C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No., 1, February 1985 février

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 1, February 1985 février

Memoirs - Mémoires

From time to time Mathematical Reports will publish longer (maximum 20 pages) survey articles by Fellows, reporting also on their own research. These are meant to correspond to inaugural lectures traditionally presented by fellows of other national Academies. Our programme of short notes written or presented by Fellows remains unchanged.

De temps en temps, les Comptes Rendus Mathématiques publieront des articles plus longs (20 pages au plus) des membres de l'Académie, incluant une description de leurs propres recherches. Ceci tient le rôle des leçons inaugurales, qui sont traditionnellement présentées par les membres d'autres académies nationales. Notre programme de notes courtes écrites ou présentées par les membres reste inchangé.

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 $\mathfrak{p}$ of A, with Zariski's topology. The sheaf of rings has stalk at $\mathfrak{p}$ equal to the localization of A at $\mathfrak{p}$.

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 [6]).

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.

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

Let $(G'_{i'})_{i'\in I'}$, $\phi_{i'j'}$, $\mathbf{G}'$, π' be given similarly.

A map $\mu: \mathbf{G} \to \mathbf{G}'$ is *compatible* when it satisfies:

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

$$\begin{array}{ccc} & \mu & \\ \mathbf{G} & \to & \mathbf{G}' \\ \pi \downarrow & & \downarrow \pi' \\ I & \to & I' \\ & \underline{\mu} & \end{array}$$

2) $\underline{\mu}$ preserves the order.

If $\mu: \mathbf{G} \to \mathbf{G}'$, $\mu': \mathbf{G}' \to \mathbf{G}''$ are compatible, so is $\mu'\circ\mu$ and $\underline{\mu'\circ\mu} = \underline{\mu'}\circ\underline{\mu}$.

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

If $\mu: \mathbf{G} \to \mathbf{G}'$, $\mu': \mathbf{G}' \to \mathbf{G}''$ 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 $\mu: \mathbf{G} \to A$ is a mapping such that if $\pi(g) = \pi(h)$ then $\mu(gh) = \mu(g)\mu(h)$.

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

If $\mu: \mathbf{G} \to \mathbf{G}'$, $\mu': \mathbf{G}' \to \mathbf{G}''$ are isomorphisms so are $\mu'\circ\mu$ and the inverse map $\mu^{-1}: \mathbf{G}' \to \mathbf{G}$.

A homomorphism $\mu: \mathbf{G} \to \mathbf{G}$ is called an *endomorphism* of $\mathbf{G}$. An isomorphism from $\mathbf{G}$ to $\mathbf{G}$ is called an *automorphism* of $\mathbf{G}$. Let $\mathrm{Aut}(\mathbf{G})$ denote the group of automorphisms of $\mathbf{G}$.

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

(1) If $\pi(g) = \pi(h)$ then $\tau_{gh} = \tau_g \circ \tau_h$,

(2) If 1_i is the unit element of G_i then τ_{1_i} is the identity automorphism of $\mathbf{G}$,

(3) If $g \in G_i$ then $\tau_{g \mid G_i}$ is the inner automorphism of G_i defined by g (hence $\underline{\tau_g}(i) = i$),

(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 $\underline{\tau_g}$ is the identity map of I, for every $g \in \mathbf{G}$, 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 ϕ_{ij} to be the inclusion map. Let $\mathbf{G} = \coprod_{i \in I} G_i$. For each $i \in I$, $g \in \mathbf{G}$ *assume* that there exists $j \in I$ (necessarily unique) such that $g^{-1} G_i g = G_j$. Let $\underline{\tau_g}: I \to I$ be defined by $\underline{\tau_g}(i) = j$ and let $\tau_g: \mathbf{G} \to \mathbf{G}$ be given by the conjugation by g, that is, if $h \in G_i$ then $\tau_g(h) = g^{-1} h g \in G_{\underline{\tau_g}(i)}$ thus τ 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 $\mathbf{P}$ of all primary subgroups (i.e. having prime-power order); or the family $\mathbf{S}$ of all Sylow subgroups; or the family $\mathbf{M}$ 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 $g \in \mathbf{G}$ the mapping $\underline{\tau_g}$ is the identity map of I, that is the action τ 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 $K \mid \mathbb{Q}$ be a Galois extension, $G = \mathrm{Gal}(K \mid \mathbb{Q})$. For each prime ideal $\mathfrak{p}$ of the ring of integers of K let $D_{\mathfrak{p}} = \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$ be the corresponding decomposition group. Let $\mathbf{D} = (D_{\mathfrak{p}})_{\mathfrak{p}}$ 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 $((G_i)_{i \in I}, \tau)$ be an active family of groups. Then there exists a unique group A and a homomorphism ρ: $\mathbf{G} \to A$ (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 $g \in \mathbf{G}$ the following diagram is commutative:

$$\begin{array}{ccc} & {\scriptstyle \tau_g} & \\ \mathbf{G} & \longrightarrow & \mathbf{G} \\ {\scriptstyle \rho}\downarrow & & \downarrow{\scriptstyle \rho} \\ A & \longrightarrow & A \\ & {\scriptstyle \iota_{\rho(g)}} & \end{array}$$

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

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

A, ρ are unique up to a unique isomorphism; A is called the *active sum* of the given active family of groups.

If the action τ 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 $A = \boxplus_{i \in I} G_i$ (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

$$\begin{cases} [g]^{-1}[h][g][\tau_g(h)]^{-1}, & \forall g,h \in \mathbf{G} \\ [\phi_{ij}(g)][g]^{-1}, & \forall g \in G_i,\ i \leq j \end{cases}$$

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

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 $A = \boxplus_{i\in I} G_i$ is a finite group with order at most $\prod_{i\in I} \#(G_i)$. Moreover if the action is normal then $\#(A)$ divides $\prod_{i\in I} \#(G_i)$. 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 $\rho: \mathbf{G} = \coprod_{i\in I} G_i \to A = \boxplus_{i\in I} G_i$ let $\tau: \mathbf{G} \to G$ be the homomorphism induced by the inclusions $G_i \subseteq G$. By the universal property, there is a unique homomorphism $\psi: A \to G$ such that $\psi\circ\rho = \iota$. Then ψ is surjective if and only if $\bigcup_{i\in I} G_i$ generates G.

Taking G to be a finite group and $(G_i)_{i\in I} = \mathbf{P}$ (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 $G = \boxplus\mathbf{P} \xrightarrow[\psi]{\sim} G$.

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 $\mathbf{P}$ of finite primary groups, there exists a finite group G with this family $\mathbf{P}$ of primary groups and action given by conjugation.

The preceeding main theorem does not hold in general for the family $\mathbf{S}$ of Sylow subgroups. For example, if $G = S_4$ (symmetric group in 4 letters), then $\boxplus\mathbf{S} = G \times C_2$ 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 $\mathbf{A}$ of atomic subgroups stable under conjugation such that the canonical homomorphism $\psi: \boxplus\mathbf{A} \to G$ is an iso-

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 $\mathbf{D} = (D_p)_p$ 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 $\bigcap_p D_p = \{1\}$ and also that $\bigcup_p D_p$ is a dense subset of $G = \mathrm{Gal}(K \mid K_0)$. Then $\psi\colon \boxplus \mathbf{D} \to G$ is surjective.

All the above concepts and results are fully explained and developed in the papers [6] 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 (Kontorovič, 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 Π be any set of prime numbers, and let G be a group.

(1) G is a *U_Π-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_Π-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_Π-group* when it is a U_Π-group group and a E_Π-group.

If Π is the set of all prime numbers then U_Π-groups were called R-groups by Kontorovič and E_Π-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 $Y_1,...,Y_n,X$.

For every group G, consider the set

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

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 $W_G = \{X^m g^{-1} \mid g \in G, m \in S\}$.

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 $Y_1,...,Y_n,X$.

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 Π is any set of prime numbers, then G is W-complete exactly if it is a E_Π-group and G is W-perfect when it is a D_Π-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,ϕ^W) with

(1) G^W is a W-perfect group $\phi^W\colon G \to G^W$ is a homomorphism.

(2) If H is a W-perfect group and $\psi\colon G \to H$ is a homomorphism then there eixsts a unique homomorphism $\psi^W\colon G^W \to H$ 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:

$$W = W_S = \{X^s Y^{-1} \mid s \in S\} \quad \text{where} \quad S \subseteq \{1,2,3\},$$

or more particularly, $W = W_\Pi$ where Π is a set of prime numbers.

If Π' is the complement of Π in the set of all prime numbers, then the Π'-perfection of G has been called the *Π-localization* of G, explicitly denoted by (G_Π,ϕ_Π). It has the following properties:

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

(2) the analogous universal property.

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

The existence of Π-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 Π-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 $p \in \Pi$, $g \in G$ let $X_{g,p}$ be a symbol, let $F = F(X_{g,p})$ be the free group generated by these symbols and consider the free product $G^*F(X_{g,p})_{g,p}$. Let R be the normal subgroup generated by all elements $X_{g,p}^p g^{-1}$. Thus in G^*F/R every $g \in G$ has a p-th root in G^*F, however it is not necessarily unique.

The Π-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 Π is a set of prime numbers, an element $y \in K$ is an *element of torsion-type* relative to H (and Π) if there exists elements $h_1,h_2 \in H$, $k_1,k_2 \in K$ such that $y = k_1k_2^{-1}$ and $k_1^p h_1 = h_2 p_2^p$. 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 $T_\Pi(K,H) = T(H) = \bigcup_{i=1}^{\infty} T_i(H)$. $T_H(K,H)$ is a normal subgroup of K called the *Π-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 *Π-torsion free* when $T_\Pi(K,\{1\}) = \{1\}$. Thus, if H is a normal subgroup of K, then $K/T_\Pi(K,H)$ is Π-torsion free; etc.

Now, I return to the construction of the Π-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 $G^\Pi = \varinjlim G^i$, with obvious homomorphism $\phi^\Pi: G \to G^\Pi$. This is the Π-perfection of G.

The construction of the Π-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 Π-localization, the theory has been developed (see for example Hilton, Mislin and Roitberg, Warfield) in a different way. If $N \in \mathbf{N}_c$ (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 $N' \in \mathbf{N}_{c-1}$. By induction on c, the Π-localizations A_Π, N'_Π are known and N_Π is obtained by taking the central extension defined by A_Π, N'_Π and the cocycle which served to define N, so that the following diagram is commutative

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

In my own construction, it follows from a theorem of Černikov that if $N \in \mathbf{N}_c$ if $N^{I\Pi}$ is the Π-perfection of N, then in fact $N^{I\Pi} \in \mathbf{N}_c$, and so $N^{I\Pi}$ 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 $\bigcap_{i \in I} \mathrm{Ker}(\phi^{\Pi_i}) = \{1\}$, where $\phi^{\Pi_i} \colon G \to G^{\Pi_i}$ is the Π-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

[1] Baumslag, G., *Some aspects of groups with unique roots.* Acta Math. *104* (1960), 217-303.

[2] Birkhoff, G., *On the structure of abstract algebras.* Proc. Cambridge Phil. Soc. *31* (1935), 433-354.

[3] Herfort, W. and Ribenboim, P., *Localization of profinite groups.* Arch. Math. *42* (1984), 1-15.

[4] Hilton, P., *Nilpotente Gruppen und nilpotente Räume.* Lecture Notes in Math., No. 1053. Springer, New York, 1984.

[5] Hilton, P., Mislin, G., and Roitberg, J., *Localization of nilpotent groups and spaces.* North Holland Publ. Co., Amsterdam, 1975.

[6] Ribenboim, P., *Active sums of groups.* J. Reine Angew. Math. *325* (1981), 153-182.

[7] Ribenboim, P., *Active sums of profinite groups.* Bol. Soc. Bras. Mat. *14* (1983), 125-132.

[8] Ribenboim, P., *Equations in groups, with special emphasis on localization and torsion.* To appear in Mem. Accad. Lincei.

[9] Warfield, R.B., *Nilpotent groups.* Lecture Notes in Math. No. 513, Springer, New York, 1976.

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

Received November 10, 1984.

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 1, February 1985 février

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

$$B_m + \sum_{\substack{p-1 \mid m \\ p:\text{prime}}} \frac{1}{p} \in \mathbb{Z}.$$

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

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

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

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

In particular, if $p - 1 \nmid m$, then

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

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 $\operatorname{ord}_p(r)$ to be the exponent of the highest power of p that divides the integer r. Suppose that

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

is the decomposition of $n > 0$ into the prime divisors. And, let

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

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

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

$$\prod_{p \in S(n)} (1 - p^{m-1})(a^m - 1) \beta_m \equiv a^{m-1} \sum_{\substack{1 \leq j \leq w-1 \\ (j,n)=1}} j^{m-1} [ja/w] \pmod{n}. \tag{4}$$

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

$$(a^m - 1) N_m \equiv m a^{m-1} D_m \sum_{j=1}^{w-1} j^{m-1} [ja/w] \pmod{w}. \tag{5}$$

If $p^t \mid m$ and $p-1 \nmid m$, then $p \nmid D_m$, 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 $\operatorname{ord}_p(D_m) = 1$. 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:

$$(a^m - 1) \beta_m \equiv a^{m-1} \sum_{j=1}^{w-1} j^{m-1} [ja/w] \pmod{n}. \tag{6}$$

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

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

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

$$\begin{aligned} \sum_{j=1}^{w-1} j^{m-1} [ja/w] &= \sum_{\substack{1 \le j \le w-1 \\ (j,n)=1}} j^{m-1} [ja/w] + \sum_{\substack{1 \le j \le w-1 \\ (j,n) \ne 1}} j^{m-1} [ja/w] \\ &= \sum_{\substack{1 \le j \le w-1 \\ (j,n)=1}} j^{m-1} [ja/w] + \sum_{k=1}^{s} \sum_{I \in P_k} T_I. \end{aligned} \tag{7}$$

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

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

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

$$(-1)^{\eta(I)-1} \prod_{i \in I} p_i^{m-1} (a^m - 1) \beta_m \equiv a^{m-1} T_I \pmod{n}. \tag{8}$$

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

$$\{1 + \sum_{k=1}^{s} (-1)^k \sum_{I \in P_k} \Big(\prod_{i \in I} p_i^{m-1} \Big)\}(a^m - 1)\beta_m$$

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

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

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 $n \ge 3$, $e \ge 1$ and m, a, $S(n)$, β_m be as in Theorem 1. And, let $\phi(n)$ denote the Euler ϕ-function of n. Then,

$$\sum_{k=0}^{e} (-1)^k \binom{e}{k} \prod_{p \in S(n)} (1 - p^{m-1+k\phi(n)})(a^{m+k\phi(n)} - 1)\beta_{m+k\phi(n)} \equiv 0 \pmod{n^e}. \tag{9}$$

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

$$\sum_{k=0}^{e} (-1)^k \binom{e}{k} \prod_{p \in S(n)} (1 - p^{m-1+k\phi(n)})\beta_{m+k\phi(n)} \equiv 0 \pmod{n^e}. \tag{10}$$

Proof. For brevity, we set

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

Since $n \ge 3$, $m + k\phi(n)$ $(k = 1, 2, \dots, e)$ 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, $g_i = \operatorname{ord}_{p_i}(D_m) = \operatorname{ord}_{p_i}(D_{m+k\phi(n)})$ for $i = 1, 2, \dots, s$. Now, let $w' = n^e u'(m, n, e)$, where

$$u'(m, n, e) = \prod_{i=1}^{s} p_i^{f_i' + g_i} \quad \text{and} \quad f_i' = \max_{0 \le k \le e} \{\operatorname{ord}_{p_i}(m + k\phi(n))\}.$$

Consider the congruence (4), where m, n and w are replaced by $m + k\phi(n)$, n^e and w', respectively:

$$A_{m+k\phi(n)} \equiv \sum_{\substack{1\le j\le w'-1 \\ (j,n)=1}} (aj)^{m-1+k\phi(n)} [ja/w'] \pmod{n^e}, \tag{11}$$

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

$$\sum_{k=0}^{e} (-1)^k \binom{e}{k} A_{m+k\phi(n)} \equiv \sum_{\substack{1\le j\le w'-1 \\ (j,n)=1}} (aj)^{m-1}\{1 - (aj)^{\phi(n)}\}^e [ja/w'] \pmod{n^e}.$$

In this congruence, $(aj, n) = 1$, so that $\{(aj)^{\phi(n)} - 1\}^e \equiv 0 \pmod{n^e}$. 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 $a > 0$ such that $(a, n) = 1$, $a^{\phi(n)} \equiv 1 \pmod{n^e}$ and $(a^m - 1, n) = (a^{m+k\phi(n)} - 1, n) = 1$. Thus, by dividing (9) by $a^m - 1$, we can deduce the congruence (10). ||

If $m - 1 \ge e$, then the congruences (2) and (3) can be easily deduced from (9) and (10) respectively, by taking $n = p$ ($\ne 2$). Also, we note that Theorem 2 for the case $n = p^r$ ($r \ge 1$) 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 can not say exactly now, but it seems that perhaps the congruences (1) and (4) are intimately connected with the construction of p-adic L-fuctions.

