^{2^n}) = 1 + 0/z + (-\omega_2^+ + 2\omega_1^+/z)z + (-4\omega_1^+ + 4\omega_1^+)z^2 + \cdots \]  

(3.5)

The class multiplier for $\chi^+$ on $C_2$ is $(2/2n)(z+A_1-1)$ by (1.5).
Theorem 3.1. The class multiplier functions $\omega_x$ and $\omega_y$ for $G_n$ are

$$\omega_x = \omega_x - 2\omega_x = T^2(na_1 + a_2) - (T^2 - 1)/3 + n^2 - 1$$  \hspace{1cm} (3.6)$$

$$\omega_y = 4(\omega_4 - \omega_4) = T^3(na_1(n + a_1) + a_1a_2 - a_3)$$  \hspace{1cm} (3.7)$$

Proof: $\omega_x = Z(Z-1)/2$ for $G_n$, so $N_{\omega_x}^{+}/\omega_1 = 1 + A_1/(Z-1)$. By (1.4)

$$\omega_x + 2D = \omega_x - 2\omega_x + 2(\omega_2 + \omega_2 - a_2) = 3\omega_2 + 2\omega_3 - 2a_2$$

$$= \omega_2 - 2a_2 = A_1^2 - 2A_2 - (N^2 - 1)$$  \hspace{1cm} (3.8)$$

It follows from (3.5), (3.4) and (3.8) that

$$N_{\omega_x}^{+}/Z^{2n} = 1 - (\omega_x + A_1^2 - A_2 - N^2 + 1)/Z^2 - \omega_y/Z^3 + \cdots$$  \hspace{1cm} (3.9)$$

To complete the proof, we compare coefficients of $Z^{-2}$ and $Z^{-3}$ in (3.9) and apply (3.2a) and (3.3a).

Theorem 3.2. The class multiplier functions $\omega_x^+$ and $\omega_y^+$ for $G_n^+$ are

$$\omega_x^+ = \omega_x^+ - 2\omega_x^+ = (T/2)^2((N-1)(a_1 - 1) + a_2) - (T^2 - 2)/3 + \frac{1}{2}N(N+1)$$  \hspace{1cm} (3.10)$$

$$\omega_y^+ = 4(\omega_4^+ - \omega_4^+) = (T/2)^3((N-1)(a_1 - 1)(N + a_1) + a_1a_2 - a_3) + \frac{1}{2}N(N + a_1 - 1)$$

Proof: We replace $\omega_1$ by $\omega_x$, $A_1$ by $A_1^2$ and $\omega_\lambda$ by $\omega_x^+$ in (3.4) and (3.5), and note that $N_{\omega_x}^{+}/\omega_1 = (Z^2 + A_1Z - N)/(Z^2 - 1)$. Then

$$N_{\omega_x}^{+}/Z^{2n} = 1 - (\omega_x^+ + A_1^2 - 2A_2 - N(N-1)/2)/Z^2 - \omega_y/Z^3 + \cdots$$  \hspace{1cm} (3.12)$$

To complete the proof, we compare coefficients in (3.12), getting

$$\omega_x^+ = A_2 + (N-1)(N/2 + 1), \quad \omega_y^+ = A_3 - A_1A_2 - A_1N$$  \hspace{1cm} (3.13)$$

Finally, we apply (1.9) to get the pairs of class multipliers from which the character values $\chi_\lambda$ and $\chi_\lambda^+$ can be computed.

Reference


Michigan State University
East Lansing, Michigan
SUM FORM EQUATIONS ON AN OPEN DOMAIN I

L. Losonczi

Presented by J. Aczél, F.R.S.C.

Abstract. The general solution of the functional equation (1) is given on an open domain. This equation is connected to characterizations of the entropy of degree $\kappa$. The measurable solutions of (1) have recently been found by Kannappan and Sahoo [5].

1. Introduction

Let $\Gamma_n^0 = \{ P = (p_1, \ldots, p_n) \mid p_k > 0, \sum_{i=1}^{n} p_i = 1 \}$ be the set of all complete $n$-ary probability distributions with positive probabilities and let $\Gamma_n$ be the closure of $\Gamma_n^0$. The functional equation

$$\sum_{i=4}^{k} \sum_{j=4}^{k} f(p_i q_j) = \sum_{i=4}^{k} f(p_i) + \sum_{j=4}^{k} f(q_j) + \lambda \sum_{i=4}^{k} x(p_i) \sum_{j=4}^{k} f(q_j)$$

where $f: [0,1] \rightarrow \mathbb{R}$, $P \in \Gamma_n$, $Q \in \Gamma_n$, $\lambda = 2^{1-\kappa} - 1 \neq 0$ has been used to characterize the entropy of degree $\kappa$

$$H_{\kappa}^n(P) = (2^{1-\kappa} - 1)^{-1} (\sum_{i=4}^{n} p_i^\kappa - 1) \quad (\kappa \neq 1).$$

If $f$ is continuous and (1) holds for all $k, \ell \geq 2$ the solutions were given by Behara and Nath [2]. Equation (1) was solved by Kannappan [3], [4], Losonczi [6] under various regularity conditions while the general solution was found by Losonczi and Maksa [8]. Recently (1) has been studied by Kannappan and Sahoo [5] on the "open domain" i.e. in the case when the unknown function $f$ is defined on $(0,1)$ and (1) holds for $P \in \Gamma_n^0$, $Q \in \Gamma_n^0$. They found the measurable solutions supposed that $k, \ell \geq 3$ are fixed integers. For related equations on the open domain see e.g. [1], [9].

