C. R. Math. Rep. Acad. Sci. Canada - Vol. 1 (1979) No. 3

Mailing Addresses

1. Aczel, J. Department of Pure Mathematics, University of Waterloo, Waterloo, Ont. Canada M2L 3G1

2. Bellman, R. Dept. of Mathematics, Electrical Engineering and Medicine, University of Southern California, Los Angeles, California 90007 U.S.A.

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

4. Herrmann, R.A. Dept. of Mathematics, U.S. Naval Academy, Annapolis, Maryland 21402 U.S.A.

5. Hilton, P. Department of Mathematics, Case Western Reserve University, Cleveland, Ohio 44106 U.S.A.

6. Hirschfeld, J.W.P. Mathematics Division, University of Sussex, Brighton, England BN1 9QH

7. Hopkins, G.H. Department of Mathematics, University of Mississippi, University, Miss. 38677 U.S.A.

8. Hubaut, X. Dépt. de Mathématiques, Université Libre de Bruxelles, Blvd. du Triomphe 1050, Bruxelles, Belgium

9. Jonker, L. Department of Mathematics and Statistics, Queen's University, Kingston, Ont. Canada K7L 3N6

10. Leite, P. Universidade de São Paulo, São Paulo, Brazil

11. Lipman, J. Purdue University, West Lafayette, Indiana 47907 U.S.A.

12. Makkai, M. Department of Mathematics, McGill University, Montréal, P.Q. Canada H3A 2K6

13. Phillips, J. Department of Mathematics, Dalhousie University, Halifax, N.S. Canada B3H 3J5

14. Raeburn, I. School of Mathematics, University of New South Wales, P.O. Box 1, Kensington NSW 2033 Australia

15. Rand, D. Math. Institute, University of Warwick, Coventry, England CV4 7AL

16. Rigby, J.F. University College, Cardiff, Wales U.K. CF1 1XL

17. Smith, R.A. Department of Mathematics, University of Toronto, Toronto, Ontario Canada M5S 1A1

18. Snapper, E. Department of Mathematics, Dartmouth College, Hanover, New Hampshire, 03755 U.S.A.

19. Thas, J.A. Seminar of Higher Geometry, University of Ghent, Krijgslaan 271, 9000 Ghent, Belgium

C. R. Math. Rep. Acad. Sci. Canada - Vol. 1 (1979) No. 3

On nilpotent spaces and $\mathcal{C}$-theory

by

Peter Hilton and Paulo Leite

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

0. Introduction.

In this note we make a new approach to the programme of generalizing methods which have proved highly serviceable in the homotopy theory of simply-connected spaces to the study of nilpotent spaces [1]. We work in the context of the generalization of Serre's application of the concept of class of abelian groups introduced in [2]; thus we consider a class $\mathcal{C}$ of nilpotent groups verifying suitable axioms and our principal result asserts that, if Y is a nilpotent space whose fundamental group belongs to $\mathcal{C}$ and if $p:\tilde{Y} \to Y$ is the projection of the universal cover of Y, then p induces $\mathcal{C}$-bijections $p_*: H_i\tilde{Y} \to H_iY$, $i \geq 1$. As a consequence, we obtain a version of the mod $\mathcal{C}$ Hurewicz Theorem for nilpotent (or even homologically nilpotent) spaces which is an improvement on the version given in [2]. We would expect to be able to obtain the mod $\mathcal{C}$ version of the Whitehead Theorem for nilpotent spaces in this way, too.

1. Algebraic preliminaries.

Let $\mathcal{C}$ be a non-empty class of nilpotent groups. We consider the following properties which $\mathcal{C}$ might have:

(S: Serre property) If $N \rightarrowtail G \twoheadrightarrow Q$ is a central extension of nilpotent groups, then $N,Q \in \mathcal{C} \Leftrightarrow G \in \mathcal{C}$;

(A: acyclicity) If $\pi \in \mathcal{C}$, then $H_i\pi \in \mathcal{C}$, $i \geq 1$;

(completeness)* If A,B are abelian groups with $A \in \mathcal{C}$, then $A \otimes B \in \mathcal{C}$.

*On categorical grounds it would be better to call this property 'cocompleteness'.

We then observe that the following proposition holds.

Proposition 1.1 If A, B are abelian groups and $\mathcal{C}$ is a class satisfying property S, then, if $A \in \mathcal{C}$, we may infer that

$$A \otimes B \in \mathcal{C}, \quad \mathrm{Tor}(A,B) \in \mathcal{C},$$

provided that $\mathcal{C}$ is complete or B is finitely generated.