REFERENCES

1. G. Frobenius: Über die Bernoullischen Zahlen und die Eulerschen Polynome, Sitzungsber. Akad. d. Wiss. zu Berlin, 1910, 809 - 843.

2. K. Iwasawa: Lectures on p-adic L-functions, Annals of Math. Studies, Princeton Univ. Press, Princeton, 1972.
3. N. Nielsen: Traité Élémentaire des Nombres de Bernoulli, Gauthier-Villars, Paris, 1923.
4. J. V. Uspensky and M. A. Heaslet: Elementary Number Theory, McGraw-Hill, New York - London, 1939.

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

Received July 13, 1984.

SUR LE RADICAL DE JACOBSON DANS LES ALGEBRES LOCALEMENT A-CONVEXES

M. OUDADESS

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

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

$$(P) : \forall x \in E, \quad Sp(x) = \{\chi(x) \mid \chi \in M\},$$

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,τ) un espace localement convexe et $(p_\lambda)_\lambda$ une famille de semi-normes définissant sa topologie τ. Si E est munie d'une structure d'algèbre telle que la multiplication soit séparèment continue, on dit que (E,τ) est une algèbre

localement convexe (a.l.c.).

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

$p_\lambda(x\cdot y) \leq M(\lambda,x)\cdot p_\lambda(y)$ et $p_\lambda(y\cdot x) \leq N(\lambda,x)\cdot p_\lambda(y)$, $\forall\, y$.

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

$\forall\ \lambda$: $p_\lambda(x\cdot y) \leq M(x)\cdot p_\lambda(y)$ et $p_\lambda(y\cdot x) \leq N(x)\cdot p_\lambda(y)$, $\forall\, y$.

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

$p_\lambda(x\cdot y) \leq p_\lambda(x)\cdot p_\lambda(y)$, pour tout λ 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 considèrons que des algèbres complexes et unitaires. Si (E,τ) est une a.l.c. on désigne par M^* l'ensemble des caractères (algèbriques) 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. $M \neq M^*$.

Nous allons maintenant décrire une situation où non seulement $M \neq M^*$ mais où $M = \emptyset$.

Contre-exemple III.1: Soit E une algèbre de Banach commutative, intègre radicale et à unité approchée bornée. Considérons l'algèbre $M(E)$, des multiplicateurs T de E, munie de la topologie stricte β définie par la famille de semi-normes $(p_x)_x$, $x \in E$, 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 $M^* \neq \emptyset$, et l'on sait que tout $\chi \in M^*$ est β-borné ([7] ou [8]). Par ailleurs E est β-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) β-continu. Ainsi $M(M(E)) = \emptyset$. 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 $\text{Rad } E = \cap \{\ker \chi \mid \chi \in M\}$; et donc Rad E est fermé.

Dans le contre-exemple III.1, Rad M(E) n'est pas égale à $\cap\{\ker \chi \mid \chi \in M\}$. 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

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

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 $x \to T_x$, 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 $E \subset \text{Rad}(M(E))$. Mais l'on sait que E est β-dense dans M(E) ([9], theorem 2.4, p.1134). Alors Rad(M(E)) n'est pas β-fermé car

sinon il serait égale à $M(E)$, ce qui ne peut être car M(E) est unitaire.

Remarque IV.3. Comme M(M(E)) = Ø, 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 Qué 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.

[1] M. AKKAR. "Sur certaines algèbres munies de normes particulières". C. R. Acad. Sc. Paris, T. 280 (1975), Série A, 345-348.

[2] A.C. COCHRAN, R. KEOWN, C.R. WILLIAMS. "On a class of topological algebras". Pacific J. Math., 34 (1970), 17-25.

[3] A.C. COCHRAN. "Representation of A-convex algebras". Proc. Amer. Math. Soc.,41 (1973), 473-479.

[4] T. HUSAIN, S.A. WARSI. "A note on A-convex Q-algebras". Bull. Soc. Roy. des Sc. de Liège, nr. 5-8, (1976), 163-165.

[5] R. LARSEN. "The multiplier problem". Lect. Notes in Math., nr. 105, Springer - Verlag (1969).

[6] E.A. MICHAEL. "Locally multiplicatively convex topological algebras". Memoirs of Amer. Math. Soc., 11, Providence (1952).

[7] M. OUDADESS. "Théorèmes de structure et propriétés fondamentales des algèbres localèment uniformement A-convexes". C. R. Acad. Sc. Paris, T. 269 (1983), Série I, 851-853.

[8] M. OUDADESS. "Continuité des caractères dans les algèbres uniformèment A-convexes". Ann. Sc. Math. Québec, 1983, Vol VII nr. 2, 193-201.

[9] J.K. WANG. "Multipliers of commutative Banach algebras". Pacific J. Math., 11 (1961), 1131-1149.

[10] W. ŻELAZKO. "Selected topics in topological algebras". Lect. Notes, Series 31 (1977), Matematisk Institut, Aarhus Universitet, Aarhus.

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.

0. 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_1 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 Γ with $\Gamma(I)$ and note that the topology of I defines open neighbourhoods on Γ.

The arc Γ 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 $t \in I\backslash\{s\}$ 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 $U'(t) = U(t)\setminus\{t\}$, $U^-(t) = \{s \in U(t) \mid s < t\}$ and $U^+(t) = \{s \in U(t) \mid t < s\}$. 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 (ord $\Gamma(U(t)) = n$) and $\Gamma(t)$ is ordinary.

An $(n-1)$-flat R_{n-1} supports [cuts] Γ 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] Γ at t if k is odd [even]; $0 \le k \le n-1$; cf. [3], p. 168.

From now on, we assume that Γ 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 $\Gamma_k(t)$, $0 \le k \le n-1$, depends continuously on t. Furthermore,

(1) Γ is dually differentiable; that is,

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

for $s \in I$ and $-1 \le k \le n-1$; 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 $0 \le k \le n-1$:

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

B(k): $\Gamma_k(s) \cap \text{int } C = \phi$ 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

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

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 (i), 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 Γ 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 Γ. As $\Gamma_k(s)$ depends continuously on s and Γ is elementary, (iv) follows.

2. From now on, we assume that $\Gamma(I) \subset C$ and that Γ 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

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

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

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

For every $p \in R_n$, we put

$$I_p^\circ = \{s \in I \mid p \in \Gamma_{n-1}(s)\} \text{ and } I_p^\pm = \{s \in I \backslash I_p^\circ \mid p \in C_s^\pm\}.$$

From (2), we readily obtain

2. LEMMA. (i) I_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* $t \in (r,s) \subset I$, *then either* $(r,s) \subset I_p^-$ *or* $(r,s) \subset I_p^+$.

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* $c \in \Gamma_{n-1}(t) \cap \operatorname{int} C$. *Then* $U^-(t) \subset I_c^+$ *and* $U^+(t) \subset I_c^-$ *for some* U(t).

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

4. *We prove Lemma 3.* Since Γ 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) ord $\Gamma(U(t)) = n$.

Let Γ^c denote the projection of Γ from c onto an $(n-1)$-flat R_{n-1} not through c. By [2], p. 113, Γ^c is an elementary arc in R_{n-1} with the osculating flats

$$\Gamma_k^c(s) = \begin{cases} \langle \Gamma_k(s), c\rangle \cap R_{n-1} & \text{if } c \notin \Gamma_k(s) \\ \Gamma_{k+1}(s) \cap R_{n-1} & \text{if } c \in \Gamma_k(s) \end{cases}; \quad s \in I,\ -1 \le k \le n-1.$$

Since Γ^c is elementary, we may assume

(c) ord $\Gamma^c(U^-(t)) =$ ord $\Gamma^c(U^+(t)) = n-1$.

By symmetry, it suffices to deal with $U^-(t)$. Let $s \in U^-(t) = (r,t)$. Then (b) implies $\Gamma_{n-1}(s) \cap \Gamma(r,t) = \{\Gamma(s)\}$ and therefore by (a), $\Gamma_{n-1}(s) \cap \Gamma(r,t] = \{\Gamma(s)\}$,

$$\Gamma(r,s) \subset C_s^-, \Gamma(s,t] \subset C_s^+ \quad \text{and} \quad s \in I^+_{\Gamma(t)}.$$

Thus $(r,t) \subset I^+_{\Gamma(t)}$ and we may assume that $c \neq \Gamma(t)$. -

By (a), $\alpha(s) = \langle c, \Gamma_{n-2}(s)\rangle$ is an $(n-1)$-flat distinct from $\Gamma_{n-1}(s)$ and thus $\Gamma^c_{n-2}(s) = \alpha(s) \cap R_{n-1}$. We note that $\alpha(s)$ supports Γ at s. By (c), $\Gamma^c_{n-2}(s) \cap \Gamma^c(r,t) = \{\Gamma^c(s)\}$. Hence

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

Let $\tilde{C}_s$ denote the component of $C \backslash \alpha(s)$ containing $\Gamma(r,t)\backslash\{\Gamma(s)\}$. Thus

(d) $\Gamma(r,s) \subset C_s^- \cap \tilde{C}_s$ and $\Gamma(s,t) \subset C_s^+ \cap \tilde{C}_s$.

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

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

(e) $\tilde{C}_s$, $\Gamma(r,t)\backslash\{\Gamma(s)\}$ and thus $\Gamma^\circ_{n-1}(s)$ lie in the same closed quadrant bounded by $\alpha(s)$ and $\pi(s)$

and (f) C_s^+ lies in the closed quadrant bounded by $\pi(s)$ and $\Gamma^\circ_{n-1}(s)$ containing $\Gamma(s,t)$.

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

4. Remarks. (i) If k is odd then

$$A(k) \Rightarrow B(k-1) \Rightarrow B(k) \Rightarrow A(k)$$

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

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

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

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

$$A(n-1) \Rightarrow B(n-2) \Rightarrow A'(n-1) \Rightarrow A(n-1).$$

REFERENCES

[1] T. BISZTRICZKY, Inflectional convex space curves, Can. J. Math., 36 (1984), 537-549.

[2] R. PARK, Topics in direct differential geometry, Can. J. Math. 24 (1972), 98-148.

[3] P. SCHERK, Über differenzierbare Kurven und Bögen I, II. Časopis pěst mat. a fys. 66 (1937), 165-191.

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 $\{X_i = \sigma^i(X_0) \mid i = 0,1,\ldots,p-1\}$ over $R_K[p^{-1}]$. We consider in the group ring $R_L[p^{-1}][G]$ the element

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

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

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

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

$$\chi_k : L[G] \to L(\zeta) \quad \text{via} \quad \chi_k(\sigma) = \zeta^k \ .$$

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 $\overline{\chi_k(X)} = \sum_{i=0}^{p-1} X_i \zeta^{-ik} = \sum_{i=0}^{p-1} X_i \zeta^{ik} = \chi_k(X)^{-1}$ by (1).

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

$$\hat{X}_k \overline{\hat{X}_k} = 1 \quad \text{for all} \quad k = 0,1,\ldots,p-1 \ . \tag{2}$$

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

$$\hat{X}_k \, R_{L(\zeta)} = \prod_{\mathfrak{P}} \mathfrak{P}^{\alpha(\mathfrak{P})} \ , \quad \text{where} \quad \alpha(\mathfrak{P}) \in \mathbb{Z} \quad \text{and}$$

$\alpha(\mathfrak{p}) = 0$ 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

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

$$\mathfrak{p}_i \neq \mathfrak{p}_j \quad \text{for} \quad i \neq j \quad ,$$

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

$$\hat{Y}_k := \chi_k(Y) = \frac{\hat{X}_k}{\overline{\hat{X}_k}} \quad ,$$

therefore (3) implies

$$\hat{Y}_k R_{L(\zeta)} = \frac{\prod \mathfrak{p}_i^{\alpha_i}}{\prod \overline{\mathfrak{p}}_i^{\alpha_i}} \quad .$$

Since there is only one prime ideal above p in $R_{K(\zeta)}$ we have $\mathfrak{p} = \overline{\mathfrak{p}}$ 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

$$(4) \quad L(\zeta) = K(\zeta)(\sqrt[p]{\zeta}) \quad .$$

If there is $k \in \{0,1,\dots,p-1\}$ such that $L(\zeta) = K(\zeta)(\hat{Y}_k)$ then $\hat{Y}_k^p = \zeta^j$ for some $j \in \{1,\dots,p-1\}$ since $X^p \in K[G]$ and so $\hat{Y}_k^p \in K(\zeta)$. This shows

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

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

$$\sum_{k=0}^{p-1} \hat{Y}_k \zeta^{ik} = \sum_{k=0}^{p-1} \chi_k(Y)\zeta^{ik} = \sum_{k=0}^{p-1}\left(\sum_{m=0}^{p-1} Y_m \zeta^{-mk}\right)\zeta^{ik} = p\,Y_i \ , \quad \text{hence}$$

$$Y_i \in K(\zeta)\left(\sqrt[p]{\zeta}\right) \quad \text{for all} \quad i = 0,1,\dots,p-1 \ .$$

Showing that $Y_0,\dots,Y_{p-1}$ 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 $i = 0,\dots,p-1$, where $Y_p = Y_0$.