The aim of the present note is to find the general solution of (1) on the open domain.
2. Solution of (1) if $P \in (0,1)$

Introducing $g(p) = p + Xf(p)$, equation (1) goes over into

$$
\sum_{i=1}^{k} \sum_{j=1}^{l} \left[ g(p_i q_j) - g(p_i) g(q_j) \right] = 0 \quad (P \in \mathbb{Z}^0, Q \in \mathbb{Z}^0).
$$

The general solution of (2) is given by

**Theorem 1.** Let $k, l \geq 3$ be fixed integers. The function $g: (0,1) \to \mathbb{R}$ satisfies (2) if and only if either

(3) \hspace{1cm} g(p) = a(p) + b \quad p \in (0,1)

or

(4) \hspace{1cm} g(p) = A(p) + h(p) \quad p \in (0,1),

where $a, A: \mathbb{R} \to \mathbb{R}$ are additive functions with $A(1) = 0$, $h: (0,1) \to \mathbb{R}$ is a multiplicative function (that is $h(pq) = h(p)h(q)$ if $p, q \in (0,1)$) and $b$ is a constant such that

(5) \hspace{1cm} a(1) + kb = [a(1) + kb][a(1) + kb]

holds.

**Proof.** We follow the ideas of [8] with some modifications. We need the next lemma which is a special case of lemma 1 of Losonczi [7].

**Lemma.** Let $k \geq 3$ be a fixed integer, $c$ be a constant. The function $\phi: (0,1) \to \mathbb{R}$ satisfies the functional equation

(6) \hspace{1cm} \sum_{i=1}^{k} \phi(p_i) = c \quad (P \in \mathbb{Z}^0)

if and only if there exists an additive function $a: \mathbb{R} \to \mathbb{R}$ and a constant $b$ such that

(7) \hspace{1cm} \phi(p) = a(p) + b \quad p \in (0,1)

and

(8) \hspace{1cm} a(1) + kb = c

holds.

Since from (8) $b = a(-1/k) + c/k$ equation (7) can also be written as
Applying our lemma for the function

\[ \Phi(p,q_1,\ldots,q_\ell) = \sum_{j=1}^{\ell} [g(pq_j) - g(p)g(q_j)] \]

we obtain from (2)

\[ \sum_{j=1}^{\ell} [g(pq_j) - g(p)g(q_j)] = A_1(p-1/k,q_1,\ldots,q_\ell), \]

where \( A_1 : \mathbb{R}^\ell \rightarrow \mathbb{R} \) is an additive function in the first variable.

Let now \( P = (p_1,\ldots,p_\ell) \in \mathbb{R}^\ell \) and substitute in (10) \( pp_i \) for \( p \) \( i = 1,\ldots,\ell \). Adding the equations so obtained and using (10) again to calculate \( \sum_{i=1}^{\ell} g(pp_i) \), we get

\[ \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} [g(pp_iq_j) - g(p)g(pq_j)] = A_1(p-1/k,q_1,\ldots,q_\ell) + A_1(p-1/k,p_1,\ldots,p_\ell) \sum_{j=1}^{\ell} g(q_j). \]

The left hand side of (11) is symmetric in \( p_i,q_j \) therefore so is the right hand side:

\[ A_1(p-1/k,q_1,\ldots,q_\ell) + A_1(p-1/k,p_1,\ldots,p_\ell) \sum_{j=1}^{\ell} g(q_j) = A_1(p-1/k,q_1,\ldots,q_\ell) + A_1(p-1/k,p_1,\ldots,p_\ell) \sum_{i=1}^{\ell} g(p_i). \]

Putting here \( p = 1/k \) we conclude that

\[ A_1(1, q_1, \ldots, q_\ell) = \text{constant} = c_1. \]

Substituting (13) into (11) we have

\[ A_1(p, q_1, \ldots, q_\ell)(1 - \sum_{i=1}^{\ell} g(p_i)) + c_1/k \sum_{i=1}^{\ell} g(p_i) = A_1(p, p_1, \ldots, p_\ell)(1 - \sum_{j=1}^{\ell} g(q_j)) + c_1/k \sum_{j=1}^{\ell} g(q_j). \]

We shall distinguish two cases.

Case 1. If \( \sum_{i=1}^{\ell} g(p_i) = 1 \) for all \( p \in \mathbb{R}^\ell \) then by our lemma

\[ g(p) = a(p) + b \quad p \in (0,1) \]
i.e. (3) holds. This function satisfies (2) if and only if (5) is true.

**Case 2.** If there is a $P^*=(p_1^*,...,p_k^*) \in \Gamma_\ell^0$ such that $\sum_{i=4}^{\ell} g(p_i^*) \neq 1$
then with $P=P^*$ we obtain from (14)

$$A_1(p,q_1,...,q_k)=A(p)(1-\sum_{j=4}^{\ell} g(q_j))+d \sum_{j=4}^{\ell} g(q_j)+e,$$

where $A$ is an additive function and $d,e$ are constants. With $p=1$ we get
from (13), (15) that $A(1)=d$ thus (10) can be written as

$$\sum_{i=4}^{\ell} [g(pq_i)-g(p)g(q_i)]=A(p-1/k)(1-\sum_{j=4}^{\ell} g(q_j))+A(1) \sum_{j=4}^{\ell} g(q_j)+e.$$

Putting here $p=p_i (i=1,...,k)$ where $(p_1^*,...,p_k^*) \in \Gamma_\ell^0$ and adding the
equations so obtained we have by (2)

$$\sum_{i=4}^{\ell} \sum_{j=4}^{\ell} [g(p_iq_j)-g(p_i)g(q_j)]=0 =kA(1) \sum_{j=4}^{\ell} g(q_j)+ke$$

thus $A(1)=0,e=0$.