Corollary 1.2 Let $\mathcal{C}$ be a class satisfying properties SA, let $\pi \in \mathcal{C}$, and let π act nilpotently on the abelian group B. Then $H_i(\pi;B) \in \mathcal{C}$, $i \geq 1$, provided that $\mathcal{C}$ is complete or B is finitely generated.

Proposition 1.3 Under the hypotheses of Corollary 1.2,

$$I[\pi] \otimes_{\pi} B \in \mathcal{C},$$

where $I[\pi]$ is the augmentation ideal in the integer group ring of π.

Corollary 1.4 Under the hypotheses of Corollary 1.2, the projection

$$\rho : B \twoheadrightarrow B_{\pi}$$

is $\mathcal{C}$-bijective, where B_{π} is obtained from B by killing the action of π.

2. Topological results.

Let Y be a nilpotent space, and let $\bar{Y}$ be a regular covering space of Y with cover transformation group π. Let $p : \bar{Y} \to Y$ be the covering map, inducing $p_* : H_i\bar{Y} \to H_iY$.

Proposition 2.1 The group π operates nilpotently on the homology of $\bar{Y}$.

Theorem 2.2 *If* $\pi \in \mathcal{C}$, *a class satisfying properties SA, then* $p_* : H_i\bar{Y} \to H_iY$ *is* $\mathcal{C}$-*bijective*, $i \geq 1$, *provided that* $\mathcal{C}$ *is complete or* Y *is of finite type*.

Sketch of proof. We consider the homology spectral sequence of the covering $\bar{Y} \to Y \to K(\pi,1)$. Then we have $(H_i\bar{Y})_\pi = E^2_{0i} \twoheadrightarrow \ldots \twoheadrightarrow E^n_{0i} \twoheadrightarrow E^{n+1}_{0i} \twoheadrightarrow \ldots \twoheadrightarrow E^{i+1}_{0i} = E^\infty_{0i} = F_0H_iY \subseteq F_1H_iY \subseteq \ldots \subseteq F_{p-1}H_iY \subseteq F_pH_iY \subseteq \ldots \subseteq F_iH_iY = H_iY$, where the kernel of $E^n_{0i} \twoheadrightarrow E^{n+1}_{0i}$ is the d^n-image of $E^n_{n,i-n+1}$, and the cokernel of $F_{p-1}H_iY \subseteq F_pH_iY$ is $E^\infty_{p,i-p}$. Now $E^2_{pq} = H_p(\pi; H_q\bar{Y}) \in \mathcal{C}$ for $p \geq 1$ by Corollary 1.2 and Proposition 2.1 (note that if Y is of finite type so is $\bar{Y}$). Thus, by property S, the d^n-image of $E^n_{n,i-n+1}$ $(n \geq 2)$ and $E^\infty_{p,i-p}$ $(p \geq 1)$ belong to $\mathcal{C}$, so that

$$(H_i\bar{Y})_\pi \to H_iY$$

is a $\mathcal{C}$-bijection (recall that property S guarantees that a composite of $\mathcal{C}$-bijections of abelian groups is again a $\mathcal{C}$-bijection). Next we invoke Corollary 1.4 to ensure that $H_i\bar{Y} \to (H_i\bar{Y})_\pi$ is $\mathcal{C}$-bijective, so that finally $p_* : H_i\bar{Y} \to H_iY$ is $\mathcal{C}$-bijective.

Corollary 2.3 *Let* $\mathcal{C}$ *satisfy properties SA and let* Y^* *be a covering of* Y *such that* $p_* : \pi_1Y^* \to \pi_1Y$ *is* $\mathcal{C}$-*surjective. Then* $p_* : H_iY^* \to H_iY$ *is* $\mathcal{C}$-*bijective, provided that* $\mathcal{C}$ *is complete or* Y *is of finite type*.

Theorem 2.4 (Hurewicz Theorem, plus addendum, for nilpotent spaces) *If* $\pi_iY \in \mathcal{C}$, $1 \leq i \leq n-1$, $n \geq 2$, *then the Hurewicz map* $h : \pi_jY \to H_jY$ *is* $\mathcal{C}$-*bijective if* $j = n$ *and* $\mathcal{C}$-*surjective if* $j = n+1$, *provided that* $\mathcal{C}$ *is complete or* Y *is of finite type*.