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

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

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

because Y is a unit in $L[G]$. Thus $\alpha_i = 0$ for all i and $Y_0,\ldots,Y_{p-1}$ are K-linear independent in L. Let η be a primitive p^2-th root of unity then (4) implies that $L(\zeta)=\mathbb{Q}(\eta)$, but $\mathbb{Q}(\eta)$ 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

[1] I. Kersten and J. Michaliček, Kubische Galoiserweiterungen mit Normalbasis, Commun. Algebra 9 (1981), 1863-1871.

[2] M.-A. Knus and M. Ojanguren, Théorie de la Descente et Algèbres d'Azumaya, Springer Lecture Notes Math., 389 (1974).

[3] P. Ribenboim, Algebraic Numbers, Wiley-Interscience, 1972.

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 $[0,\infty)$. 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 $d\omega$ on $[0,\infty)$ of the form $d\omega = (2/\pi)d\lambda + d\sigma$ for suitable bounded $d\sigma$ and consider "polynomials" (*) $\pi(\lambda,t) = \text{Cos}\lambda t + \int_0^t c(t,s)\text{Cos}\lambda s\,ds$ (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" $L(\text{Cos}\lambda t) = \int_0^\infty \text{Cos}\lambda t\,d\omega(\lambda) = g(t) = 1 + g_r(t)$ where $g_r(t) = \int_0^\infty \text{Cos}\lambda t\,d\sigma(\lambda)$ (this will be characterized below in terms of generalized translation). One wants to construct orthogonal "polynomials" (relative to $d\omega$) of the form (*)

$$(1.1)\qquad f(\lambda,t) = \text{Cos}\lambda t + \int_0^t K(t,s)\text{Cos}\lambda s\,ds$$

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

$$(1.2)\qquad \int_0^\infty \text{Cos}\lambda s f(\lambda,t)d\omega(\lambda) = \tilde{\beta}(t,s) = 0$$

for $t > s$. Then write

$$(1.3)\qquad A(t,s) = \langle \text{Cos}\lambda t, \text{Cos}\lambda s \rangle_\omega = \delta(t-s) + \Omega(t,s)$$

$$(1.4)\qquad \Omega(t,s) = \int_0^\infty \mathrm{Cos}\lambda t \mathrm{Cos}\lambda s\, d\sigma = \tfrac{1}{2}[g_r(t+s) + g_r(|t-s|)]$$

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

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

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 (♦). 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 Ω 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

$$(1.6)\qquad Q(D_t)K(t,\tau) = D_\tau^2 K(t,\tau);\ Q(D_t) = D^2 - q;\ q(t) = 2D_t K(t,t);\ K_\tau(t,0) = 0$$

while f satisfies $Q(D_t)f = -\lambda^2 f$; $f(\lambda,0) = 1$; $f'(\lambda,0) = h = -g_r(0)$.

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 π by orthogonal "polynomials" f relative to various measures. The G-L equation arises again intrinsically relative to $d\omega$ as well as a certain generalized Bessel inequality relative to $d\nu = (2/\pi)d\lambda$. We refer to [9] for details.

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 associate with $d\nu$ the differential operator $Q_m u = Pu = (\Delta_p u')'/\Delta_p$ where $\Delta_p = t^{2m+1}$. There are orthogonal functions $\varphi_\lambda^p(t)$ relative to $d\nu$ given as the spherical function solutions of $Pu = -\lambda^2 u$ ($\varphi_\lambda^p(0) = 1$; $D_t\varphi_\lambda^p(0) = 0$); explicitly $\varphi_\lambda^p(t) = (1/c_m)\, J_m(\lambda t)/(\lambda t)^m$ where $c_m = 1/2^m \Gamma(m+1)$. The object now is to discover orthogonal

functions φ_λ^Q relative to $d\omega$ by showing that in suitable circumstances one can construct a singular differential operator Q and a transmutation B: P → Q so that the spherical functions $\varphi_\lambda^Q(t) \sim f(\lambda,t)$ can be obtained via B from φ_λ^P. 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

$$(2.1) \qquad f(\lambda,t) = A(t)\varphi_\lambda^P(t) + \int_0^t K(t,\tau)\varphi_\lambda^P(\tau)d\tau$$

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

$$(2.2) \qquad \Omega(\xi,x) = \int_0^\infty \varphi_\lambda^P(\xi)\varphi_\lambda^P(x)\sigma(\lambda)d\nu = \langle \varphi_\lambda^P(\xi), \varphi_\lambda^P(x)\sigma(\lambda)\rangle_\nu$$

Let us give a canonical expression for Ω in terms of the "moment functional" $g(t) = L[\Omega_\lambda^P(t)] = \int_0^\infty \Omega_\lambda^P(t)d\omega(\lambda) = \delta(t) + \Sigma(t)\Delta_P(t)$ $(\Omega_\lambda^P = \Delta_P\varphi_\lambda^P)$. Thus

$$(2.3) \qquad \Omega(t,s) = T_s^t\Sigma(s);\ \Sigma(s) = \int_0^\infty \sigma(\lambda)\varphi_\lambda^P(s)d\nu$$

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 (▪) $\tilde{\beta}(t,s) = \Delta_P(s)\langle f(\lambda,t), \varphi_\lambda^P(s)\rangle_\omega = 0$ 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 $f(\lambda,y) = \varphi_\lambda^Q(y)$ the form of $\tilde{\beta}$ in (•) plus the G-L representation $\tilde{\beta}(y,x) = \langle \beta(y,\xi)T_\xi^x\check{W}(\xi)\rangle\Delta_p(x), \check{W}(t)\Delta_p(t) = \delta(t) + \Sigma(t)\Delta_p(t)$, lead one to deduce the triangularity of $\tilde{\beta}(y,x)$ as an impulse response in a hyperbolic equation.

Now the G-L equation (*) in Theorem 4 contains two unknowns A and K so we write $A(t)\hat{K}(t,s) = K(t,s)$ and $\Delta_p(s)\Omega(t,s) = \hat{\Omega}(t,s)$ with $f(\lambda,t) = A(t)\hat{f}(\lambda,t)$ so that $\hat{f}(\lambda,t) = \varphi_\lambda^p(t) + \int_0^t \hat{K}(t,\tau)\varphi_\lambda^p(\tau)d\tau$ and (•) $0 = \hat{\Omega}(t,s) + \hat{K}(t,s) + \int_0^t \hat{K}(t,\tau)\hat{\Omega}(\tau,s)d\tau$ for $s < t$.

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

One shows next that if $f(\lambda,t) \sim \varphi_\lambda^Q(t)$ with $Q\varphi_\lambda^Q = -\lambda^2\varphi_\lambda^Q$ for $\Delta_Q = A_Q\Delta_p$ and $Qu = Q_0u + qu$, then, with K as in (2.1) and $A = A_Q^{-\frac{1}{2}}$, one obtains $\hat{q}(y) = 2D_y\hat{K}(y,y) = -q + q_0$ where $q_0 = \frac{1}{2}(A_Q''/A_Q) + (A_Q'/A_Q)[(m+\frac{1}{2})/y] - \frac{1}{2}(A_Q'/A_Q)^2$. Further $A_Q^{-\frac{1}{2}}P\hat{f} = (Q_0 + q_0)f$. Hence from Theorem 6, $Q_0f + qf = A_Q^{-\frac{1}{2}}P\hat{f} + (q-q_0)f = -\lambda^2f + (\hat{q}+q-q_0)f = -\lambda^2f$. We have now q and A_Q 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 $A = A_Q^{-\frac{1}{2}}$ will arise from an underlying operator $Q = Q_0$ with B: $\varphi_\lambda^p \to f$ in (2.1) representing a transmutation provided A_Q can be found satisfying $(C = A_Q)\ C'' + [(2m+1)/y]C' - \hat{q}C = 0$ where $\hat{q}$ is known from solving (•). The resulting f are then orthogonal relative to $d\omega$.

REFERENCES

1. F. Atkinson, Discrete and continuous boundary problems, Academic Press, N.Y., 1964

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

3. R. Carroll, Transmutation and operator differential equations, North-Holland, Amsterdam, 1979

4. R. Carroll, Some topics in transmutation, Diff. Eqs., Math. Studies 92, North-Holland, Amsterdam, 1984, pp. 87-104

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

6. R. Carroll, Transmutation, filtering, and scattering, Proc. Japan Acad., 60 (1984), 82-85

7. R. Carroll, Least squares, transmutation, and the Marčenko equation, CR Royal Soc. Canada, 6 (1984), 85-88

8. R. Carroll, Transmutation and linear stochastic estimation, Applicable Anal., 17 (1984), 217-226

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

10. R. Carroll and S. Dolzycki, Transmutation as a minimizing procedure, Jour. Math. Physics, 25 (1984), 91-93

11. K. Case, Inverse scattering, orthogonal polynomials, and linear estimation, Advances Math. Supp. 5 (1978), 25-43

12. K. Case and M. Kac, A discrete version of the inverse scattering problem, Jour. Math. Physics, 14 (1973), 599-603

13. T. Chihara, An introduction to orthogonal polynomials, Gordon-Breach, N.Y., 1978

14. J. Geronimo and K. Case, Scattering theory and polynomials orthogonal on the real line, Trans. Amer. Math. Soc., 258 (1980), 467-494

15. T. Kailath, A. Vieira, and M. Morf, Inverses of Toeplitz operators, innovations, and orthogonal polynomials, SIAM Review, 20 (1978), 106-119

16. M. Krein, The continuous analogues of theorems on polynomials orthogonal on the unit circle, Dokl. Akad. Nauk SSSR, 104 (1955), 637-640

17. B. Levy and J. Tsitsiklis, Linear estimation of stationary stochastic processes, vibrating strings, and inverse scattering, IEEE Trans. IT- , 1984

Mathematics Department
University of Illinois
Urbana, Illinois 61801

Received November 12, 1984.

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 1, February 1985 février

On a Functional Equation Connected to Sum Form Nonadditive Information Measures on an Open Domain

Pl. Kannappan and P.K. Sahoo

Presented by J. Aczél, FRSC

Abstract. Shannon's entropy is additive. However, there are information measures such as the entropies of degree β which are nonadditive. The sum form representation of these measures along with additivity and specific nonadditivity properties yield many interesting functional equations for instance (S) 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.

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

where $P \in \Gamma_n$ and $Q \in \Gamma_m$. The entropies of degree β

$$H_n^\beta(P) = \frac{\sum_{i=1}^{n} p_i^\beta - 1}{2^{1-\beta}-1} \quad (\beta \neq 1) \tag{1}$$

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

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

then the entropies of degree β take the form

$$H_n^\beta(P) = \sum_{i=1}^{n} f(p_i). \tag{3}$$

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

$$\sum_{i=1}^{n}\sum_{j=1}^{m} f(p_i q_j) = \sum_{i=1}^{n} f(p_i) + \sum_{j=1}^{m} f(q_j) + \lambda \sum_{i=1}^{n} f(p_i) \sum_{j=1}^{m} f(q_j), \tag{4}$$

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_i:]0,1[$\to R$ (reals) and satisfy the functional equation

$$\sum_{i=1}^{n} f_i(p_i) = 0 \quad (0 < p_i < 1, \sum_{i=1}^{n} p_i = 1) \tag{5}$$

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

$$f_i(p) = ap + b_i, \tag{6}$$

where a and the b_i's are arbitrary constants satisfying

$$a + \sum_{i=1}^{n} b_i = 0. \tag{7}$$

Result 2 (J. Aczél). Let $\Phi,\psi:]0,1[\to R$ be real valued functions. They satisfy the functional equation

$$q\Phi(p) - p\Phi(q) = \psi(q) - \psi(p) \tag{8}$$

for all p and q in $]0,1[$ if, and only if,

$$\Phi(p) = ap + b, \tag{9}$$

$$\psi(p) = bp + c, \tag{10}$$

where a,b,c are arbitrary constants.

Proof. Writing

$$g(p) = \psi(p) - \psi(\delta), \tag{11}$$

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

$$q\Phi(p) - p\Phi(q) = g(q) - g(p), \tag{12}$$

and

$$g(\delta) = 0. \tag{13}$$

Now we put $p = \delta$ in (12) and use (13) to obtain

$$g(q) = \alpha q - \delta\Phi(q). \tag{14}$$

Putting this back into (12), we get

$$q\Phi(p) - p\Phi(q) = \alpha q - \delta\Phi(q) - \alpha p + \delta\Phi(p). \tag{15}$$

Writing

$$h(p) = \Phi(p) - \alpha \tag{16}$$

in (15), we obtain

$$(q-\delta)h(p) = (p-\delta)h(q). \tag{17}$$

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

$$h(p) = a(p-\delta). \tag{18}$$

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

$$\Phi(p) = ap + b, \tag{19}$$

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

$$\psi(p) = \alpha p - a\delta p - \delta b + \psi(\delta) = bp + c. \tag{20}$$

The if part of the result is trivial.

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

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

$$\sum_{i=1}^{n}\sum_{j=1}^{m} f(p_i q_j) = \sum_{i=1}^{n} f(p_i) \sum_{j=1}^{m} f(q_j), \tag{21}$$

for a fixed pair of positive integers n,m (≥ 3) *and for all* $P \in \Gamma_n^0$ *and* $Q \in \Gamma_m^0$. *Then*

$$f(p) = p^{\beta}, \quad p \in]0,1[, \tag{22}$$

or

$$f(p) = Ap + B, \quad p \in]0,1[\tag{23}$$

where β *is an arbitrary constant and* A,B *are constants satisfying*

$$(A+mnB) = (A+nB)(A+mB). \tag{24}$$

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

Theorem. *Suppose that* $f:]0,1[\to R$ *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* $(p_1,p_2,\ldots,p_n) \in \Gamma_n^0$, $(q_1,q_2,\ldots,q_m) \in \Gamma_m^0$. *Then the function* f *is given by*

$$f(p) = \frac{(a-1)}{\lambda} p + \frac{b}{\lambda} \tag{25}$$

or

$$f(p) = \frac{p^\beta - 1}{\lambda}, \tag{26}$$

where β *is an arbitrary constant while the constants* a,b *satisfy the equation*

$$(a+mnb) = (a+nb)(a+mb). \tag{27}$$

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

[1] Aczél, J., *Information functions on open domain III.* C.R. Math. Rep. Acad. Sci. Canada *2* (1980), 281-285.

[2] Aczél, J. and Ng, C.T., *Determination of all symmetric, recursive information measures of multiplicative type of n positive discrete probability distributions.* Linear Algebra Appl. *52/53* (1983), 1-30.

[3] Behara, M. and Nath, P., *Additive and nonadditive entropies of finite measurable partitions.* Probability and Information Theory, Vol. 2, Lecture Notes in Math. Vol. 296, Springer, Berlin 1973, 102-138.

[4] Havrda, J. and Charvat, F., *Quantification method of classification processes, Concept of structural a-entropy.* Kybernetika (Prague) *3* (1967), 30-35.

[5] Kannappan, Pl., *On a generalization of some measures in information theory.* Glasnik Mat. Ser. III *9 (29)* (1974), 81-93.

[6] Kannappan, Pl., *On some functional equations from additive and nonadditive measures—I.* Proc. Edinburgh Math. Soc. (2) *23* (1980), 145-150.

[7] Kannappan, Pl. and Sahoo, P.K., *On a functional equation in two variables connected to sum form information measures on an open domain.* To appear.