Returning to (16) we have

$$\sum_{i=4}^{\ell} [g(pq_i)-g(p)g(q_i)]=A(p)(1-\sum_{j=4}^{\ell} g(q_j))$$
or with $h(p)=g(p)-A(p), p \in (0,1)$.

$$\sum_{j=4}^{\ell} [h(pq_j)-h(p)h(q_j)]=0 \quad p \in (0,1), q=(q_1,...,q_k)e^{\Gamma_\ell^0}.$$

By the lemma,

$$h(pq)-h(p)h(q)=\xi(p,q-1/\ell) \quad p,q \in (0,1)$$

where $\xi:(0,1) \times R \rightarrow R$ is an additive function in the second variable.

For any $p,q,r \in (0,1)$ we have from (18)

$$h(pqr)-h(p)h(q)h(r)=
\xi(pq,r-1/\ell)+h(r)\xi(p,q-1/\ell)=\xi(p,qr-1/\ell)+h(p)\xi(q,r-1/\ell).$$

**Case 2.1.** If $\xi(p,q-1/\ell)=0$ for all $p,q \in (0,1)$ then (18) shows that
h is multiplicative and \( g(p) = h(p) + A(p) \) i.e. (4) holds. It is easy to check that (4) is a solution of (2) indeed.

**Case 2.2.** If there exist \( p^*, q^* \in (0,1) \) such that \( E(p^*, q^* - 1/\ell) \neq 0 \) then from (19)

\[
h(r) = \frac{1}{E(p^*, q^* - 1/\ell)} E(p^*, q^*/r - 1/\ell) + h(p^*) E(q^*, r - 1/\ell) - E(p^*, q^*, r - 1/\ell)
\]

which shows that

\[
h(r) = a_1(p) + b,
\]

where \( a_1 \) is additive on the triangle \( \{(p,q) \mid p,q,p+q \in (0,1)\} \) and \( b \) is a constant. \( a_1 \) can additively be extended to \( \mathbb{R} \) and

\[
g(p) = h(p) + A(p) = a_1(p) + A(p) + b = a(p) + b,
\]

where \( a(p) = a_1(p) + A(p) \) is an additive function again. Thus in this case (3) holds. \( \square \)

Returning to the original equation (1) we have

**Theorem 2.** The function \( f: (0,1) \rightarrow \mathbb{R} \) satisfies (1) for all \( p \in \Gamma_0 \) if and only if

\[
f(p) = \frac{a(p) - p + b}{\lambda} \quad p \in (0,1)
\]
or

\[
f(p) = \frac{A(p) - p + h(p)}{\lambda} \quad p \in (0,1),
\]

where \( a, A \) are additive functions, \( b \) is a constant, such that \( A(1) = 0 \) and (5) holds and \( h \) is a multiplicative function. \( \square \)
REFERENCES


Department of Mathematics
University of Lagos
Lagos, Nigeria (present address)

Department of Mathematics
L. Kossuth University
4010 Debrecen pf. 12, Hungary
(permanent address)

Received December 11, 1984.
1) Abstract

Given a field of algebraic functions $E$ with constant field $k$ and an $X \in E \setminus k$, one can deduce a paraphernalia of new objects, for example $K = k(X)$, $A = k[X]$ and $B$ the integral closure of $A$ in $E$.

$B$ is a Dedekind ring whose group of units will be denoted by $\mathcal{U}$, and the aim of the paper is to study the group $\mathcal{G} = \mathcal{U}_{k^*}$; first in general terms, then in a more constructive way in a particular case. Arithmetical applications could be given but would require more space.

2) Étude algébrique du cas général

Nous appellerons "place à l'infini" de $K$, la place constante sur $k$ qui envoie $1\over X$ sur $0$. Nous désignerons par $P_0, \ldots, P_{t-1}$ les places (non équivalentes) de $E$ qui la prolongent et par $\mathcal{M}$ le groupe $\mathbb{Z}P_0 + \ldots + \mathbb{Z}P_{t-1}$.

Théorème 1.- Soit $\varphi \in E$, les conditions suivantes sont équivalentes :

1) $\varphi \in \mathcal{U}$
2) $\mathcal{N}_{E/k} \varphi \in k^*$
3) $\text{div}(\varphi) \in \mathcal{M}$

Le groupe des diviseurs de $E$ est la somme directe de $\mathcal{M}$ et du sous-groupe $\mathcal{N}$ engendré par les autres places de $E$ et on désignera par $\pi_1$ et $\pi_2$ les projecteurs associés à cette décomposition en somme directe. On désignera aussi par $\mathcal{D}_0$ le groupe des diviseurs de degré zéro et on posera $\mathcal{M}_0 = \mathcal{N}_0 \cap \mathcal{M}$, $\mathcal{N}_0 = \mathcal{U}_0 \cap \mathcal{N}$. 
Théorème 2. — Soit $\mathcal{P}$ le groupe des diviseurs principaux de $E$, alors si l'on désigne par $\mathcal{C}_j$ le groupe $\mathfrak{H}/k^*$, on peut dire que :

1) $\mathcal{C}_j = \mathcal{M}_0 \cap \mathcal{P}$

2) Le groupe des classes d'idéaux de $B$ est isomorphe à $\mathfrak{H}/\pi_2(\mathcal{P})$.