<u>Proof</u>. Consider the diagram

$$\begin{array}{ccc} \pi_n\tilde{Y} & \xrightarrow{\tilde{h}} & H_n\tilde{Y} \\ \downarrow{\scriptstyle p_{**}} & & \downarrow{\scriptstyle p_*} \\ \pi_n Y & \xrightarrow{h} & H_n Y \end{array} .$$

The diagram commutes; p_{**} is an isomorphsim; $\tilde{h}$ is $\mathcal{C}$-bijective [3]; and p_* is $\mathcal{C}$-bijective by Theorem 2.2. Thus h is $\mathcal{C}$-bijective. The result for $j = n+1$ is proved similarly.

REFERENCES

[1] Peter Hilton, Guido Mislin and Joseph Roitberg, <u>Localization of nilpotent groups and spaces</u>. North Holland (1975).

[2] Peter Hilton and Joseph Roitberg, Generalized C- theory and torsion phenomena in nilpotent spaces, Houston Journ. Math. 2 (1976), 525-559.

[3] Jean-Pierre Serre, Groupes d'homotopie et classes de groups abéliens, Ann. of Math. 58 (1953), 258-294.

Case Western Reserve University
Cleveland, Ohio 44106

Universidade de São Paulo,
São Paulo, Brazil

11-30-78/ts

Received November 15, 1978

AUTOMORPHISMS OF C*-ALGEBRAS AND SECOND ČECH COHOMOLOGY

John Phillips* and Iain Raeburn**

Presented by G.F.D. Duff, F.R.S.C.

If A is a C*-algebra, we let Inn A denote the group of inner automorphisms of A and let $\pi(A)$ denote the group of automorphisms which are weakly inner in every representation of A. One main result of our investigation is the identification of $\pi(A)/\text{Inn } A$, for certain C*-algebras A, including continuous trace C*-algebras. For continuous trace C*-algebras, this takes the form: $\pi(A)/\text{Inn } A \hookrightarrow H^2(\hat{A}, \mathbb{Z})$.

1. Let X be a compact space, and let E be a (locally trivial) bundle of $n \times n$ matrix algebras over X. Then the space $\Gamma(E)$ of sections of E is an algebra over the ring $C(X)$; these are called Azumaya algebras over $C(X)$. If $A = \Gamma(E)$ is such an algebra, then E determines an element of $H^1(X,G)$ (where G is the sheaf of germs of Aut $M_n(C)$-valued functions) and hence, by standard sheaf cohomology, an element $\delta(A) \in H^3(X,\mathbb{Z})$. This element always has finite order, and by a theorem of Serre (under restrictions on X) everything in the torsion subgroup of $H^3(X,\mathbb{Z})$ arises this way [6]. Now let E be a bundle over X with fibre $K(H)$, the algebra of compact operators on a separable infinite-dimensional Hilbert space, and structure group Aut $K(H)$, the group of *-automorphisms of $K(H)$ with the topology of pointwise convergence. Then $A = \Gamma(E)$ is a C*-algebra, and the same construction yields an element $\delta(A) \in H^3(X,\mathbb{Z})$; Dixmier and Douady [4] showed that every element of $H^3(X,\mathbb{Z})$ is of this form -- in fact, $H^3(X,\mathbb{Z})$ classifies such algebras up to isomorphism.

It is a standard result (due to Rosenberg and Zelinsky) that for every Azumaya algebra A over $C(X)$ there is an exact sequence

$$0 \to \text{Inn } A \to \text{Aut}_{C(X)} A \xrightarrow{\pi} \text{Pic } C(X) \cong H^2(X,\mathbb{Z})$$

where $\text{Aut}_{C(X)} A$ denotes the group of $C(X)$-algebra automorphisms of A, and

*Dalhousie University; **University of New South Wales

Inn A is the subgroup of inner automorphisms. A theorem of Knus [7,5.4] says that the range of π is contained in the torsion subroup of $H^2(X,\mathbb{Z})$. Our results concern the extension of this construction to the case where A is the C*-algebra of sections of a bundle of C*-algebras. In particular, for the K(H)-bundles of Dixmier and Douady we still have the exact sequence, and the map π is surjective, so that $H^2(X,\mathbb{Z})$ classifies the outer C(X)-algebra automorphisms of A. Complete proofs will appear elsewhere.

2. Let X be a paracompact locally compact space, and let E be a field of elementary C*-algebras over X (loosely speaking, E is a not-necessarily-locally-trivial bundle with fibre K(H): we assume H separable [3, chapter 10]) satisfying Fell's condition (locally there are sections whose values are rank one projections [3, 10.5.7]). The space $\Gamma_0(E)$ of sections which vanish at infinity is a C*-algebra with spectrum X, called a continuous trace C*-algebra. Such algebras play a crucial role in the structure theory of type I C*-algebras [3, chapters 4,9]). When the field E is locally trivial and the fibres all have dimension $\aleph_0$, we say $A = \Gamma_0(E)$ is stable; this is equivalent to imposing the condition $A \otimes K(H) \cong A$.