[8] Kannappan, Pl. and Sahoo, P.K., *On a functional equation connected to sum form nonadditive information measures on an open domain—I.* Submitted.

[9] Losonczi, L., *A characterization of entropies of degree a.* Metrika *28* (1981), 237-244.

[10] Losonczi, L. and Maksa, Gy., *On some functional equations of the information theory.* Acta Math. Acad. Sci. Hungar. *39* (1982), 73-82.

[11] Ng, C.T., *Information functions on open domains I, II.* C.R. Math. Rep. Acad. Sci. Canada *8* (1980), 119-123 and 155-158.

[12] Sahoo, P.K., *On some functional equations connected to sum form information measures on open domains.* Utilitas Math. *23* (1983), 161-175.

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

Received November 28, 1984.

APPROXIMATION DIOPHANTIENNE PAR CERTAINS COUPLES D'ENTIERS

Peter THURNHEER

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

RESUME. Soient α,β réels. D'après un théorème de Dirichlet il existe une infinité de points entiers $\underline{x}=(a,b)\in\mathbb{Z}^2$, avec $\|\alpha a+\beta b\| \leq (\max(|a|,|b|))^{-2}$, 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 $\underline{x}=(a,b)$ à certains sous-ensembles de $\mathbb{R}^2$. De plus on peut étudier l'approximation diophantienne de α,β par des points entiers $\underline{x}$ dans un domaine angulaire.

RESULTATS. Soit

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

$$\Phi_0=\{(\xi_1,\xi_2)\in\mathbb{R}^2 \mid |\xi_2|<|\xi_1|\},$$

et soit Λ une transformation linéaire régulière. On note Ψ et Φ les images de Ψ_0, respectivement de Φ_0 par Λ. Par $\|.\|$ on désigne la distance à l'entier le plus proche et pour $\underline{x}=(a,b)\in\mathbb{R}^2$ soit $\langle\underline{x}\rangle=\max(|a|,|b|)$.

THEOREME 1. *Pour tout couple α,β de nombres réels il existe une infinité de points entiers $\underline{x}=(a,b)\in\mathbb{Z}^2$ avec*

$$\underline{x}\in\Psi \quad \text{et} \quad \|\alpha a+\beta b\| \leq c_1 \langle\underline{x}\rangle^{-2},$$

où c_1 dépend tout au plus de α,β et Λ.

Remarquons que le même énoncé est vrai avec $c_1=c_1(\Lambda)$ indépendant de α,β si dans la définition de Ψ on remplace l'ensemble Ψ_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 α,β réels avec $1,\alpha,\beta$ $\mathbb{Q}$-linéairement indépendants. Soit $1/2 \leq \eta < 1$. On suppose qu'avec $c_2(\alpha,\beta,\eta) > 0$ on a

$$\max(\|\alpha q\|, \|\beta q\|) \geq c_2 |q|^{-\eta} \qquad (1)$$

pour tout $q \in \mathbb{Z}$, $q \neq 0$.
Alors il existe une infinité de points entiers $\underline{x} = (a,b) \in \mathbb{Z}^2$, tels que

$$\underline{x} \in \Phi \quad \text{et} \quad \|\alpha a + \beta b\| \leq c_3 \langle \underline{x} \rangle^{-h(\eta)},$$

avec

$$h(\eta) = \frac{1}{4\eta}\left\{1 + \eta + \sqrt{1 + 2\eta + 17\eta^2}\right\},$$

où c_3 dépend tout au plus de α,β,Λ et η.

On a $h(1/2)=2$ et $h(1)=(1+\sqrt{5})/2$. Pour $\eta=1$ 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 "$1,\alpha,\beta$ $\mathbb{Q}$-linéairement indépendants" est indispensable. Presque tous les couples α,β de nombre réels - au sens de la mesure de Lebesgue dans $\mathbb{R}^2$ - vérifient la condition (1) avec $\eta = \frac{1}{2} + \delta$, pour tout $\delta > 0$ ([2]). De plus l'ensemble des $(\alpha,\beta) \in \mathbb{R}^2$ avec $1,\alpha,\beta$ $\mathbb{Q}$-linéairement dépendants est de mesure zéro. Le théorème 2 contient donc le

COROLLAIRE. Soit $\varepsilon > 0$. Pour presque tous les couples α,β de nombres réels il existe une infinité de points entiers $\underline{x} = (a,b) \in \mathbb{Z}^2$ avec

$$\underline{x} \in \Phi \quad \text{et} \quad \|\alpha a + \beta b\| \leq \langle \underline{x} \rangle^{-2+\varepsilon}.$$

Ce corollaire démontre pour presque tous les couples α,β 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 $\varepsilon > 0$. 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 infinité de points entiers $\underline{x}=(a,b) \in \mathbb{Z}^2$, avec $\|\alpha a^k + \beta b^k\| \leq c \langle \underline{x} \rangle^{-R+\varepsilon}$, où c ne dépend que de k et ε. 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 α, β réels et irrationnels, k entier, $k \geq 2$ et $0 < \varepsilon < R/4$. Alors il existe une infinité de points entiers $\underline{x}=(a,b) \in \mathbb{Z}^2$, tels que

$$\underline{x} \in \Phi \quad \text{et} \quad \|\alpha a^k + \beta b^k\| < \langle \underline{x} \rangle^{-R+r+\varepsilon},$$

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

$$\|\alpha w\| > w^{-((k+R-1)/(1-\varepsilon/2R))^2}$$

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

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

REFERENCES.

[1] R.J. Cook: The fractional parts of an additive form. Proc. Camb. Phil. Soc. 72 (1972) p.209-212.
[2] W.M. Schmidt: Approximation to algebraic numbers. L'enseignement math. t. XVII (1971) p.187-253.
[3] W.M.Schmidt: Two questions in diophantine approximation. Monatshefte für Math. 82 (1976) p. 237-245.
[4] W.M. Schmidt: Open problems in diophantine approximation. Colloque de Luminy 1982. Birkhäuser 1983.
[5] P. Thurnheer: Approximation diophantienne par certains couples d'entiers. Publ. math. de l'Univ. P. et M. Curie,1984.
[6] P. Thurnheer: Zur diophantischen Approximation von zwei reellen Zahlen. Acta Arithm. (à paraître).

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

$$(1)_n \qquad X^n + Y^n = Z^n$$

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

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

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 $\pm a \pm b = c$ 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 $m > N(r) = \left[\frac{\log L(r)}{\log 2}\right] + 1$ and if (a,b,c) is a non-trivial solution in coprime integers of $X^{rm} + Y^{rm} = Z^{rm}$ 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

$$S_{P,N} = \{n \in \mathbb{N} \mid 1 \leq n \leq N \text{ and there exists } p \in P \text{ such that } p \mid n\}.$$

Lemma. With the above notation

$$\frac{\#(S_{P,N})}{N} \geq 1 - \prod_{p \in P}\left(1 - \frac{1}{p}\right) - \frac{2^k}{N}$$

Proof: Let $Q = \prod_{p \in P} p$. Then

$$\#(S_{p,N}) = \sum_{p \in P} \left[\frac{N}{p}\right] - \sum_{\substack{p_1, p_2 \in P \\ p_1 \neq p_2}} \left[\frac{N}{p_1 p_2}\right] + \ldots + (-1)^{k+1} \left[\frac{N}{Q}\right]$$

$$= -\sum_{\substack{d \mid Q \\ d \neq 1}} \mu(d) \left[\frac{N}{d}\right] = N - \sum_{d \mid Q} \mu(d) \left[\frac{N}{d}\right].$$

But

$$\left| \sum_{d \mid Q} \mu(d) \left[\frac{N}{d}\right] - \sum_{d \mid Q} \mu(d) \left[\frac{N}{d}\right] \right| = \left| \sum_{d \mid Q} \mu(d) \left(\frac{N}{d} - \left[\frac{N}{d}\right]\right) \right|$$

$$\leq \sum_{d \mid Q} 1 = 2^k. \quad \text{Therefore}$$

$$\#(S_{p,N}) \geq N - \sum_{d \mid Q} \mu(d) \frac{N}{d} - 2^k =$$

$$N\left(1 - \sum_{d \mid Q} \frac{\mu(d)}{d}\right) - 2^k = N\left\{1 - \prod_{p \in P} \left(1 - \frac{1}{p}\right)\right\} - 2^k.$$

Then $$\frac{\#(S_{p,N})}{N} \geq 1 - \prod_{p \in P} \left(1 - \frac{1}{p}\right) - \frac{2^k}{N}.$$

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 $N_k = \max_{2 \leq j \leq k} \{p_j\, N(p_j)\}$.

For each integer $N \geq 1$ we also consider the sets

$S'_{P_k,N} = \{n \in \mathbb{N} \mid N_k < n \leq N$ and there exists $p_j \in P_k$ such that $p_j \mid n\}$

and $F_N = \{n \in \mathbb{N} \mid 3 \leq n \leq N$ such that equation $(1)_n$ has only trivial solutions$\}$.

We note that $S'_{P_k,N} \subseteq S_{P_k,N} \subseteq S'_{P_k,N} \cup \{1,2, \ldots, N_K\}$

With above notations, we have:

Theorem 2. $\lim_{N \to \infty} \frac{\#(F_N)}{N} = 1$

Proof: Let $\varepsilon > 0$. Since

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right) = \frac{1}{\sum_{n=1}^{\infty} \frac{1}{n}} = 0$$

there exists $k \geq 2$ such that

$$2 \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) + \frac{1}{p_k} < \varepsilon.$$

Let $N' = (2^{k-1} + N_k) N_k$ and $N > N'$. By Filaseta's theorem, $S'_{P_k,N} \subseteq F_N$, because if $n \in S'_{P_k,N}$ then $N_k < n \leq N$ and there exists $p_j \in P_k$ such that $p_j | n$; so $n = p_j m > N_k \geq p_j N(p_j)$ hence $m > N(p_j)$ and therefore $n = p_j m \in F_N$.

As $\#(S_{P_k,N}) - N_k \leq \#(S'_{P_k,N})$ it follows that

$$\frac{\#\left(S_{P_k,N}\right)}{N} - \frac{N_k}{N} \leq \frac{\#\left(S_{P_k,N}\right)}{N} \leq \frac{\left(F_N\right)}{N} \leq 1$$

On the other hand, by the lemma,

$$\frac{\#(S_{P_k,N})}{N} \geq 1 - \prod_{j=2}^{k}\left(1-\frac{1}{p_j}\right) - \frac{2^{k-1}}{N} =$$

$$1 - 2\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right) - \frac{2^{k-1}}{N}.$$

$$\text{Thus } 1 - 2\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right) - \frac{2^{k-1}+N_k}{N} \leq \frac{\#(F_N)}{N} \leq 1$$

hence if $N \geq N' \geq N_k \geq p_k$ then

$$1-\varepsilon \leq \frac{\#(F_N)}{N} \leq 1. \quad \text{This shows that } \lim_{N\to\infty} \frac{\#(F_N)}{N} = 1,$$

which completes the proof of the theorem.

3. A final remark concerns the equations

$$(2)_n \qquad aX^n + bY^n = cZ^n$$

where a,b,c are non-zero integers, and solueions with $(X,Y,Z) \in (-1,0,1)$ 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 $|X|, |Y|, |Z| > |$.

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

1. Ankeny, N.C. & Erdös, P. The insolubility of classes of diophantine equations, Amer. J. Math., 76, 1954, 488-496.

2. Faltings, G. Einige Sätze zum Thema Abelsche Varietaten über Zahlkönpern. To appear in Invent. Math.

3. Filaseta, M. An application of Faltings' results to Fermat's last theorem. C.R. Math. Reports Acad. Sci. Canada, 6, 1984, 31-32.

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 α 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 $\frac{(p-1)^{2^{p-1}-1}-1}{p-2}$ and Meixner [4] has improved this bound to $(p-1)^{2^{p-1}-2}$.

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 $\frac{p^2-1}{4}$. 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 $a_1a_2a_3\ldots a_n$ the left-nromed monomial $[[\ldots[[a_1a_2]a_3]\ldots]a_n]$.

By Higman ([2] p. 327) we may assume that L (in the Introduction) is a Lie ring over $Z[\omega]$ where ω is a primitive p^{th} root of unity and that L is generated by $G = \bigcup G_i$ $(1 \leq i < p)$ where $G_i = \{a \in L \mid \alpha(a) = \omega^i a\}$, the elements of L of weight i. We think of these weights as being in Z_p, the field of order p. Since α 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 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 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 Z_p is zero.

Let $x_1x_2\ldots x_n$ be a word in element of 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 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 $x_1x_2\cdots x_{i-1}x_{i+1}\cdots x_n$ and that of the second term is $x_1x_2\cdots x_{i-1}(x_{i-1}-x_i+x_{i+1})x_{i+1}\cdots x_n$.

We abuse notation and write

$$x_1x_2\cdots x_n = x_1x_2\cdots x_{i-1}x_{i+1}\cdots x_n + x_1x_2\cdots x_{i-1}(x_{i-1}-x_i+x_{i+1})x_{i+1}\cdots x_n.$$

We denote the "sum" on the right by $x_1x_2\cdots x_{i-1}\overset{\downarrow}{x_i}x_{i+1}\cdots x_n$. 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 arguement 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 $\rho(w)$.

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 α by α^k $(1\leq k<p)$ it is not difficult to see that if the word $x_1x_2\cdots x_n$ is zero (with the x_i's in Z_p) then so is $(kx_1)(kx_2)\cdots(bx_n)$. We denote the latter by $k(x_1\cdots x_n)$.

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 $k(5) = 6$.

As usual we denote the elements of Z_p by $0,1,2,\ldots,p-1$. For x in Z_p we denote by $x!$ the word $123\ldots x$. For x in Z_p we denote the element $p - x$ in Z_p by $\bar{x}$.

Lemma 1: $3!yzt = 0$ for all y, z, t in Z_p .

Theorem: (G. Higman [2] p. 331-334) $k(5) = 6$.

Proof: We must show that every word of length seven in elements of 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 Z_5 . Also $(\frac{1}{2})\overset{\downarrow}{3}23(\frac{1}{2}) = 0$ and $\overset{\downarrow}{3}234 = 34\overset{\downarrow}{3}4 = 0$. Thus,

$$a323b = 0 \quad \text{for all} \quad a, b \quad \text{in} \quad Z_5 \qquad (**)$$

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 Z_5. Also $3\overset{\downarrow}{2}42 = 0$. Now $3\overset{\downarrow}{2}43 = 323 + 32\overset{\downarrow}{1}3$, and so $a3243b = 0$ for all a, b by (**) except $43\overset{\downarrow}{2}43b = 4\overset{\downarrow}{3}43b = 0$. We conclude that the middle three digits of w cannot be 324 (or 423 by symmetry). Finally $2(\overset{\downarrow}{4}24) = 2(414) = 323$ 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 cba 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 $513(\frac{4}{6})$.
   (b) abc124defgh = 0 .

5. (a) abcdm324efgh = 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

1. BLACKBURN, N., HUPPART, B.: Finite Groups II, Springer-Verlag, Berlin 1982.

2. HIGMAN, G.: Groups and Rings having automorphisms without non-trivial fixed elements, J. London Math. Soc., Vol. 32 (1957), pp. 321-334.