Si l'on désigne par $J$ le groupe $\mathcal{D}/\mathcal{P}$ (jacobienne de $E$), par $J_\infty$ le sous-groupe $\mathcal{M}/\mathcal{M}_0 \mathcal{P}$ et par $T$ le sous-groupe de torsion de $J_\infty$, on a :

Corollaire

1) $\text{rang } (J_\infty /T) + \text{rang}(\mathcal{C}_j) = t-1$. En particulier si $k$ est fini, $\text{rang}(\mathcal{C}_j) = t-1$.

2) S'il existe un diviseur $P_1$ de degré 1, $i=0,\ldots,t-1$, alors le groupe des classes d'idéaux de $B$ est isomorphe à $J/J_\infty$.

Exemple. — Si $E = K(Y)$, avec $Y^P = D(X)$, $p$ premier avec le degré de $D(X)$, $J_\infty = \{0\}$.

Définition. — On dira que $\varphi \in B \setminus \{0\}$ est un "comma de $E$ relativement à $X$" (ou une "meilleure approximation" dans $B$) si $\varphi$ vérifie :

$$(\forall \varphi' \in B \setminus \{0\}, v_1(p) (\varphi') \geq v_1(p) (\varphi) \text{ pour } i=0,\ldots,t-1) \Rightarrow (\exists \lambda \in k^*, \varphi' = \lambda \varphi).$$

Alors, en utilisant Riemann-Roch, on démontre facilement le résultat suivant :

Propriété. — Toute unité de $B$ est un comma de $E$ relativement à $X$.

3) Étude analytique d'un cas particulier

a) On reprend $E = K(Y)$ avec $Y^P = D(X) \in A$, mais on suppose que $D(X)$ est un polynôme unitaire de degré $p^n$ (p n'est pas nécessairement premier). Si l'on suppose que la caractéristique de $k$ ne divise pas $p$, alors $Y^P = D(X)$ possède une solution $\Delta = X^{p^n} \ldots$ dans le corps des séries formelles $k((\frac{1}{X}))$. Si l'on suppose que $D(X)$ n'a pas de racine multiple dans une clôture algébrique $\bar{k}$ de $k$ et si l'on désigne par $\mu_p$ le groupe des racines $p$-ième de l'unité dans $\bar{k}$, on a la situation :
Nous poserons $G = \text{Gal}(k(\mu_p)/k) \cong (\mathbb{Z}/p\mathbb{Z})^2$. $G$ opère sur $\mu_p$ et on désigne par $d(k)+1$ le nombre d'orbites de $\mu_p$ pour l'action de $G$, alors on a :

**Théorème 3.**

1) La place à l'infini de $K$ se prolonge en $d(k)+1$ places (non équivalentes) dans $E$.

2) $B = A[Y] = k[X,Y]$

3) $\text{rang} G \leq d(k)$.

**Corollaire.** Si $d(k) = 1$ (c'est-à-dire $[k(\mu_p) : k] = p-1$, $\mathcal{O} = \{\overline{p}\}$ est soit trivial, soit cyclique infini.

b) **Définition des meilleures approximations** : Soit $U=(U_0, U_1, \ldots, U_{p-1}) \in \mathbb{A}^p$,

nous lui associerons $\varphi(U) = U_0 + U_1 \Delta + \ldots + U_{p-1} \Delta^{p-1} \in B$, et réciproquement. On écrira encore (en désignant par $\zeta$ un générateur de $\mu_p$):

$$\varphi_i(U) = U_0 + U_1 \zeta^i \Delta + \ldots + U_{p-1} \zeta^{i(p-1)} \Delta^{p-1} \in B(\mu_p)$$

et on utilisera les notations suivantes :

$$\text{deg } U = \text{Max } \text{deg } U_0, \text{deg } U_1 \Delta, \ldots, \text{deg } U_{p-1} \Delta^{p-1}$$

$$\Pi(U) = \text{deg } [\mathcal{O}_{E/K}(U)]$$

$$\phi_h(U) = \sum_{\zeta^i \in \omega_h} \text{deg } \varphi_i(U), \quad h = 0, \ldots, d(k)$$

où $\omega_0, \ldots, \omega_{d(k)}$ sont les orbites de $\mu_p$ sous l'action de $G$. 
On dira donc que $U \in \mathbb{A}^p$ est une meilleure approximation (ou m.a.) si $U \neq 0$ et si $U$ vérifie la propriété :

$$\{\forall U' \in \mathbb{A}^p, \ U' \neq 0, \ \forall h, \ 0 < h < d(k), \ \phi_h(U') < \phi_h(U)\} \Rightarrow \{\exists \lambda \in \mathbb{K}^*, \ U' = \lambda U\}$$

- dans le cas où $d(k) = 1$, la définition d'une m.a. entraîne :

$$(U \text{ est une m.a. et } \phi_o(U) < 0) \Leftrightarrow (\forall U' \neq \lambda U, \ \lambda \in \mathbb{K}^*, \ \phi_o(U') < \phi_o(U) < 0 \Rightarrow \deg U' > \deg U)$$