If A is a C*-algebra, we denote by M(A) the multiplier algebra of A (cf, e.g. [2]), and we call a *-automorphism α of A inner if there is a unitary $u \in M(A)$ such that $\alpha(a) = uau^*$ for $a \in A$. If A is a continuous trace algebra with spectrum X, then A is a module over the ring $C_b(X)$ of bounded continuous functions, and every inner automorphism is also a $C_b(X)$-module homomorphism. We denote by $\mathrm{Aut}_{C(X)}A$ the group of $C_b(X)$-module *-automorphisms, and by Inn A the group of inners. Our main theorem is:

<u>THEOREM</u>. Let A be a separable continuous trace C*-algebra with spectrum X. There is an exact sequence of groups

$$0 \longrightarrow \mathrm{Inn}\, A \longrightarrow \mathrm{Aut}_{C(X)} A \xrightarrow{\pi} H^2(X,\mathbb{Z}) .$$

If A is stable, then π is surjective.

A similar result in the case where X is compact and separable and $A = C(X,B(H))$ has been proved by Smith [9, 4.1] and is implicit in a result of Lance [8, 4.3]. Our proof follows Lance's for the trivial bundle $X \times B(H)$; ours is complicated by the presence of transition functions.

3. We observe that if $A = \Gamma_0(E)$ is a continuous trace C*-algebra with spectrum X, then (see [5]) $\mathrm{Aut}_{C(X)}A$ is precisely the set of π-inner automorphisms (i.e. weakly inner in every representation) considered by Kadison, Ringrose and Lance, among others (cf. [8] for references).

We recover from our construction theorem 3.2 of [1] that derivations of separable continuous trace C*-algebras are determined by multipliers.

4. Our construction of the homomorphism π does not depend on the specific nature of the fibres; the crucial fact is that $C(X)$-module automorphisms of $\Gamma_0(E)$ are locally inner (cf. [8],[9]). Now let B be a von Neumann algebra, and let E be a bundle with fibre B and structure group Inn B (with the norm topology) over a compact metric space X. Then we can show that every π-inner automorphism of $A = \Gamma(E)$ is necessarily locally inner; if B is a factor then the construction of section 2 gives an exact sequence with $\mathrm{Aut}_{C(X)}A$ replaced by the group of π-inners. The homomorphism π is onto if the unitary group of B is contractible -- for example, if B is a factor of type I or II . Even when B is a von Neumann algebra but not a factor, the construction works, except that now the homomorphism π takes values in $H^2(X,G)$ for a larger group G. We observe that the Dixmier-Douady arguments also work in this more general setting; that $H^3(X,\mathbb{Z})$ classifies bundles of more general Banach algebras was first noticed by Taylor [10, section 5], and it is straightforward to adapt his arguments to C*-algebras.

5. Returning to the case of C*-algebras A, with continuous trace, we determine the group $\mathrm{Aut}\, A/\mathrm{Aut}_{C(X)}A$. In fact, if $\alpha \in \mathrm{Aut}\, A$ then, in the usual way, α determines a homeomorphism of $\hat{A} = X$ and therefore an automorphism α_* of $H^3(X,\mathbb{Z})$. If we let $\mathrm{Hom}_{\delta(A)}(X)$ be the group of homeomorphisms of X whose action on $H^3(X,\mathbb{Z})$ fixes $\delta(A)$ then we get the following theorem.

<u>THEOREM</u>. Let A be a separable continuous trace C*-algebra with spectrum X. There is an exact sequence of groups

$$0 \longrightarrow \mathrm{Aut}_{C(X)}A \xrightarrow{\;i\;} \mathrm{Aut}\, A \xrightarrow{\;*\;} \mathrm{Hom}_{\delta(A)}X .$$

If A is stable, $*$ is surjective.

Acknowledgement. We'd like to thank Ian Craw for introducing us to Azumaya algebras and to Lance's work.

References

1. C.A. Akemann, G.A. Elliott, G.K. Pedersen and J. Tomiyama, Derivations and multipliers of C*-algebras, Amer. J. Math. 98 (1976) 679-708.