3. KRENKIN, V.A., KOSTRIKIN, A.I.: Lie Algebras with a regular automorphism, Dokl. Akad. Nauk SSSR 150 (1963), pp. 467-469; Soviet Math. Dokl. 4 (1963), p. 355-358.

4. MEIXNER, T: Uber endliche Gruppen mit Automorphismen deren Fixpunktgruppen beschrankt sind. Doctoral thesis, University of Erlangen-Numberg.

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],I)

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'isomorphie 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 $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_m$. On pose

$$\varepsilon^{(s)}=(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_s)\ (s\geq 0) \text{ et } \varepsilon=\varepsilon^{(m)} .$$

Soit, pour $0\leq s\leq m$, $E_s=\Gamma_1\times\Gamma_2\times\ldots\times\Gamma_s$ le produit direct des groupes $\Gamma_1,\Gamma_2,\ldots,\Gamma_s$ (donc $E_0=\{\varepsilon^{(0)}\}$;on pose en plus $E=E_m$).
Soit $a_s:E_{s-1}\to\Gamma_s$ une application de E_{s-1} dans Γ_s (en particulier $a_1:E_0\to\Gamma_1$ est une constante $\in\Gamma_1$). Aussi a_s sera écrit $a_s(x_1,\ldots,x_{s-1})$. On représente par le tableau $A=[a_1,a_2(x_1),\ldots,a_m(x_1,\ldots,x_{m-1})]$ la permutation de l'ensemble E,

définie par la correspondance

$$t=(t_1,t_2,\ldots,t_m) \to t'=(t'_1=a_1t_1, t'_2=a_2(t_1)t_2,\ldots,t'_m=a_m(t_1,\ldots,t_{m-1})t_m) .$$

Quand les a_s $(1\leq s\leq m)$ parcourrent indépendemment, pour chaque s, l'ensemble des fonctions de E_{s-1} dans Γ_s, ces permutations forment un groupe, qu'on note $G=\Gamma_1\circ\Gamma_2\circ\ldots\circ\Gamma_m$ et qu'on appelle <u>produit d'entrelacement</u> des groupes abstraits $\Gamma_1,\Gamma_2,\ldots,\Gamma_m$. La fonction $a_s(x_1,\ldots,x_{s-1})$ 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 $F_p\circ F_p\circ\ldots\circ F_p$ est précisément le groupe P_m mentionné, qui est en fait un p-groupe de Sylow de S_{p^m} [2]. Les fonctions $a_s(x_1,x_2,\ldots,x_{s-1})$, qui figurent comme coordonnées des tableaux de P_m $(1\leq s\leq m)$, peuvent être et seront représentées par des polynômes $x_1,x_2,\ldots,x_{s-1}$ et à coefficients dans F_p, dans lesquels les exposants de chaque x_i ne sont pas supérieurs à p-1.

Soient $z=(z_1,z_2,\ldots,z_n)$ un vecteur de n variables $z_1,z_2,\ldots,z_n$ et $i=(i_1,i_2,\ldots,i_n)$ un vecteur de n entiers. Alors on notera z^i le monôme

$$z_1^{i_1}z_2^{i_2}\ldots z_n^{i_n} .$$

En particulier, si on adopte les variables $x_1,x_2,\ldots,x_{m-1}$, on va poser, pour $m-1\geq\mu\geq\lambda+1$, $x_{\mu,\lambda}=(x_\mu,\ldots,x_{\lambda+1})$ et $i_{\mu,\lambda}=(i_\mu,\ldots,i_{\lambda+1})$. Si q est un entier, $i_{\mu,\lambda}$ sera noté (q), s'il est de la forme (q,q,...,q). Ainsi

$$(x_\mu x_{\mu-1}\ldots x_{\lambda+1})^q=x_{\mu,\lambda}^{(q)} .$$

On écrit également $x=x_{m-1,0}=(x_{m-1},\ldots,x_1)$ et $i=i_{m-1,0}=(i_{m-1},\ldots,i_2,i_1)$. Si

$$z=(x_{\mu,\lambda})^{i_{\mu,\lambda}} ,$$

on appelle hauteur de z l'entier

$$h(z)=i_\mu p^{\mu-1}+i_{\mu-1}p^{\mu-2}+\ldots+i_{\lambda+1}p^\lambda+1 .$$

Soit g un sous-groupe de $G=\Gamma_1\circ\Gamma_2\circ\ldots\circ\Gamma_m$. On désigne par g_i les permutations de g, qui conservent les i premières coordonnées de $\varepsilon\in E$: autrement dit, si $j\leq i$, $a_j(\varepsilon_1,\ldots,\varepsilon_{j-1})=\varepsilon_j$. On obtient ainsi une suite de sous-groupes de g

$$g=g_0\supset g_1\supset g_2\supset\ldots\supset g_m \quad (s) ,$$

dont chacun est invariant dans le précédent. Cette suite s'appelle

la suite canonique de g. L'application $\phi_i: Ag_i \to a_i(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{i-1})$, où $A \in g_{i-1}$, est un isomorphisme, dit canonique, de g_{i-1}/g_i dans Γ_i. Si g est transitif, tous les g_{i-1}/g_i le sont aussi, donc $\phi_i(g_{i-1}/g_i) = \Gamma_i$ et g_m, comme groupe de stabilité de l'élément ε 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

$$h = h_0 \supset h_1 \supset h_2 \supset \ldots \supset h_m \quad (s') ,$$

telle que a) le quotient h_{i-1}/h_i est isomorphe au groupe $\Gamma_i (1 \leq i \leq m)$ et, pour chaque $i = 1, \ldots, m$, un isomorphisme ψ_i de h_{i-1}/h_i sur Γ_i est donné b) h_m est anti-invariant dans H. Alors, il existe un isomorphisme η de h sur un sous-groupe transitif g de $G = \Gamma_1 \circ \Gamma_2 \circ \ldots \circ \Gamma_m$ vérifiant les propriétés suivantes: 1) $\eta(h_i) = g_i$; 2) $\psi_i = \phi_i \eta$, où on désigne aussi par η, comme il est habituel, l'homomorphisme induit par η sur h_{i-1}/h_i (pour quelque i). Un tel isomorphisme η sera appelé un $(\Gamma_1, \ldots, \Gamma_m)$-isomorphisme (relativement à $(s'), \psi_i (1 \leq i \leq m)$). 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 η.

Théorème de transformation [3]. Soit η un $(\Gamma_1, \ldots, \Gamma_m)$-isomorphisme de h (avec les ψ_i fixés) dans G. Alors, si $\mathrm{Int}_m(G)$ est le groupe des automorphismes interieurs ω_λ de G induits par les $\lambda \in G_m$, l'ensemble des $(\Gamma_1, \ldots, \Gamma_m)$-isomorphismes de h dans G est $\mathrm{Int}_m(G)\eta$. En particulier les $(\Gamma_1, \Gamma_2, \ldots, \Gamma_m)$-automorphismes de G forment un groupe

$$\mathrm{Aut}^{(\Gamma_1, \ldots, \Gamma_m)}(G) = \mathrm{Int}_m(G) .$$

En posant h = G, les théorèmes précédents permettent de trouver Aut(G), si on connait a) les images de la suite canonique (s) de G par les éléments de Aut(G) ainsi que b) l'ensemble 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 $A=[a_1,a_2(x_1),\ldots,a_i(x_1,\ldots,x_{i-1}),\ldots]$ sur

$$A'=[\omega_1 a_1,\omega_2 a_2(\omega_1^{-1}\cdot a_1),\ldots,\omega_i a_i(\omega_1^{-1}\cdot x_1,\ldots,\omega_{i-1}^{-1}\cdot x_{i-1}),\ldots]\ (¶).$$

Cet automorphisme stabilise la suite (s) et induit,au sens évident, l'automorphisme ω_i sur le groupe correspondant Γ_i. Ces automorphismes ω forment un groupe $\Omega_m(\Gamma_1,\ldots,\Gamma_m)$ isomorphe à $\mathrm{Aut}(\Gamma_1)\oplus\ldots\oplus\mathrm{Aut}(\Gamma_m)$. Il est visible que

$$\mathrm{Aut}(G,s)=\Omega_m(\Gamma_1,\ldots,\Gamma_m)\,\mathrm{Aut}^{(\Gamma_1,\ldots,\Gamma_m)}(G)\ .$$

Dans le cas où $\Gamma=F_p$, $\mathrm{Aut}(\Gamma)$ est le groupe des multiplications des $x\in F_p$ par les $w\in F_p$ 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

$$A=[a_1,a_2(x_1),\ldots,a_m(x_1,\ldots,x_{m-1})]\quad\text{sur}$$

$$A'=[w_1a_1,w_2a_2(w_1^{-1}x_1),\ldots,w_ma_m(w_1^{-1}x_1,\ldots,w_{m-1}^{-1}x_{m-1})]$$

et on va noter Ω_m le groupe $\Omega_m(F_p,\ldots,F_p)$.

La correspondance $A\to\bar{A}$, où $A\in P_m$ et $\bar{A}\in P_{m-1}$, telle que $[\bar{A}]_s=[A]_s$, pour $1\le s\le m-1$, est un homomorphisme de P_m sur P_{m-1}, appelé (m-1)-projection et noté pr_{m-1},dont le noyau est un sous-groupe caractéristique de P_m,noté Δ_{m-1}. Si g est un sous-groupe de P_m,son image $\bar{g}=pr_{m-1}(g)$ par pr_{m-1} est appelée <u>tête</u> de g et $\tilde{g}=g\cap\Delta_{m-1}$ est appelé <u>sous-groupe de fond</u> de g. On remarque que,pour $X\in\tilde{g}$ et $A\in g$,le conjugué

$$AXA^{-1}\in\tilde{g}\subset\Delta_{m-1}$$

dépend seulement de $\bar{A}$. Ainsi on le note $\bar{A}X\bar{A}^{-1}$ et on dit que les $\omega_{\bar{A}}:X\to\bar{A}X\bar{A}^{-1}(\bar{A}\in\bar{g},X\in\tilde{g})$ sont les conjugaisons induites par $\bar{g}$ sur $\tilde{g}$. Le groupe g est une extension de $\tilde{g}$ par $\bar{g}$. Tout $\eta\in\mathrm{Aut}(P_m)$ induit, par passage au quotient par Δ_{m-1}, un automorphisme $\bar{\eta}\in\mathrm{Aut}(P_{m-1})$, qu'on appelle (m-1)-projection de η.La correspondance $\eta\to\bar{\eta}$ définit un homomorphisme Φ. La détermination de son noyau $N(\Phi)$, de son

---

(¶) Etant donnés une application $f:A\to B$ et $x\in A$, on note aussi $f\cdot x$ l'image de x par f et ce sera le seul emploi du point en tant que signe mathématique.

image $Im(\Phi)$ et d'un certain sous-groupe $Im^*(\Phi)$ de $Aut(P_m)$, tel que $\Phi(Im^*(\Phi))=Im(\Phi)$, permet de présenter $Aut(P_m)$ sous la forme: $Aut(P_m)=Im^*(\Phi)N(\Phi)$. La détermination de $N(\Phi)$ et de $Im^*(\Phi)$ se fait de manière que la structure du groupe $Aut(P_m)$ devient parfaitement claire. On va exposer ces résultats ultérieurement.

BIBLIOGRAPHIE

[1] Marshall Hall,Jr.: The theory of groups, The Macmillan Company,New York,1959

[2] Leo Kaloujnine: Structures des p-groupes de Sylow des groupes symétriques finis, in Annales Scientifiques de l'Ecole Normale Supérieure,1948,pp.239-271

[3] M.Krasner-L.Kaloujnine: Produit complet des groupes de permutations et problème d'extension de groupes, in Acta Scientiarum Mathematicarum de Szeged: I:13(1950),pp.208-230, II:14(1951),pp.39-66 et III:14(1951),pp.69-82

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 Moebius 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 $P_2\mathbb{F}$ 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 $PGL_2(\mathbb{F})$ acting on $L = P_1\mathbb{F}$ in the usual way. Let $P_2\mathbb{O}$ be the projective plane over the alternative division algebra of octonions over $\mathbb{R}$, then the action of Π on L is equivalent to the action of the 45-dimensional Lie group $PSO_{10}(\mathbb{R},1)$ on the 8-sphere of points in $P_9\mathbb{R}$ which are isotropic with respect to a quadratic form of index 1.

Let $A_2\mathbb{F}$ be the affine plane over $\mathbb{F} = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$, then the group of affine projectivities is $\Pi^{aff} = \{x \mapsto ax+b \; ; \; a,b \in \mathbb{F}, \; a \neq 0\}$ and for $A_2\mathbb{O}$, Π^{aff} is the group $\mathbb{R}^8 \rtimes GO_8^+(\mathbb{R})$ of similitudes of $\mathbb{R}^8$ of positive determinant.

2. The group of projectivities of the Moulton planes and a class of topological Moebius 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 iff $k = k'$ [11].

Definition: A bijection σ of the projective line $P_1\mathbb{R}$ is called piecewise projective, if there exists a subdivision $P_1\mathbb{R} = I_1 \cup \ldots \cup I_n$ into closed intervals, such that on each I_j, the map σ 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 Σ by composition, acting as transformation group $(\Sigma, P_1\mathbb{R})$ on the real projective line.

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

Remarks: a) Σ contains the group $PGL_2(\mathbb{R})$ and all semi-dilatations $x \mapsto \begin{cases} x & \text{if } x \geq 0 \\ ax & \text{if } x \leq 0 \end{cases}$, $0 < a \in \mathbb{R}$. Let H_1 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) Σ acts transitively on the oriented n-tuples of points of

$P_1\mathbb{R}$ 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 Σ is known [3;5]: Σ possesses the commutator series $\Sigma \rhd \Sigma' \rhd \Sigma''$ with $\Sigma/\Sigma' \cong \mathbb{Z}_2$, $\Sigma'/\Sigma'' \cong (\mathbb{R},+)$, Σ'' is a simple group and $\Sigma' = \langle PSL_2(\mathbb{R}), H_1 \rangle$, the group of orientation preserving elements of Σ.

The group of projectivities of the classical miquelian Moebius plane is the group $PGL_2(\mathbb{R})$ (for a definition of projectivities of Moebius planes see e.g. [7,§1]). In [6,§4] G. Ewald described a class of 2-dimensional Moebius planes as follows: A great circle G 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 Moebius plane $\mathcal{M}$. The planes are of Hering-type IV 1 [10] and all derived affine planes are arguesian.