Construction des m.a. $\varphi(U)$ telles que $\phi_o(U) < 0$ sous l'hypothèse $p$ premier et $[k(p_\ell), k] = p^{-1}$

Soit $q$ un entier supérieur ou égal à 1. On pose :

$$U_i = u_i (0)^q x^{in} + u_i (1)^q x^{in-1} + \cdots + u_i (q-in), \quad 0 \leq i \leq p-1$$

$$A^i = x^{in} + a_i (1)^q x^{in-1} + \cdots + a_i (in), \quad 1 \leq i \leq p-1$$

On considère la matrice $A_q$ ayant $q$ colonnes, formée des blocs

<table>
<thead>
<tr>
<th>$q+1$</th>
<th>$q-n+1$</th>
<th>$q-(p-1)n+1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 0, ..., 0</td>
<td>1, 0, ..., 0</td>
<td>1, 0, ..., 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$a_1 (1), 1, ..., 0$</td>
<td>$a_1 (1), 1, ..., 0$</td>
<td>$a_1 (1), 1, ..., 0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$a_1 (1), 1, ..., 0$</td>
<td>$a_1 (1), 1, ..., 0$</td>
<td>$a_1 (1), 1, ..., 0$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$B^{(0)}_{1, q}$</td>
<td>$B^{(1)}_{1, q}$</td>
<td>$B^{(p-1)}_{1, q}$</td>
</tr>
</tbody>
</table>
Soit $\mathcal{U}^* = \langle \mathcal{U}_0 \rangle \ldots \langle \mathcal{U}_{q-1} \rangle$, soit $A^*$ la matrice tronquée, ayant comme $m$ lignes, les $m$ premières lignes de $A_{q,m}$. Soit $m$ le plus grand entier tel que le système $A_{q,m-1} \mathcal{U}^* = 0$, admette une solution non triviale.

**Théorème 4.** - "La" solution, définie à une constante multiplicative près, du système $A_{q,m-1} \mathcal{U}^* = 0$ est une m.a. de degré inférieur ou égal à $q$.

- Réciproquement toute m.a. $\mathcal{U}$ avec $\phi_0(\mathcal{U}) < 0$ est construite de cette façon.

- De plus, pour toute m.a. $\mathcal{U}$, on a $N(\mathcal{U}) < g$, où $g$ est le genre de la courbe $X^p = D(X)$.

En faisant varier $q$ de 1 à l'infini, on obtient la suite des m.a. $(U^{(i)})_{i \geq 1}$ non deux à deux équivalentes telle que la suite $(\deg(U^{(i)}))_{i \geq 1}$ soit strictement croissante et la suite $(\phi_0(U^{(i)}))_{i \geq 1}$ soit strictement décroissante. On dira que $U^{(i)}$ est une m.a. de rang $i$.

**Définitions 1.** - Soient $\varphi$ et $\psi$ deux éléments de $E^*$, on dit que $\varphi$ est équivalent à $\psi$ s'il existe $\lambda$ appartenant à $k^*$ tel que $\varphi = \lambda \psi$, on note $\varphi \sim \psi$.

2. - On dit que la suite des m.a. est purement pseudo-périodique si la suite $a_i = \frac{\varphi(U^{(i+1)})}{\varphi(U^{(i)})}$ est telle qu'il existe $\pi > 1$, $a_{q \pi + r} \sim a_r$.

$\forall q > 0$, $0 < r < \pi - 1$. 
Théorème 5. — \( \mathcal{C} \) est non trivial si et seulement si la suite des m.a. est purement pseudo-périodique.

Théorème 6. — Si \( P_0 \) (resp. \( P_1 \)) désigne la place associée à la valuation définie par \( v_0(\varphi(U)) = -\varphi_0(U) \) (resp. \( v_1(\varphi(U)) = -\varphi_1(U) \)).

1) \( \mathcal{C} \) est non trivial si et seulement si \((p-1)P_0 - P_1\) est un élément d'ordre fini \( \ell \) de la jacobienne \( J \).

2) De plus, on a :
   a) \( \ell = \deg U^{(n)} \), où \( U^{(n)} \) est la m.a. de rang \( n \), \( n \) étant la pseudo-période de la suite des m.a.
   b) i) Si \( p = 2 \), \( n+1 < \ell < 1+n(n-1) \)
   ii) Si \( p > 3 \),
   \( n+1 < \ell < n + \left\lfloor \frac{p+1}{2} \right\rfloor (n-1) \) si \( n < p-1 \)
   \( n+1 < \ell < n + \left\lfloor \frac{p+1}{2} \right\rfloor (n-1) \) si \( n > p-1 \)

Corollaire. — Si \( p = 2 \) et \( n = 2 \), \( \ell = n+1 \); Si \( p = 3 \) et \( n = 1 \), \( \ell = n \).

REFERENCES


Y. Hellegouarch, R. Paysant-Le Roux - Université de CAEN, FRANCE
D.L. Mc Quillan - University College, DUBLIN

Received December 17, 1984.
THE INDEX OF ELLIPTIC OPERATORS ON A MAPPING TORUS

B. Booss and K. Wojciechowski

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

The purpose of this paper is to give a new formula for the index of an elliptic operator on a mapping torus and to explain its topological meaning. All technical details and several extensions have been described in the paper [8] by the second author who treats a more general situation. A simpler case is discussed in [4] where one can find the original ideas which led us to the study of operators of this type.