2. R.C. Busby, Double centralizers and extensions of C*-algebras, Trans. Amer. Math. Soc. 132 (1968) 79-99.

3. J. Dixmier, C*-algebras, North-Holland, Amsterdam 1977.

4. J. Dixmier and A. Douady, Champs continus d'espace hilbertiennes et de C*-algèbres, Bull. Soc. Math. France 91 (1963) 237-284.

5. G.A. Elliott, Ideal Preserving automorphisms of postliminary C*-algebras, Proc. Amer. Math. Soc. 27 (1971) 107-109.

6. A. Grothendieck, Le groups de Brauer I: algèbres d'Azumaya et interprétations diverses, Séminaire Bourbaki 1964/65, Exposé 290.

7. M.A. Knus, Algèbres d'Azumaya et modules projectifs, Comm. Math. Helv. 45 (1970) 372-383.

8. E.C. Lance, Automorphisms of certain operator algebras, Amer. J. Math. 91 (1969) 160-174.

9. M.-S.B. Smith, On automorphism groups of C*-algebras, Trans. Amer. Math. Soc. 152 (1970) 623-648.

10. J.L. Taylor, Twisted products of Banach algebras and third Cech cohomology, Lecture Notes in Math., vol. 575, Springer-Verlag, Berlin 1977.

Dalhousie University
University of New South Wales

Received November 16, 1978

SETS OF TYPE (1, n, q+1) IN FINITE PROJECTIVE SPACES OF EVEN ORDER q

by J.W.P. Hirschfeld, X. Hubaut and J.A. Thas

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

1. INTRODUCTION

In PG(d,q), projective space of d dimensions over the Galois field GF(q), a non-singular Hermitian variety $U_{d,q} = V(\bar{X}_0X_0 + \ldots + \bar{X}_dX_d)$ has the property that every line either lies on it or meets it in 1 or $\sqrt{q} + 1$ points : here $x \to \bar{x} = x^{\sqrt{q}}$ is the involutory automorphism of GF(q) with q necessarily a square.

If $K \subset PG(d,q)$, then a line ℓ is an i-secant of K if $|\ell \cap K| = i$. We call K a set of type (1, n, q+1) if n is a fixed integer with $1 \le n \le q$ such that every line is an i-secant for i = 1, n or q+1. Such a set is a $k_{n,d,q}$ if $|K| = k$ and some line is an n-secant. Also, K is called singular or non-singular according as it does or does not contain a point through which only 1-secants and (q+1)-secants pass. Let τ_i be the total number of i-secants of K. A subspace of r dimensions is written Π_r, and $\Pi_r L$ is the cone formed by joining Π_r to each point of L, a subset of a subspace Π_s skew to Π_r.

Tallini Scafati [5] considered whether $U_{d,q}$ could be characterized by classifying all sets $k_{n,d,q}$. The cases n = 1,2, and q are easily resolved, [4], [5]. In a proof valid only for q odd, it is shown in [5] that, for $3 \le n \le q-1$, a non-singular $k_{n,d,q}$ is a $U_{d,q}$. In [4] the problem is almost resolved for q even and d = 3; in [3] the paradoxical case of q = 4 is completely resolved for d = 3. For d = 2, see [5] and [4].

2. THE CASE $q \geq 4$

Let Q_d be a non-singular quadric in $PG(d,q)$, $q = 2^h$; then $Q_d = H_d$ (hyperbolic) or E_d (elliptic) when d is odd and $Q_d = P_d$ (parabolic) when d is even. Let S be a point off Q_d other than the nucleus when d is even.

THEOREM 1 : The projection R_{d-1} of Q_d from S to a subspace Π_{d-1} is a $k_{n,d-1,q}$ with $n = \frac{1}{2}q + 1$ and

$$k = \tfrac{1}{2}q^{d-1} + q^{d-2} + q^{d-3} + \ldots + 1 + \tfrac{1}{2}(w - 1)\, q^{(d-1)/2},$$

where $w = 2, 1, 0$ according as $Q_d = H_d$, P_d or E_d .

THEOREM 2 : If K is a non-singular $k_{n,3,q}$ such that $3 \leq n \leq q-1$ and q is even, then

(i) for $q > 4$, $K = U_{3,q}$ or $K = K_1$;

(ii) for $q = 4$, $K = U_{3,4}$ or $K = R_3$ or $K = K^*$ or K contains a triangle but no plane.

The set K_1 is specified by a long list of properties to the extent that it "looks like" R_3 , which is the only known example of K_1 . The set K^* comprises a line ℓ and four pairs (ℓ_i, ℓ_i') such that ℓ, ℓ_i, ℓ_i' are coplanar and concurrent, and such that each set of four obtained by taking one from each pair has only ℓ as transversal.