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

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

b) $PGL_2(\mathbb{R}) \leq \Pi$, 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 stereografic projection, such that G is projected onto the y-axis. Some circle of $\mathcal{M}$ 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 φ_1 (φ_2) be the perspectivity from X to K (from K to X) with centres ∞ and $(\xi,\eta) \in K$, $\eta \neq \pm 1$ (with centres ∞ 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 $PGL_2(\mathbb{R})$ one

obtaines 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×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 ∘, defined by $(x = (x_1,\ldots,x_8),\ a = (a_1,\ldots,a_8),\ x_i,a_i \in \mathbb{R})$:

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

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 $(F_r,+,\circ)$ (if r=1 one gets the multiplication of the octonions). Using [8, 2.3.] one shows:

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

Let $Q_r := \{(x_1,x_2,0,\ldots,0) ;\ x_i \in \mathbb{R}\} \leq F_r$ and $D_r := \{(x_1,\ldots,x_4,0,\ldots,0) ;\ x_i \in \mathbb{R}\} \leq F_r$, then Q_r (D_r) with the induced addition and multiplication is a 2-dimensional (4-dimensional) sub-quasifield of F_r and $Q_1 \cong \mathbb{C}$, $D_1 \cong \mathbb{H}$. 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 descibed 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

$$(x_1,\dots,x_n) \mapsto \begin{cases} (x_1,\dots,x_n) & \text{if } x_1 \geq 0 \\ (x_1,\dots,x_n)\begin{pmatrix} c_1 & c_2 & \cdots & c_n \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} & \text{if } x_1 \leq 0 \end{cases},$$

where $c_i \in \mathbb{R}$, $c_1 > 0$ 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 $S^n = \mathbb{R}^n \cup \{\infty\}$ by mapping ∞ onto itself. H_1 is the group of semi-dilatations.

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

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

a) [4, 1.1., p. 29] $\Pi_o^{aff}(Q_r) = GL_2(\mathbb{R})^1$, $\Pi^{aff}(Q_r) = \mathbb{R}^2 \rtimes GL_2(\mathbb{R})^1$ and $\Pi(Q_r) \geq \langle PGL_2(\mathbb{C}), H_2 \rangle$.

b) [13, 1.1., 1.4.] $\Pi_o^{aff}(D_r) = GL_4(\mathbb{R})^1$, $\Pi^{aff}(D_r) = \mathbb{R}^4 \rtimes GL_4(\mathbb{R})^1$ and $\Pi(D_r) \geq \langle PGL_2(\mathbb{H}), H_4 \rangle$.

c) [13, 1.6., 1.7.] $\Pi_o^{aff}(F_r) = GL_8(\mathbb{R})^1$, $\Pi^{aff}(F_r) = \mathbb{R}^8 \rtimes GL_8(\mathbb{R})^1$ and $\Pi(F_r) \geq \langle PSO_{10}(\mathbb{R},1), H_8 \rangle$.

Remarks: As $PGL_2(\mathbb{C}) \cong PSO_4(\mathbb{R},1)$ and $PGL_2(\mathbb{H}) \cong PSO_6(\mathbb{R},1)$ [12], the groups $\langle PGL_2(\mathbb{C}), H_2 \rangle$ and $\langle PGL_2(\mathbb{H}), H_4 \rangle$ belong to the family $G_n := \langle PSO_{n+2}(\mathbb{R},1), H_n \rangle$, $n \geq 2$. 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 [4,2.7.; 13,2.6.].

References

1. Arens, R.: Topologies for homeomorphism groups. Amer. J. Math. 68, 593-610 (1956).
2. Betten, D.: 4-dimensionale Translationsebenen. Math. Z. 128, 129-151 (1972).
3. Betten, D.: Die Projektivitätengruppe der Moulton-Ebenen. J. Geometry 13, 197-209 (1979).
4. Betten, D.: Die Projektivitätengruppe einer Klasse 4-dimensionaler Translationsebenen. J. Geometry 21, 19-32 (1983).
5. Betten, D. and Wagner, A.: Eine stückweise projektive topologische Gruppe im Zusammenhang mit den Moulton-Ebenen. Arch. Math. 38, 280-285 (1982).
6. Ewald, G.: Aus konvexen Kurven bestehende Möbius-Ebenen. Abh. Math. Sem. Hamburg 30, 179-187 (1965).
7. Grundhöfer, T.: Projektivitätengruppen von ovoidalen Möbius- und Laguerreebenen. Geometriae Dedicata 13, 125-147 (1982).
8. Hähl, H.: Kriterien für lokalkompakte topologische Quasikörper. Arch. Math. 38, 273-279 (1982).
9. Hähl, H.: Eine Klasse von achtdimensionalen lokalkompakten Translationsebenen mit großen Scherungsgruppen. Mh. Math. 97, 23-45 (1984).
10. Hering, C.: Eine Klassifikation der Möbiusebenen. Math. Z. 87, 252-262 (1965).
11. Salzmann, H.: Topological Planes. Adv. Math. 2, 1-60 (1967).
12. Tits, J.: Tabellen zu den einfachen Liegruppen und ihren Darstellungen. Lecture Notes in Math. 40, Springer 1967.
13. Weigand, C.: Eine Klasse topologischer Gruppen im Zusammenhang mit Projektivitätengruppen topologischer Translationsebenen. To appear in Geometriae Dedicata.

Mathematisches Seminar
der Universität Kiel
Olshausenstraße 40
D-2300 Kiel
F. R. Germany

Received December 5, 1984.

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 1, February 1985 février

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 χ of the orthogonal group $G_n = O_{2n+1}(2)$ or χ^σ of its maximal subgroup $G_n^\sigma = O_{2n}^\sigma(2)$, with $\sigma = \pm$ (or ± 1), have values χ_λ or χ_λ^σ on class C_λ of size ${}^oC_\lambda$ or ${}^oC_\lambda^\sigma$. Their class multipliers are

$$\omega_\lambda = {}^oC_\lambda \chi_\lambda/\chi_1 \qquad \omega_\lambda^\sigma = {}^oC_\lambda^\sigma \chi_\lambda^\sigma/\chi_1^\sigma \tag{1.1}$$

For eight classes C_λ besides the classes C_1 and C_t for which they are already known, this report derives generic formulas for the class multipliers ω_λ (or ω_λ^σ) of each AIC character χ of G_n (or χ^σ of G_n^σ) as polynomials in $N = 2^n$ with coefficients determined by χ (or χ^σ). Thus χ_λ (or χ_λ^σ) can be found explicitly for each of ten classes corresponding to classes of $S_8 = G_3^+$ as follows:

$$C_1 = 1^8, \quad C_3 = 1^5 3, \quad C_5 = 1^3 5 \quad C_s = 1^4 2^2, \quad C_r = 2^4 \tag{1.2}$$
$$C_t = 1^6 2, \quad C_{3t} = 1^3 2 \cdot 3, \quad C_{st} = 1^2 2^3, \quad C_{4-} = 1^4 4, \quad C_{4+} = 2^2 4.$$

If χ (or χ^σ) has level ℓ, $L = 2^\ell$, and its "parent" character ϕ (see [1]) in G_ℓ^τ (or G_ℓ) has codegree d (= group order/ϕ_1), then the degree χ_1 (or χ_1^σ) is expressible as a polynomial in N.

$$\chi_1 d = \prod_{i=1}^{2\ell} (N - r_i) = N^{2\ell}(1 - a_1/N + a_2/N^2 - a_3/N^3 + a_4/N^4 - \cdots) \tag{1.3}$$

where the 2ℓ 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 $N-2^{v-1}$, $N+2^{v-1}$, both or neither are factors. Thus the character of G_4^+ denoted hgk/72 has degree $(N-1)(N^2-4)(N+4)/72 = 15(252)20/72 = 1050$, and $kih/6 = (N+1)(N-4)/6$. This symbolism, with powers of N adjoined where needed, describes the sizes of pertinent conjugacy classes in G_n and G_n^+ as follows:

C_λ	C_3	C_5	C_s	C_r	C_t	C_{3t}	C_{st}
${}^oC_\lambda$	$gN^2/6$	$ggN^4/2^65$	$gg/2^2$	$gg/2^23$	g	$ggN^2/2^33$	$ggg/2^43$
${}^oC_\lambda^+$	$hhN^2/24$,	$hghN^4/2^{10}5$,	$hgN/2^4$,	$hgk/2^43$,	$hN/2$,	$hgN^3/2^63$,	$hggN/2^73$

(1.4)

Also ${}^oC_{4-} = {}^oC_{4+} = ggN^2/2^5$, ${}^oC_{4-}^+ = hghN^2/2^8$, and ${}^oC_{4+}^+ = hgkN^2/2^8$. 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_i by $-r_i$, thus changing signs of $a_1, a_3, \cdots$ 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:

$$\omega_t = {}^oC_t\chi_t/\chi_1 = T(N+a_1) - 1, \quad \omega_t^\sigma = (T/2)(N+a_1-\sigma) \tag{1.5}$$

where τ is the sign of χ_t and $T = \tau N/L$.

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

$$C_t^2 = m_{t1}C_1 + 3C_3 + 2C_s, \quad m_{t1} = N(N-\sigma)/(1+\sigma^2) - 1 + \sigma^2 \tag{1.6}$$

$$C_3C_t = m_{3t}C_t + C_{3t} + 4C_{4-}, \quad m_{3t} = N(\tfrac{1}{2}N-\sigma)/(1+\sigma^2) \tag{1.7a}$$

$$C_rC_t = m_{rs}C_s + C_{st} + 2C_{4+}, \quad m_{rs} = 1 - \sigma^2. \tag{1.7b}$$

$$C_sC_t = m_{st}C_t + 3m_{rs}C_r + 3C_{3t} + 3C_{st} + 2C_{4-} \tag{1.7c}$$

where $m_{st} = (\tfrac{1}{2}N^2-2)/(1+\sigma^2)$, σ is 0 for G_n, ± 1 for $G_n^\pm$, and $m_{\lambda\mu}$ are the multiplicities of elements of C_μ in $C_\lambda C_t$. Formulas (1.6) and (1.7a,b,c) yield similar formulas for class multipliers ω_λ or ω_λ^σ, and supply four of the eight pairs of relations we require.

In Section 2 we derive formulas for ω_3, ω_3^+, ω_5, and ω_5^+, and find ω_s, ω_s^+ from (1.6). In Section 3 we evaluate the functions

$$\omega_x = \omega_3 - 2\omega_r\ , \quad \omega_y = 4(\omega_{4-} - \omega_{4+}) \tag{1.8}$$

for G_n and ω_x^+ and ω_y^+ for G_n^+. Then, applying (1.7a,b,c) we get

$$\begin{bmatrix} 4\,\omega_{3t} \\ 8\,\omega_{st} \\ 16\,\omega_{4-} \end{bmatrix} = \begin{bmatrix} 1 & 1 & -3 \\ -3 & 1 & 5 \\ 3 & -1 & 3 \end{bmatrix} \begin{bmatrix} (\omega_3 - m_{3t})\omega_t \\ (\omega_s - m_{st})\omega_t - 3m_{rs}\omega_r \\ \omega_r\omega_t - m_{rs}\omega_s + \omega_y/2 \end{bmatrix} \tag{1.9}$$

with corresponding formulas for G_n^+. Thus the ten character values can be computed explicitly for each AIC character χ 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 ϕ in G for χ of level ℓ in G_n (or in G_ℓ for χ^σ in G_n^σ) generates an extended level ℓ character Φ that contains χ (or χ^σ) 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 $\Phi = (\alpha+\beta)/2 = Y + 1$ and $(\alpha-\beta)/2 = X + 1$ that are induced in G_n by G_n^+ and G_n^-. These include the 1-character of level 0 with the level 1 AIC characters Y or X that have sign $\tau=+1$ on class C_t. The extended character Φ multiplied by the codegree d of ϕ is a linear combination of basic characters B^μ, one for each class C_μ of G_ℓ^τ (or G_ℓ), with coefficients w_μ that are the class multipliers of ϕ for C_μ. The B^μ have values B_λ^μ on each class C_λ of G_n(or G_n^σ) that are $\pm$ a power of 2 or 0. Thus we write

$$\Phi_\lambda\, d = \sum\nolimits_\mu w_\mu B_\lambda^\mu \tag{2.1}$$

$$\Phi_\lambda\, d/\alpha^\ell = 1 + W_t(\beta/\alpha) + W_3(\gamma/\alpha) + W_s(\beta/\alpha)^2 + W_r(\alpha_2/\alpha^2) \tag{2.2}$$
$$+ W_{3t}(\beta\gamma/\alpha^2) + W_{st}(\beta/\alpha)^3 + W_{4-}(\delta/\alpha^2) + W_{4+}(\beta_2/\alpha^2) + W_5(\varepsilon/\alpha^2) + \cdots$$

Values of the basic characters $\alpha, \beta, \cdots$ on four classes C_λ are

	α	α_2	β	β_2	δ	γ	ε
C_1	N^2	N^2	N	N	N	1	1
C_3	$N^2/4$	$N^2/4$	$-N/2$	$-N/2$	$-N/2$	-2	1
C_5	$N^2/16$	$N^2/16$	$-N/4$	$-N/4$	$-N/4$	1	-4
C_t	$N^2/2$	N^2	0	N	$-N$	-1	-1

(2.3)

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_i to account for any level ℓ-1 characters that may be included in Φ, we have

$$\chi_1 d/N^{2\ell} = 1+W_t/N+(W_3+W_s+W_r-D_1)/N^2+(W_{3t}+W_{st}+W_{4-}+W_{4+}-D_1W_t)/N^3+\cdots \quad (2.4a)$$

$$\chi_3 d(4/N^2)^\ell = 1-2W_t/N+(-2W_3+W_s+W_r-D_1)4/N^2+(3W_{3t}+a_3)8/N^3+\cdots \quad (2.4b)$$

$$\chi_5 d(16/N^2)^\ell = 1-4W_t/N+(W_3+W_s+W_r-D_1)16/N^2+64a_3/N^3+(a_4-5W_5)4^4/N^4+\cdots \quad (2.4c)$$

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

$$(\chi_1 d/N^{2\ell})^{-1} = 1 + a_1/N + (a_1^2 - a_2)/N^2 + (a_1^3-2a_1a_2+a_3)/N^3+\cdots \quad (2.5)$$

$$L^2\chi_3 d/N^{2\ell} = 1 + 2a_1/N + 4(a_2-3W_3)/N^2 + 8(a_3-3W_{3t})/N^3 + \cdots \quad (2.6)$$

$$L^4\chi_5 d/N^{2\ell} = 1 + 4a_1/N + 16a_2/N^2+64a_3/N^3+2^8(a_4-5W_5)/N^4+ \cdots \quad (2.7)$$

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

$$L^2\chi_3/\chi_1 = 1 +3a_1/N +3(a_1^2+a_2-4W_3)/N^2 +3(a_1^3+3a_3-4a_1W_3-8W_{3t})/N^3+\cdots \quad (2.8)$$

$$L^4\chi_5/\chi_1 = 1 +5a_1/N +5(a_1^2+3a_2)/N^2 +5(a_1^3+2a_1a_2+13a_3)/N^3+ \quad (2.9)$$
$$+5(a_1^4+a_1^2a_2-3a_2^2+14a_1a_3+51a_4-256W_5)/N^4+\cdots$$

Theorem 2.1. The class multipliers for χ and χ^+ on class C_3 are

$$\omega_3 = (T^2/2)((N^2-1)/3 + a_1(N+a_1) + a_2 - 4W_3^\tau) \quad (2.10a)$$

$$\omega_3^+ = (T^2/8)((N-1)(N-2)/3 + a_1(N+a_1-3) + a_2 - 4W_3) \quad (2.10b)$$

Proof: We multiply (2.8) by ${}^oC_3/L^2$ and ${}^oC_3^+/L^2$ from (1.4), and discard all terms in N^{-1}, $N^{-2}, \cdots$. These coefficients must vanish since ω_λ and ω_λ^+ are algebraic integers for all N and $T = \tau N/L$.