1. The formulation of the main theorem. Let \( Y \) be a closed smooth manifold of dimension \( n \); \( E, F \) vector bundles over \( Y \). Let \( \Phi_E, \Phi_F \) be diffeomorphisms of \( E, F \) giving on each fibre a linear isomorphism (possibly onto the fibre over another point of \( Y \)) and defining the same diffeomorphism of the base \( Y \); i.e. we have a commutative diagram

\[
\begin{array}{ccc}
\Phi_E & : & \begin{array}{cc}
E & \rightarrow \ E \\
Y & \rightarrow \ Y
\end{array} \\
\Phi_F & : & \begin{array}{cc}
F & \rightarrow \ F \\
Y & \rightarrow \ Y
\end{array}
\end{array}
\]

(1.1)

Under these assumptions we can construct the mapping torus, namely the manifold

\[
Y^f = I \times Y / f
\]

where we identify \( (l,y) \sim (0,f(y)) \), and the bundles

\[
E^\Phi = I \times E / \Phi \quad \text{and} \quad F^\Phi = I \times F / \Phi.
\]

Any first order elliptic differential operator

\[
A : C^\infty(Y^f; E^\Phi) \rightarrow C^\infty(Y^f; F^\Phi)
\]

takes the form
\[ \alpha(t,y) \left( \frac{\partial}{\partial t} + B(t,y) \right) \]

where \( \alpha(t,y) : E \to F \) is a bundle isomorphism and
\( B(t,\cdot) : \mathcal{C}^0(\gamma, E) \to \mathcal{C}^0(\gamma, E) \) is a smooth family of elliptic operators acting on sections of \( E \). Actually, without loss of generality we can assume that \( A \) takes the form
\[ (1.3) \quad \alpha \left( \frac{\partial}{\partial t} + B_t \right) \]
where \( \alpha \) is an isomorphism which doesn't depend on \( t \), and
\( B_t \) is a family of elliptic operators with the same principal symbol
\[ \sigma_L(B_t) = \sigma. \]

From the formulas (1.2), (1.2') we deduce
\[ \text{As}(1,y) = \Phi_F(\text{As}(0,y)) \]
for any section \( s \) of \( B^0 \) \( (s(1,y) = \Phi_E s(0,y)) \).

Using (1.3) we get the following conditions
\[ (1.4) \quad \Phi_F = \alpha \circ \Phi_E \quad \text{and} \quad B_1 = (\Phi_E)^{-1} B_0 \Phi_E. \]

For the principal symbol of \( B_t \) this means exactly
\[ (1.5) \quad \Phi_E(y) \sigma(y, \zeta) v = \sigma(f(y), (f^{-1})^* \zeta) \Phi_E(y) v \]
where \( \zeta \in \mathfrak{T}_Y, v \in E_y \).

We consider operators of the form (1.3) where \( B_t \) is an elliptic pseudodifferential operator of order 1 such that (1.4) and (1.5) are fulfilled. Operators of that type appear naturally in topological research ([1], [5]), and in many cases their index has deep topological meaning. Mapping tori appear also in Gauge Theory (Euclidean box with periodic boundary conditions, cf. [2], [6]). The natural question in this situation is whether it is possible to reduce the computation of the index of \( A \) to the manifold \( Y \).

The answer has rather negative character, and we will show in a transparent way that the index depends non-trivially on the diffeomorphism \( f \).
Now, let \( B_\epsilon \) be an elliptic operator with a principal symbol which has no imaginary eigenvalues (as a linear transformation of \( E_y \) in each \( y \)). Hence \( B_\epsilon \) has a discrete spectrum and only finitely many eigenvalues in the region \( S \) of Fig. 1.6 for sufficiently small \( \epsilon, \theta \) (see e.g. [7]), and therefore we can assume that \( B_\epsilon \) has no eigenvalues on the imaginary axis.

We denote by \( P_+ (P_-) \) the spectral projection onto the direct sum of the eigenspaces of \( B_\epsilon \) corresponding to the eigenvalues with positive real part (respectively negative real part).

Our main theorem is

**Theorem 1.** The operator \( P_+ - \Phi_E P_- \) acting on sections of \( E \) is a Fredholm operator and one gets

\[
(1.7) \quad \text{index } (P_+ - \Phi_E P_-) = \text{index } A.
\]

2. Corollaries and remarks. (I) \( P_+ , P_- \) are pseudodifferential operators of order 0 [8], but \( P_+ - \Phi_E P_- \) can be non-pseudolocal if \( f \neq \text{id} \). However, if \( f = \text{id} \) then \( Y^f = S^1 \times Y \) and \( \Phi_E \) is a bundle automorphism. In that case we get a pseudodifferential operator and its index is given by the Atiyah-Singer formula. In fact, the principal symbol \( p_+ \) of \( P_+ \) is in each point \( (y, \xi) \) (\( \xi \) is an element of \( S_y \) where \( S_Y \) is the cotangent sphere bundle) the projection onto the direct sum of the eigenspaces of the linear transformation \( \sigma(y, \xi) : E_y \rightarrow E, \) corresponding to the eigenvalues with positive (respectively negative) real part. So \( p_- \) determines a bundle \( E_- \) which is a subbundle of \( \pi^*E \) where \( \pi : S_Y \rightarrow Y \) is the projec-
tion. Now \( \Phi_F \) commutes with \( \sigma \) so it commutes with its spectral projections

\[
\Phi_E(y) P_\pm(y, \xi) = P_\pm(y, \xi) \Phi_E(y),
\]

hence it gives an automorphism of \( E_- \) and determines an element \([E_-, \Phi_E] \in K^{-1}(SY)\). If \( f = \text{id} \) then the final formula is \(([4], [8])\)

\[
(2.2) \quad \text{index } (P_+ - \Phi_E P_-) = \text{t-ind}[E_-, \Phi_E] = \text{ch}[E_-, \Phi_E] \pi^* \tau(Y) [SY].
\]

It is only an exercise in algebraic topology to see that the last expression is equal to \( \text{t-ind } \sigma_L(A) \).