3. THE CASE $q = 4$

Every line in $PG(d,4)$ meets a $k_{3,d,4}$ in 1, 3 or 5 points. So consider sets K of odd type, namely those meeting every line in an odd number of points. The complement K^c of a set K of odd type is called a set of even type. The incidence matrix M of points and lines of PG(d,4) has $r = (4^{d+1} - 1)/3$ rows and $c = (4^{d+1} - 1)(4^d - 1)/45$ columns. If the points are P_i, $i = 1,2,\ldots, r$, then write $K^c = (a_1, a_2, \ldots, a_r)^T$, where $a_i = 1$ or 0 as P_i is or is not in K^c. The columns of M generate a vector space C^* over GF(2) and the sets of even type form its orthogonal complement C(1, d, 4), of dimension m. Then C(1, d, 4) is known as the binary (r, m) projective geometry code. For d = 2 and 3 respectively, m = 11 and 24, [1]. A more geometric point of view is to consider the sets K of odd type as forming a vector space over GF(2) where $K + K' = K \nabla K'$ is the complement of the symmetric difference of K and K'. The Hermitian varieties then form a vector subspace of dimension $(d + 1)^2$.

THEOREM 3 : The sets of even type in PG(2,4) form the binary (21, 11) projective geometry code C(1, 2, 4). The sets of odd type are as follows:

Type	Description	k	21-k	Number	τ_1	τ_3	τ_5
I	$U_{2,4}$: Hermitian curve	9	12	280	9	12	0
II	PG(2,2) : subplane	7	14	360	14	7	0
III	Oval + external line	11	10	1008	5	15	1
IV	Complement of oval	15	6	168	0	15	6
V	$\Pi_0 U_{1,4}$: 3 concurrent lines	13	8	210	2	16	3
VI	Π_1 : a single line	5	16	21	20	0	1
VII	PG(2,4)	21	0	1	0	0	21
				2^{11}			

THEOREM 4 : The sets of even type in PG(3,4) form the binary (85, 24) projective geometry code C(1, 3, 4). The sets K of odd type are as follows, where $N_I, \ldots, N_{VII}$ are the numbers of plane sections of type I,..., VII.

Type	K	k	85-k	Number	9 N_I	7 N_{II}	11 N_{III}	15 N_{IV}	13 N_V	5 N_{VI}	21 N_{VII}
1	PG(3,4)	85	0	1							85
2	Π_2	21	64	85						84	1
3	$\Pi_1 U_{1,4}$	53	32	$85.2.3.7$					80	2	3
4	$\Pi_0 K_I$	37	48	$85.2^3.5.7$	64				12	9	
5	$\Pi_0 K_{II}$	29	56	$85.2^3.3^2.5$		64			7	14	
6	$\Pi_0 K_{III}$	45	40	$85.2^4.3^2.7$			64		15	5	1
7	$\Pi_0 K_{IV}$	61	24	$85.2^3.3.7$				64	15		6
8	$U_{3,4}$	45	40	$85.2^6.7$	40				45		
9	R_3	53	32	$85.2^5.3^3.7$			32	32	20		1
10	K^*	37	48	$85.2^5.3^3.5.7$	16	32	32		4	1	
11	$\Pi_0 K_{IV} \nabla \Pi_2$	33	52	$85.2^9.3.7$	15	45	18	1		6	
12	$\Pi_0 K_{III} \nabla \Pi_2$	41	44	$85.2^{10}.3^2.7$	15	15	1+45	3	5	1	
13	$\Pi_0 K_{II} \nabla \Pi_2$	49	36	$85.2^9.3^2.5$	7	1	42	21	14		
14	$K^* \nabla \Pi_2$	45	40	$85.2^6.3^3.5.7$	8	8	48	8	1+12		
				2^{24}							

REFERENCES

[1] J.-M. Goethals and P. Delsarte, On a class of majority-logic decodable cyclic codes, IEEE Trans. Information Theory IT-14 (1968), 182-188.

[2] J.W.P. Hirschfeld, Projective geometries over finite fields, Oxford, (to appear).

[3] J.W.P. Hirschfeld and X. Hubaut, Sets of even type in PG(3,4), alias the binary (85, 24) projective geometry code, (to appear).

[4] J.W.P. Hirschfeld and J.A. Thas, Sets of type (1, n, q+1) in PG(d,q), (to appear).