Theorem 2.2. The class multipliers for χ and χ^+ on class C_s are

$$\omega_s = (T^2/4)(N^2+1+a_1(N-a_1) -3a_2 +12W_3^T) -T(N+a_1) +1 -N^2/2 \quad (2.11a)$$

$$\omega_s^+ = (T^2/16)(N^2-N+a_1(N-a_1+5) -3a_2 +12W_3) - N(N-1)/4 \quad (2.11b)$$

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

Theorem 2.3. The class multipliers for χ and χ^+ on class C_5 are

$$\omega_5 = (T^4/2^65)[N^4+5a_1N^3+5(a_1^2+3a_2-1)N^2 +5(a_1^3-5a_1+2a_1a_2+13a_3)N +5(a_1^4-5a_1^2+a_1^2a_2-3a_2^2-15a_2+14a_1a_3+51a_4-2^8W_5) +4] \quad (2.12)$$

$$\omega_5^+ = (T^4/2^{10}5)[N^4+5(a_1-1)N^3+5(a_1^2-5a_1+3a_2)N^2+5(a_1^3-5a_1^2+4+2a_1a_2)N+5(13a_3-15a_2)N+5(a_1^4-5a_1^3+20a_1+a_1^2a_2-3a_2^2-10a_1a_2+14a_1a_3-65a_3+5a_2-4 - 16 -2^8(5W_5)] \quad (2.13)$$

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

3. Formulas generated by level n characters. Next let λ in G_n be the parent of a level n character ζ^+ in G_z^+ whose roots R_j are

R_j: 1, ±2, ±4, $\cdots\pm T/2$, $-r_iT$, $-NT$, with all roots r_i of χ (3.1a)

and let χ^+ of G_n^+ be the parent of ζ in G_z, whose roots $\bar{R}_j$ are

$\bar{R}_j$: ±1, $\pm2,\cdots,\pm T/4$, $T/2$, $-\bar{r}_iT/2$, $-NT/2$, with all roots $\bar{r}_i$ of χ^+ (3.1b)

where $Z = 2^z$ plays the role of N in Section 2, and Λ the role of L.

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

$$-A_1 = \omega_t = T(N+a_1) - 1, \quad A_2-A_1 = T^2(Na_1+a_2) - (T^2-1)/3 \quad (3.2a)$$

$$-\bar{A}_1 = \omega_t^+ = (T/2)(N+a_1-1), \quad \bar{A}_2 = (T/2)^2((N-1)(a_1-1)+a_2)-(T^2-1)/3$$

$$A_3-A_1(A_2-A_1+1) = T^3(Na_1(N+a_1) + a_1a_2) \quad \text{for } G_n \quad (3.3a)$$

$$\bar{A}_3-\bar{A}_1\bar{A}_2 = (T/2)^3((N-1)(a_1-1)(N+a_1) + a_1a_2-a_3) \quad \text{for } G_n^+ \quad (3.3b)$$

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

$$\zeta_1^+ d/z^{2n} = 1 + \omega_t/z +(\omega_3+\omega_s+\omega_r-D)/z^2 + (\omega_{3t}+\omega_s+\omega_{4-}+\cdots)/z^3+\cdots \quad (3.4)$$

$$= 1 - A_1/z + A_2/z^2 - A_3/z^3 + \cdots$$

$$\zeta_t^+ d(2/z^2)^n = 1 + 0/z +(-\omega_3+2\omega_r-D)2/z^2 + (-4\omega_{4-}+4\omega_{4+})/z^3+\cdots \quad (3.5)$$

The class multiplier for ζ^+ on C_t is $(z/2N)(z+A_1-1)$ by (1.5).

Theorem 3.1. The class multiplier functions ω_x and ω_y for G_n are

$$\omega_x = \omega_3 - 2\omega_r = T^2(Na_1+a_2) - (T^2-1)/3 + N^2-1 \tag{3.6}$$

$$\omega_y = 4(\omega_{4-}-\omega_{4+}) = T^3(Na_1(N+a_1) + a_1a_2-a_3) \tag{3.7}$$

Proof: ${}^oC_t = Z(Z-1)/2$ for G_z^+, so $N\zeta_t^+/\zeta_1^+ = 1+A_1/(Z-1)$. By (1.4)

$$\omega_x + 2D = \omega_3-2\omega_r+2(\omega_3+\omega_s+\omega_r-A_2) = 3\omega_3+2\omega_s-2A_2$$
$$= \omega_t^2 - {}^oC_t - 2A_2 = A_1^2 - 2A_2 - (N^2-1) \tag{3.8}$$

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

$$N\zeta_t^+ d/Z^{2n} = 1 - (\omega_x + A_1^2-A_2-N^2+1)/Z^2 - \omega_y/Z^3 + \ldots \tag{3.9}$$
$$= (1 +A_1/Z +A_1/Z^2 +A_1/Z^3+\cdots)(1 -A_1/Z +A_2/Z^2 +A_3/Z^3+\cdots)$$

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 ω_x^+ and ω_y^+ for G_n^+ are

$$\omega_x^+ = \omega_3^+ - 2\omega_r^+ = (T/2)^2((N-1)(a_1-1)+a_2) - (T^2+2)/3+\tfrac{1}{2}N(N+1) \tag{3.10}$$

$$\omega_y^+ = 4(\omega_{4-}^+-\omega_{4+}^+) = (T/2)^3((N-1)(a_1-1)(N+a_1)+a_1a_2-a_3)+\tfrac{1}{2}NT(N+a_1-1) \tag{3.11}$$

Proof: We replace ζ^+ by ζ, A_i by $\bar{A}_i$ and ω_λ by ω_λ^+ in (3.4) and (3.5), and note that $N\zeta_t/\zeta_1 = (Z^2+\bar{A}_1Z-N)/(Z^2-1)$. Then

$$N\zeta_t d/Z^{2n} = 1 - (\omega_x^+ + \bar{A}_1^2-2\bar{A}_2 - N(N-1)/2)/Z^2 - \omega_y^+/Z^3 +\cdots \tag{3.12}$$
$$=(1 +\bar{A}_1/Z -(N-1)/Z^2 +A_1/Z^3+\cdots)(1-\bar{A}_1/Z +\bar{A}_2/Z^2-\bar{A}_3/Z^3+\cdots)$$

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

$$\omega_x^+ = \bar{A}_2 + (N-1)(N/2 +1), \quad \omega_y^+ = \bar{A}_3 - \bar{A}_1\bar{A}_2 - \bar{A}_1N \tag{3.13}$$

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

Reference

1. J.S.Frame, Degree polynomials for the orthogonal groups over GF(2). Mathematical Reports, vol. 2, no. 5 (1980), 253-258.

Michigan State University
East Lansing, Michigan

Received December 5, 1984.

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 α. The measurable solutions of (1) have recently been found by Kannappan and Sahoo [5].

1. Introduction

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

$$(1)\qquad \sum_{i=1}^{k}\sum_{j=1}^{\ell} f(p_iq_j)=\sum_{i=1}^{k} f(p_i)+\sum_{j=1}^{\ell} f(q_j)+\lambda\sum_{i=1}^{k} f(p_i)\sum_{j=1}^{\ell} f(q_j)$$

where $f:[0,1]\to R$, $P\in\Gamma_k$, $Q\in\Gamma_\ell$, $\lambda=2^{1-\alpha}-1\neq 0$ has been used to characterize the entropy of degree α

$$H_n^{\alpha}(P)=(2^{1-\alpha}-1)^{-1}\left(\sum_{i=1}^{n} p_i^{\alpha}-1\right)\qquad(\alpha\neq 1).$$

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 $P\in\Gamma_k^0$, $Q\in\Gamma_\ell^0$. 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 $P \in \Gamma_k^\circ, Q \in \Gamma_\ell^\circ$

Introducing $g(p)=p+\lambda f(p)$ $p \in (0,1)$ equation (1) goes over into

$$\sum_{i=1}^{k}\sum_{j=1}^{\ell}\left[g(p_iq_j)-g(p_i)g(q_j)\right]=0 \qquad (P\in\Gamma_k^\circ, Q\in\Gamma_\ell^\circ). \tag{2}$$

The general solution of (2) is given by

THEOREM 1. Let $k,\ell \geq 3$ be fixed integers. The function $g:(0,1)\longrightarrow R$ satisfies (2) if and only if either

$$g(p)=a(p)+b \qquad p\in(0,1) \tag{3}$$

or

$$g(p)=A(p)+h(p) \qquad p\in(0,1), \tag{4}$$

where $a,A:R\longrightarrow R$ are additive functions with $A(1)=0$, $h:(0,1)\longrightarrow R$ 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

$$a(1)+k\ell b=[a(1)+kb][a(1)+\ell b] \tag{5}$$

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 $\Phi:(0,1)\longrightarrow R$ satisfies the functional equation

$$\sum_{i=1}^{k}\Phi(p_i)=c \qquad (P\in\Gamma_k^\circ) \tag{6}$$

if and only if there exists an additive function $a:R\longrightarrow R$ and a constant b such that

$$\Phi(p)=a(p)+b \qquad p\in(0,1) \tag{7}$$

and

$$a(1)+kb=c \tag{8}$$

holds.

Since from (8) $b=a(-1/k)+c/k$ equation (7) can also be written as

(9) $$\Phi(p)=a(p-1/k)+c/k \qquad p\in(0,1).$$

Applying our lemma for the function

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

we obtain from (2)

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

where $A_1:R\times\Gamma_\ell^0\to R$ is an additive function in the first variable. Let now $P=(P_1,\dots,P_\ell)\in\Gamma_\ell^0$ and substitute in (10) pp_i for p $i=1,\dots,\ell$. Adding the equations so obtained and using (10) again to calculate $\sum_{i=1}^{\ell} g(pp_i)$, we get

(11) $$\sum_{i=1}^{\ell}\sum_{j=1}^{\ell}\left[g(pp_iq_j)-g(p)g(p_i)g(q_j)\right]=$$
$$=A_1(p-\ell/k,q_1,\dots,q_\ell)+A_1(p-1/k,P_1,\dots,P_\ell)\sum_{j=1}^{\ell}g(q_j).$$

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

(12) $$A_1(p-\ell/k,q_1,\dots,q_\ell)+A_1(p-1/k,P_1,\dots,P_\ell)\sum_{j=1}^{\ell}g(q_j)=$$
$$=A_1(p-\ell/k,P_1,\dots,P_\ell)+A_1(p-1/k,q_1,\dots,q_\ell)\sum_{i=1}^{\ell}g(p_i).$$

Putting here $p=1/k$ we conclude that

(13) $$A_1(1,q_1,\dots,q_\ell)=\text{constant}=c_1.$$

Substituting (13) into (11) we have

(14) $$A_1(p,q_1,\dots,q_\ell)(1-\sum_{i=1}^{\ell}g(p_i))+c_1/k\sum_{i=1}^{\ell}g(p_i)=$$
$$=A_1(p,P_1,\dots,P_\ell)(1-\sum_{j=1}^{\ell}g(q_j))+c_1/k\sum_{j=1}^{\ell}g(q_j).$$

We shall distinguish two cases.

Case 1. If $\sum_{i=1}^{\ell}g(p_i)=1$ for all $P\in\Gamma_\ell^0$ then by our lemma

$$g(p)=a(p)+b \qquad p\in(0,1)$$

i.e. (3) holds.This function satisfies (2) if and only if (5) is true.

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

$$A_1(p,q_1,\dots,q_\ell)=A(p)\Big(1-\sum_{j=1}^{\ell} g(q_j)\Big)+d\sum_{j=1}^{\ell} g(q_j)+e, \tag{15}$$

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

$$\sum_{j=1}^{\ell}\big[g(pq_j)-g(p)g(q_j)\big]=A(p-1/k)\Big(1-\sum_{j=1}^{\ell} g(q_j)\Big)+A(1)\sum_{j=1}^{\ell} g(q_j)+e. \tag{16}$$

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

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

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

Returning to (16) we have

$$\sum_{j=1}^{\ell}\big[g(pq_j)-g(p)g(q_j)\big]=A(p)\Big(1-\sum_{j=1}^{\ell} g(q_j)\Big)$$

or with $h(p)=g(p)-A(p)$, $p\in(0,1)$.

$$\sum_{j=1}^{\ell}\big[h(pq_j)-h(p)h(q_j)\big]=0 \qquad p\in(0,1),Q=(q_1,\dots,q_\ell)\in\Gamma_\ell^0. \tag{17}$$

By the lemma,

$$h(pq)-h(p)h(q)=E(p,q-1/\ell) \quad p,q\in(0,1) \tag{18}$$

where $E:(0,1)\times R\longrightarrow R$ is an additive function in the second variable. For any $p,q,r\in(0,1)$ we have from (18)

$$h(pqr)-h(p)h(q)h(r)=$$
$$=E(pq,r-1/\ell)+h(r)E(p,q-1/\ell)=E(p,qr-1/\ell)+h(p)E(q-1/\ell). \tag{19}$$

Case 2.1.If $E(p,q-1/\ell)=0$ 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)

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

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 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. □

Returning to the original equation (1) we have

THEOREM 2.The function $f:(0,1)\longrightarrow R$ satisfies (1) for all $p\in\Gamma_k^\circ, Q\in\Gamma_\ell^\circ$ (where $\lambda\neq 0,k,\ell\geq 3$ are fixed integers) if and only if

$$f(p)=\frac{a(p)-p+b}{\lambda}\qquad p\in(0,1)$$

or

$$f(p)=\frac{A(p)-p+h(p)}{\lambda}\qquad p\in(0,1),$$

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

REFERENCES

[1] Aczél, J., Information functions on open domain III. C.R.Math.Rep. Acad.Sci.Canada 2 (1980), 281-285.

[2] Behara, M. and Nath, P., Additive and nonadditive entropy of finite measurable partitions. Probability and Information Theory, Vol.2 Springer-Verlag 1973, V.296, 102-138.

[3] Kannappan, Pl., On a generalization of some measures in information theory. Glasnik Mat. 29 (1974), 81-93.

[4] Kannappan, Pl., On some functional equations from additive and non-additive measure-I. Proc. Edinburgh Math. Soc. 23 (1980), 145-150.

[5] Kannappan, Pl. and Sahoo, P.K., On a functional equation connected to sum form nonadditive information measures on an open domain. C.R.Math.Rep.Acad.Sci.Canada (this issue).

[6] Losonczi, L., A characterization of entropies of degree α. Metrika 28 (1981), 237-244.

[7] Losonczi, L., Functional equations of sum form. Publ.Math.Debrecen (to appear).

[8] Losonczi, L. and Maksa, Gy., On some functional equations of the information theory. Acta Math.Acad.Sci.Hung. 39 (1982), 73-82.

[9] Sahoo, P.K., On some functional equations connected to sum form information measures on open domains. Utilitas Math. 23 (1983), 161-175.

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.