(II) We meet here a pair of projections in \( L^2(Y; E) \) such that \( P_+ + P_- = \text{id} \), \( P_- P_+ = P_+ P_- = 0 \). The set of all linear automorphisms \( \psi \) of \( L^2 \) such that \( P_+ - \psi P_- \) is Fredholm is also very interesting from a topological point of view. It is proved in \[4\], \[8\] that it is a classifying space for the functor \( K \).

(III) If \([E_-, \Phi_E] \) or \([E, \Phi_E] \) (as an element of \( K^{-1}(Y) \) or \( K(Y^f) \)) is a torsion element of the respective \( K \)-group then it is clear from (2.2) that the index has to vanish. We present the simplest case of this situation:

**Corollary 2.** If \( \Phi_E^k = \text{id} \) for some integer \( k \), then

\[
\text{index } (A) = 0.
\]

**Proof.** \( (P_+ - \Phi_E P_-)^{2k} = P_+ + P_- + \Sigma P_+ \Phi_E P_- \ldots = \text{id} + \Sigma P_+ \Phi_E P_- \ldots = \text{id} + \text{comp. op.} \)

because \( P_+ \Phi_E - \Phi_E P_+ = \Phi_E (\Phi_E^{-1} P_+ \Phi_E - P_+) \) and \( \Phi_E^{-1} P_+ \Phi_E - P_+ \) is a pseudodifferential operator of order -1 hence compact (from 2.1) we see that the 0-order term of the symbol of \( \Phi_E^{-1} P_+ \Phi_E - P_+ \) vanishes). Hence

\[
2k \text{index}(P_+ - \Phi_E P_-) = \text{index}(P_+ - \Phi_E P_-)^{2k} = \text{index} (\text{id} + \text{comp.}) = 0.
\]
3. Proof of Theorem 1. It is easy to check

\[
\text{index}(P_+ - \Phi_E P_-) = \dim \{ f \in \text{Range } P_- \mid \Phi_E f \in \text{Range } P_+ \} - \dim \{ f \in \text{Range } P_+ \mid \Phi_E f \in \text{Range } P_- \}.
\]

This last number is called the spectral flow of the family \( \{B_t\}_{t \in I} \) since it is equal to the difference between the number of eigenvalues of \( B_t \) where their real parts change the sign from \(-\) to \(+\) when \( t \) goes from 0 to 1 and the number of eigenvalues of \( B_t \) with real parts changing the sign from \(+\) to \(-\). We denote it by \( \text{sf}(B_t) \). This concept was used by Atiyah, Patodi and Singer in [1], part III. Now \( \Phi_E^{-1} B_1 \Phi_E = B_1 \), so \( \{B_t\} \) is a periodic family. The spectral flow is a homotopy invariant of such families with values in the integers. There is also another homotopy invariant of the family \( \{B_t\} \), the analytical index \( \text{index}(B_t) \). We will describe it very briefly: Let \( \{B_t\} \) denote a family of Fredholm operators over \( S^1 \times S^1 \)

\[
B_{s,t} = \left\{ \begin{array}{ll}
1 \cos(s) + \sin(s) & 0 \leq s < \pi \\
e^{i(s+\pi/2)} & \pi \leq s < 2\pi
\end{array} \right.
\]

Remark: Instead of \( B_{s,1} = B_{s,o} \), we have of course

\[
B_{s,1} = \Phi_E^{-1} B_{s,o} \Phi_E,
\]

but this is not a problem for operators on \( L^2(Y;E) \) since the group of linear invertible transformations of it is contractible and we always can find a family \( \{\psi_t\} \) of automorphisms of \( L^2 \) with \( \psi_1 = \text{id} \) and \( \psi_0 = \Phi_E \) thus connecting \( \{B_{s,t}\}_{t \in I} \) with a true family over \( S^1 \) using a family of operators which have the same spectrum as \( B_1 \) and \( B_0 \).

Recall that for any compact space \( A \) and any closed subspace \( B \) the group \( K(A/B) \) is equal to the group of homotopy classes of families of Fredholm operators which are invertible over \( B \). Hence \( \{B_{s,t}\} \) determines an element of

\[
K(S^1 \times S^1/S^1) \cong K^{-1}(S^1) \cong \mathbb{Z}
\]

which we call the analytical index of the family \( \{B_t\} \).

In fact it is equal to the spectral flow of the family ([1],
We obtain the value of that index from the Atiyah-Singer theorem for families [2]. Then Theorem 1 is a corollary of the following

**Theorem 3.** \( \text{index } A = \text{index } \{ B \} \).

**Proof.** We have to compare the index formula for one operator on \( Y \) with the cohomological formula for the families, [2], th. 5.1. In fact they are equivalent since the symbol of \( A \) is, up to small continuous deformations, equal to the principal symbol of the family given by the formula (3.2) (see also [1], part III, section 7 and [8]).