[5] M. Tallini Scafati, Caratterizzazione grafica delle forme hermitiane di un $S_{r,q}$, Rend. Mat. e Appl.(5) 26 (1967), 273-303.

University of Sussex
Brighton, England

Received November 30, 1978

THE NON-WANDERING SET OF UNIMODAL MAPS OF THE UNIT INTERVAL

Leo Jonker and David Rand

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

1. INTRODUCTION

Let I denote a closed interval on the real line. A unimodal map is a C^1 map $f:I\to I$ such that f has a unique critical point which is a maximum or minimum and $f(\partial I)\subset\partial I$. Throughout this note we shall generally assume that $I = [-1,1]$ and that the critical point is a maximum at 0. There is no loss of generality.

This note is an announcement of some of the results proved in [2]. Our aim in this paper is to obtain a global canonical decomposition of the non-wandering set $\Omega(f)$ of a unimodal map f.

2. EXAMPLES

The simplest unimodal maps are unimodal maps g with zero topological entropy. We show that then $\Omega(g)$ is the closure of the periodic points plus, possibly, the orbit of $g(0)$. Moreover, every periodic orbit has period 2^m for some $m \geq 0$.

An important role is played by the maps $F_s(x) = -s|x|-(1-s)$. These are not smooth at $x = 0$, but their non-wandering sets are easy to describe, and we prove that the non-wandering set of a unimodal map has a natural description in terms of the non-wandering sets of maps such as g and F_s.

Another example of a unimodal map is given by the quadratic function

$$x \mapsto -ux^2 + u - 1$$

for $u \in (0,2]$. This particular map can have at most one attracting periodic orbit (see[1]). We prove that this result holds for any unimodal map in the following weakened sense: Let $Per(f)$ denote the set of periodic points of a unimodal map f . If $x,y \in Per(f)$, we say that x and y are (monotone) equivalent $(x \sim y)$ if f^k restricted to the closed interval between x and y is a homeomorphism for all $k \geq 0$. Orbits of equivalent periodic points are also considered (monotone) equivalent, and $[\gamma]$ is used to denote the equivalence class of the periodic orbit γ . Let $\langle x \rangle$ denote the convex hull of points in $[x]$. Suppose m is the period of x . If there is a closed interval $B_f[x] \supsetneq \langle x \rangle$ consisting entirely of points which are asymptotic to $[x]$ under iterates of f^m , this will be true for every point in the orbit γ of x . If this happens, we call $[\gamma]$ an <u>attracting periodic orbit class</u>.

ASSERTION. f <u>has at most one attracting periodic orbit class</u>.

3. THE DECOMPOSITION.

Suppose I_1 and I_2 are real intervals, and $f:I_1 \to I_1$ and $g:I_2 \to I_2$ continuous. We call f and g <u>strongly semi-conjugate</u> if f and g have the same topological entropy and there is a monotone continuous map $K:I_1 \to I_2$ such that $K \circ f = g \circ K$.

THEOREM 1. For every unimodal map there is a canonical decomposition of the non-wandering set $\Omega(f)$ of f into a finite or a countable number of non-empty closed invariant subsets Ω_j, $j=0,1,2,\ldots$, including a set Ω_∞ if the number of sets is infinite.

For every finite value of j, Ω_j is a finite union of closed sets Ω_j^0 Ω_j^1, ..., $\Omega_j^{N(j)-1}$ such that $f(\Omega_j^i) \subset \Omega_j^{i+1 (\mathrm{mod}\ N(j))}$ and such that the restrictions $f^{N(j)}|\Omega_j^i$, $i=0,1,2,\ldots$ are topologically equivalent. With the possible exception of the last component Ω_p of $\Omega(f)$, $f^{N(j)}|\Omega_j^0$ is strongly semi-conjugate to $F_{s(j)}|\Omega(F_{s(j)}) \cap (-1,1)$ for some $s(j) \in (1,2)$. If this is not true for Ω_p then one of the following holds:

(a) $p < \infty$, and $f^{N(p)}|\Omega_p^0$ is a map of zero topological entropy, or

(b) $p < \infty$, and $f^{N(p)}|\Omega_p^0$ is strongly semi-conjugate to $F_2|\Omega(F_2)$, or

(c) $p = \infty$ and $f|\Omega_\infty$ is strongly semi-conjugate to a fixed point free homeomorphism of zero entropy on a Cantor set.