UNITES DE CERTAINS SOUS-ANNEAUX DE CORPS DE FONCTIONS ALGEBRIQUES

R. PAYSANT-LE ROUX, D.L. Mc QUILLAN, Y. HELLEGOUARCH

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

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) Etude algébrique du cas général

Nous appellerons "place à l'infini" de K, la place constante sur k qui envoie $\frac{1}{X}$ 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) $\mathrm{div}(\varphi) \in \mathcal{M}$

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 π_1 et π_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 $\mathcal{M}_0 = \mathcal{D}_0 \cap \mathcal{M}$, $\mathcal{N}_0 = \mathcal{D}_0 \cap \mathcal{N}$.

Théorème 2.- Soit $\mathcal{P}$ le groupe des diviseurs principaux de E, alors si l'on désigne par $\mathcal{G}$ le groupe $\mathcal{U}/k^*$ on peut dire que :

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

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

Si l'on désigne par J le groupe $\mathcal{D}^0/\mathcal{P}$ (jacobienne de E), par J_∞ le sous-groupe $\mathcal{M}_0/\mathcal{M}_0 \cap \mathcal{P}$ et par T le sous-groupe de torsion de J_∞ on a :

Corollaire

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

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

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 φ vérifie :

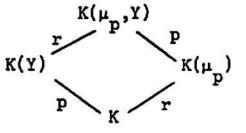
$$(\forall \varphi' \in B \setminus \{0\},\ v_{P_i}(\varphi') \geq v_{P_i}(\varphi) \text{ pour } i = 0,\ldots,t-1) \Rightarrow (\exists \lambda \in k^*,\ \varphi' = \lambda\varphi).$$

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) Etude 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 pn (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 $\Delta = X^n + \ldots$ 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 μ_p le groupe des racines $p^{ième}$ de l'unité dans $\bar{k}$, on a la situation :



avec $r \leqslant \varphi(p)$ et isomorphisme des groupes de Galois sur les côtés opposés du parallélogramme.

Nous poserons $G = \mathrm{Gal}(k(\mu_p)/k) \subseteq (\mathbb{Z}/p\mathbb{Z})^*$. G opère sur μ_p et on désigne par $d(k)+1$ le nombre d'orbites de μ_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) rang $\mathcal{G} \leqslant d(k)$.

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

b) Définition des meilleures approximations : Soit $U = (U_0, U_1, \ldots, U_{p-1}) \in A^p$, 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 ζ un générateur de μ_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 :

$$\begin{cases} \deg U = \mathrm{Max}\ \deg U_0, \deg U_1\Delta, \ldots, \deg U_{p-1}\Delta^{p-1} \\ N(U) = \deg\,[\mathcal{P}_{E/K}(U)] \\ \phi_h(U) = \sum_{\zeta^i \in \omega_h} \deg \varphi_i(U), \qquad h = 0, \ldots, d(k) \end{cases}$$

où $\omega_0, \ldots, \omega_{d(k)}$ sont les orbites de μ_p sous l'action de G.

On dira donc que $U \in A^p$ est une meilleure approximation (ou m.a.) si $U \neq 0$ et si U vérifie la propriété :

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

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

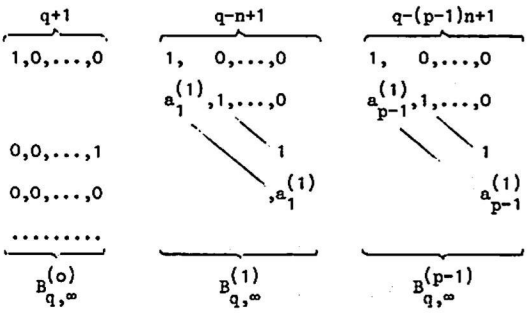
$$(U \text{ est une m.a. et } \phi_o(U) \leqslant 0) \Leftrightarrow (\forall U' \neq \lambda U,\ \lambda \in k^*,\ \phi_o(U') \leqslant \phi_o(U) \leqslant 0 \Rightarrow \deg U' > \deg U)$$

Construction des m.a. $\varphi(U)$ telles que $\phi_o(U) \leqslant 0$ sous l'hypothèse p premier et $[k(\mu_p).k] = p-1$

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

$$U_i = u_i^{(0)} X^{q-in} + u_i^{(1)} X^{q-in-1} + \ldots + u_i^{(q-in)}, \quad 0 \leqslant i \leqslant p-1$$
$$\Delta^i = X^{in} + a_i^{(1)} X^{in-1} + \ldots + a_i^{(in)}, \quad 1 \leqslant i \leqslant p-1$$

On considère la matrice $A_{q,\infty}$ ayant ℓ_q colonnes, formée des blocs



Soit $\tilde{U} \in k^{\ell q}$, $\tilde{U} = (\underbrace{u_o^{(o)},\ldots,u_o^{(q)}}_{U_o},\ldots,\underbrace{u_{p-1}^{(o)},\ldots,u_{p-1}^{(q-(p-1)n)}}_{U_{p-1}})$

Soit $A_{q,m}$ la matrice tronquée, ayant comme m lignes, les m premières lignes de $A_{q,\infty}$.

Soit m_q le plus grand entier tel que le système $A_{q,m-1}\tilde{U} = 0$, admette une solution non triviale.

Théorème 4.-

- "la" solution, définie à une constante multiplicative près, du système $A_{q,m_q-1}\tilde{U} = 0$ est une m.a. de degré inférieur ou égal à q.

- Réciproquement toute m.a. U avec $\phi_o(U) \leqslant 0$ est construite de cette façon.

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

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

Définitions 1.- Soient φ et ψ deux éléments de E^*, on dit que φ est équivalent à ψ s'il existe λ appartennant 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 $\alpha_i = \dfrac{\varphi(U^{(i+1)})}{\varphi(U^{(i)})}$ est telle qu'il existe $\pi \geqslant 1$, $\alpha_{q\pi+r} \sim \alpha_r$, $\forall q \geqslant 0$, $0 \leqslant r \leqslant \pi-1$.

Théorème 5.- $\mathcal{G}$ 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 $v_0(\varphi(U)) = -\phi_0(U)$ (resp. $v_1(\varphi(U)) = -\phi_1(U)$).

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

2) De plus, on a :

a) $\ell = \deg U^{(\pi)}$, où $U^{(\pi)}$ est la m.a. de rang π, π étant la pseudo période de la suite des m.a.

b) i) Si $p = 2$, $\pi + n - 1 \leqslant \ell \leqslant 1 + \pi(n-1)$

ii) Si $p \geqslant 3$,
$$\begin{cases} \pi + n - 1 \leqslant \ell \leqslant n + [\frac{pn}{2}](\pi - 1) & \text{si } n \leqslant p-1 \\ \pi + n - 1 \leqslant \ell \leqslant n + \frac{(p+1)n}{2}(\pi - 1) & \text{si } n > p-1 \end{cases}$$

Corollaire.- Si $p = 2$ et $n = 2$, $\ell = \pi + 1$; Si $p = 3$ et $n = 1$, $\ell = \pi$.

REFERENCES

[1] E. Artin, "Quadratische Körper im Gebiet der höheren Kongruenzen I,II", Math. Zeitschrift 19 (1924) pp. 153-246 (Thesis).

[2] M. Deuring, "Lectures on the theory of algebraic functions of one variable". Lecture Notes in Mathematics, n° 314.

[3] Y. Hellegouarch - M. Lozach, "Equation de Pell et points d'ordre fini". Colloque "Théorie analytique et élémentaire des nombres", 30 mai - 3 juin 1983 (à paraître).

[4] M. Neubrand, "Einheiten in algebraischen Funktionen und Zahlkörpern", J. Reine Angew. Math. 303/304 (1978), S. 170-204.

[5] A. Schinzel, "On some problems of the arithmetical theory of continued fractions", Acta Arithmetica VI 1961 and VII 1962.

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 Φ_E, Φ_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

$$
\begin{array}{ccc}
 & \overset{\Phi_E}{} & \\
E & \to & E \\
\downarrow & & \downarrow \\
Y & \overset{f}{\to} & Y
\end{array}
\qquad
\begin{array}{ccc}
 & \overset{\Phi_F}{} & \\
F & \to & F \\
\downarrow & & \downarrow \\
Y & \overset{f}{\to} & Y
\end{array}
\tag{1.1}
$$

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

$$Y^f = I \times Y / f \tag{1.2}$$

where we identify $(1,y) \sim (0,f(y))$, and the bundles

$$E^\Phi = I \times E / \Phi \quad \text{and} \quad F^\Phi = I \times F / \Phi \,. \tag{1.2'}$$

Any first order elliptic differential operator

$A : C^\infty(Y^f; E^\Phi) \to C^\infty(Y^f; F^\Phi)$ takes the form

$$\alpha(t,y)\ (\frac{\partial}{\partial t} + B(t,y))$$

where $\alpha(t,y) : E \to F$ is a bundle isomorphism and $B(t,\cdot) : C^\infty(Y, E) \to C^\infty(Y, E)$ 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

$$\alpha(\frac{\partial}{\partial t} + B_t) \tag{1.3}$$

where α is an isomorphism which doesn't depend on t, and $\{B_t\}_{t\in I}$ 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

$$As(1,y) = \Phi_F((As)(0,y))$$

for any section s of E^Φ $(s(1,y) = \Phi_E s(0,y))$.
Using (1.3) we get the following conditions

$$\Phi_F = \alpha \circ \Phi_E \quad \text{and} \quad B_1 = (\Phi_E)^{-1} B_o \Phi_E . \tag{1.4}$$

For the principal symbol of B_t this means exactly

$$\Phi_E(y)\ \sigma(y,\zeta)\ v = \sigma(f(y), (f^{-1})^*\zeta)\ \Phi_E(y)\ v \tag{1.5}$$

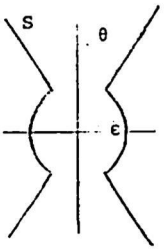
where $\zeta \in T_y^*Y$, $v \in E_y$.

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_t 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_t has a discrete spectrum and only finitely many eigenvalues in the region S of Fig. 1.6 for sufficiently small ε, θ (see e.g. [7]), and therefore we can assume that B_o has no eigenvalues on the imaginary axis.

(1.6)



We denote by P_+ (P_-) the spectral projection onto the direct sum of the eigenspaces of B_o 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*

$$\text{index } (P_+ - \Phi_E P_-) = \text{index } A \,. \tag{1.7}$$

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

tion. Now Φ_F commutes with σ so it commutes with its spectral projections

$$\Phi_E(y)\ p_\pm(y,\zeta) = p_\pm(y,\zeta)\ \Phi_E(y), \tag{2.1}$$

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

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

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

(II) We meet here a pair of projections in $L^2(Y; E)$ such that $P_+ + P_- = id$, $P_\pm P_- = P_- P_+ = 0$. The set of all linear automorphisms ψ 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* $\Phi_E^{\,k} = id$ *for some integer* k, *then* index $(A) = 0$.

Proof. $(P_+ - \Phi_E P_-)^{2k} = P_+ + P_- + \Sigma\ P_+\Phi_E P_- \ldots.$

$= id + \Sigma\ P_+\Phi_E P_- \ldots. = id + \text{comp. op.}$

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

$$2k\ \text{index}(P_+ - \Phi_E P_-) = \text{index}(P_+ - \Phi_E P_-)^{2k} = \text{index}(id + \text{comp.}) = 0.$$

3. Proof of Theorem 1. It is easy to check

$$\text{index}(P_+ - \Phi_E P_-) = \dim\{f \in \text{Range } P_- \mid \Phi_E f \in \text{Range } P_+\} - \dim\{f \in \text{Range } P_+ \mid \Phi_E f \in \text{Range } P_-\} \quad (3.1)$$

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 $\Phi_E^{-1} B_o \Phi_E = B_1$, 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 $S^1 \times S^1$

$$B_{s,t} = \begin{cases} i\cos(s) + \sin(s)\, B_t & 0 \leqslant s \leqslant \pi \\ e^{i(s+\frac{\pi}{2})} & \text{if} \\ & \pi \leqslant s \leqslant 2\pi \end{cases} \quad (3.2)$$

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_o.

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

$$K(S^1 \times S^1/S^1) \simeq K^{-1}(S^1) \simeq Z$$

which we call the *analytical index* of the family $\{B_t\}$. In fact it is equal to the spectral flow of the family ([1],

[8]). 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. index A = index $\{B_t\}$.

Proof. We have to compare the index formula for one operator on Y^f 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

1. Atiyah, M.F., Patodi, V.K. & Singer, I.M., Spectral asymmetry and Riemannian geometry. I, III, *Math. Proc. Camb. Phil. Soc. 77* (1975), 43-69 and *79* (1976), 71-99.
2. Atiyah, M.F. & Singer, I.M., The index of elliptic operators. IV, *Ann. of Math. 93* (1971), 119-138.
3. van Baal, P., Some results for SU(N) gauge fields on the hypertorus, *Comm. Math. Phys. 85* (1982), 525-547.
4. Booss, B. & Wojciechowski, K., *Desuspension of Splitting Elliptic Symbols*, Tekst 52, IMFUFA, Roskilde, 1982.
5. Gilkey, P.B. & Smith, L., The twisted index problem for manifolds with boundary, *J. Differential Geom. 18* (1983), 393-444.
6. t'Hooft, G., Some twisted self-dual solutions for the Yang-Mills equations on a hypertorus, *Comm. Math. Phys. 81* (1982), 267-275.
7. Shubin, M., *Pseudodifferential Operators and Spectral Theory*, Nauka, Moscow, 1978. (Russian)
8. Wojciechowski, K., Spectral flow and the general linear conjugation problem. To appear in *Simon Stevin*.

B.B.
Institut for Studiet af
Matematik og Fysik
Roskilde Universitetscenter
DK-4000 Roskilde.

K.W.
Instytut Matematyczny
Uniwersytet Warszawski
PL-00-901 PKiN Warszawa

Received January 2, 1985.

Mailing Addresses

1. T. Agoh
   Department of Mathematics
   Science University of Tokyo
   Noda, Chiba 278, Japan

2. D. Betten
   Mathematisches Seminar der
   Universität Kiel
   Olshausenstrasze 40
   D-2300 Kiel, F.R. Germany

3. T. Bisztriczky
   Department of Mathematics
   University of Calgary
   Calgary, Alberta, Canada T2N 1N4

4. B. Booss
   Institut for Studiet af Matematikog Fysik
   Roskilde Universitetscenter
   DK-4000 Roskilde

5. R. Carroll
   Mathematics Department
   University of Illinois
   Urbana, IL 61801, U.S.A.

6. J.S. Frame
   Department of Mathematics
   Michigan State University
   East Lansing, MI 48823, U.S.A.

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

8. Y. Hellegouarch
   Département de Mathematiques
   Université de Caen
   Caen, France

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

10. Pl. Kannappan
    Faculty of Mathematics
    University of Waterloo
    Waterloo, Ontario, Canada N2L 3G1

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

12. P. Lentoudis
    Université de Patras
    Département de Mathématiques
    Patras - Greece

13. L. Losonczi
    Department of Mathematics
    University of Lagos
    Lagos, Nigeria

14. D.L. McQuillan
    Department of Mathematics
    University College
    Dublin, Ireland

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
Universität Kiel
Olshausenstrasze 40
D-2300 Kiel, F.R. Germany

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