**References**


Received January 2, 1985.
<table>
<thead>
<tr>
<th>Mailing Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. T. Agoh</td>
</tr>
<tr>
<td>Department of Mathematics</td>
</tr>
<tr>
<td>Science University of Tokyo</td>
</tr>
<tr>
<td>Noda, Chiba 278, Japan</td>
</tr>
<tr>
<td>2. D. Betten</td>
</tr>
<tr>
<td>Mathematisches Seminar der</td>
</tr>
<tr>
<td>Universität Kiel</td>
</tr>
<tr>
<td>Olshausenstrasse 40</td>
</tr>
<tr>
<td>D-2300 Kiel, F.R. Germany</td>
</tr>
<tr>
<td>3. T. Bisztriczky</td>
</tr>
<tr>
<td>Department of Mathematics</td>
</tr>
<tr>
<td>University of Calgary</td>
</tr>
<tr>
<td>Calgary, Alberta, Canada T2N 1N4</td>
</tr>
<tr>
<td>4. B. Booss</td>
</tr>
<tr>
<td>Institut for Studiet af Matematikog Fysik</td>
</tr>
<tr>
<td>Roskilde Universitetscenter</td>
</tr>
<tr>
<td>DK-4000 Roskilde</td>
</tr>
<tr>
<td>5. R. Carroll</td>
</tr>
<tr>
<td>Mathematics Department</td>
</tr>
<tr>
<td>University of Illinois</td>
</tr>
<tr>
<td>Urbana, IL 61801, U.S.A.</td>
</tr>
<tr>
<td>6. J.S. Frame</td>
</tr>
<tr>
<td>Department of Mathematics</td>
</tr>
<tr>
<td>Michigan State University</td>
</tr>
<tr>
<td>East Lansing, MI 48823, U.S.A.</td>
</tr>
<tr>
<td>7. A. Granville</td>
</tr>
<tr>
<td>Department of Mathematics and Statistics</td>
</tr>
<tr>
<td>Queen's University</td>
</tr>
<tr>
<td>Kingston, Ontario, Canada K7L 3N6</td>
</tr>
<tr>
<td>8. Y. Hellegouarch</td>
</tr>
<tr>
<td>Département de Mathématiques</td>
</tr>
<tr>
<td>Université de Caen</td>
</tr>
<tr>
<td>Caen, France</td>
</tr>
<tr>
<td>9. I. Hughes</td>
</tr>
<tr>
<td>Department of Mathematics and Statistics</td>
</tr>
<tr>
<td>Queen's University</td>
</tr>
<tr>
<td>Kingston, Ontario, Canada K7L 3N6</td>
</tr>
<tr>
<td>Faculty of Mathematics</td>
</tr>
<tr>
<td>University of Waterloo</td>
</tr>
<tr>
<td>Waterloo, Ontario, Canada N2L 3G1</td>
</tr>
<tr>
<td>11. I. Kersten</td>
</tr>
<tr>
<td>NWF-I Mathematik</td>
</tr>
<tr>
<td>Universitätstr. 31</td>
</tr>
<tr>
<td>D-8400 Regensburg, W.-Germany</td>
</tr>
<tr>
<td>12. P. Lentoudis</td>
</tr>
<tr>
<td>Université de Patras</td>
</tr>
<tr>
<td>Département de Mathématiques</td>
</tr>
<tr>
<td>Patras - Greece</td>
</tr>
<tr>
<td>13. L. Losonczi</td>
</tr>
<tr>
<td>Department of Mathematics</td>
</tr>
<tr>
<td>University of Lagos</td>
</tr>
<tr>
<td>Lagos, Nigeria</td>
</tr>
<tr>
<td>14. D.L. McQuillan</td>
</tr>
<tr>
<td>Department of Mathematics</td>
</tr>
<tr>
<td>University College</td>
</tr>
<tr>
<td>Dublin, Ireland</td>
</tr>
</tbody>
</table>
15. J. Michaliček                          Mathematisches Seminar
                                         Bundesstr. 55
                                         D-2000 Hamburg 13, W.-Germany

16. M. Oudadess                           Ecole Normale Supérieure Takaddoum
                                         Avenue Oued Akreuch
                                         B.P. 5118, Rabat, Maroc

17. R. Paysant-le Roux                   Département de Mathématiques
                                         Université de Caen
                                         Caen, France

18. P. Ribenboim                          Department of Mathematics and Statistics
                                         Queen's University
                                         Kingston, Ontario, Canada K7L 3N6

19. P.K. Sahoo                            Faculty of Mathematics
                                         University of Waterloo
                                         Waterloo, Ontario, Canada N2L 3G1

20. P. Scherk                             Department of Mathematics
                                         University of Toronto
                                         Toronto, Ontario, Canada M5S 1A1

21. P. Thurnheer                          Englischviertelstr. 17
                                         8032 Zürich, Switzerland

22. C. Weigand                            Mathematische Seminar du
                                         Universitität Kiel
                                         Olshausenstrasse 40
                                         D-2300 Kiel, F.R. Germany

23. K. Wojciechowski                      Instytut Matematyczny
                                         Uniwersytet Warszawski
                                         PL-00-901 RKiN, Warszawa, Poland