The decomposition is natural under strong semi-conjugacies: If K is a strong semi-conjugacy between f and g, and if $\Omega(f) = \Omega_1 \cup \Omega_2 \cup \ldots \cup \Omega_p$ and $\Omega(g) = \bar{\Omega}_1 \cup \bar{\Omega}_2 \cup \ldots \cup \bar{\Omega}_q$, then $p \geq q$, $K(\Omega_1) \subset \bar{\Omega}_i$ for $i \leq q$, while $K(\Omega_i)$ is contained in the (periodic) g-orbit of 0 if $i > q$.

THEOREM 2. f has an attracting periodic orbit class if and only if either the exceptions (a), (b) (c) in Theorem 1 do not occur, or else (a) holds with an upper bound on the periods $N_p \cdot 2^m$ of periodic points contained in Ω_p^o .

The proofs of the theorems are obtained by analyzing the kneading invariant $\nu(f)$ of Milnor and Thurston (cf. Milnor [3]; Milnor and Thurston [4]).

REFERENCES

[1] M.P. FATOU. "Sur les equations fonctionelles." Bull. Soc. Math. de France 47 (1919) 161-271, 48 (1920) 33-94 and 208-314.

[2] L. JONKER and D.A. RAND. "Bifurcations in One Dimension. I: The Nonwandering Set". Warwick Preprint, 1978.

[3] J. MILNOR: "The Theory of Kneading" and "A Piecewise Linear Model for Kneading". Handwritten Notes, 1976 (cf.[4]).

[4] J. MILNOR and W. THURSTON. "On Iterated maps of the Interval. I and II". Preprint. Princeton University and the Institute for Advanced Study, Princeton 1977.

Queen's University
Kingston, Ont. Canada

University of Warwick
Coventry, England

Received December 8, 1978

Some Functional Equations Arising in the Calculus of Variations

by

Richard Bellman

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

1. Introduction

The purpose of this paper is to indicate some interesting functional equations arising in the minimization of quadratic functionals. The method is quite general, as we shall discuss in Section 3, but to illustrate it we shall treat the following problem: Minimize the functional

$$J(u) = \int_r^s (u'^2 + g(t)u^2)\,dt, \tag{1}$$

where u is subject to the conditions

$$u(r) = a, \quad u(s) = b. \tag{2}$$

Let us write

$$f(r,s,a,b) = \min_u J(u). \tag{3}$$

Departments of Mathematics, Electrical Engineering and Medicine
University of Southern California, Los Angeles, California 90007

We know, [1], that f is a quadratic function of a and b. We have

(4) $$f(r,s,a,b) = a^2 f_1(r,s) + ab f_2(r,s) + b^2 f_3(r,s).$$

Let us assume that $g(t)$ is positive so that the minimum exists for all r and s. We know, in this case, that f is positive definite.

2. Derivation of the Functional Equations

Let p be a point between r and s. Set

(1) $$u(p) = b.$$

Then we have

(2) $$f(r,b,a,c) = \min_c \left[f(r,p,a,c) + f(p,s,c,b) \right].$$

The minimization is easily obtained in view of the quadratic character of f. Equating the coefficients, we obtain the desired functional equations.

3. Some Generalizations

The result may easily be generalized in various ways. Let us point out some of them.

To begin with we can consider functionals involving higher derivatives, and we can consider the vector-matrix form. We may also use several points between r and s. We can consider non-quadratic integrands but it is now not easy to determine the form of f or to perform the minimization.

We may also employ sums rather than integrals. The derivative is now replaced by the difference. We may also consider other quadratic functionals such as those connected with linear integral equations and with non-local phenomenon.

Finally, we may consider multidimensional cases. Here, the analytic details are more complex, although the basic idea is the same.

Reference

1. R. Bellman, Introduction to the Mathematical Theory of Control Processes, Vol. I, Academic Press, Inc., New York, 1968.

Received December 8, 1978

CONVERGENCE SPACES AND PERFECT MAPS

Robert A. Herrmann[1]

Presented by B. Banaschewski, F.R.S.C.

The purpose of this paper is to summarize some major results which have recently been obtained in the theory of generalized perfect maps. Full details, other propositions and applications may be found in (2).

Let F(X) (resp. U(X)) be the set of all filters (resp. ultrafilters) on X and for each $\emptyset \neq A \subset X$, let <A> be the principal filter generated by A. The pair (X,q) is a <u>convergence space</u> where the map $q: F(X) \to P(X)$ has the properties (i) for each $x \in X$, $x \in q(\langle\{x\}\rangle)$; (ii) if $F, G \in F(X)$, $F \subset G$, then $q(F) \subset q(G)$. Throughout this paper X,Y and Z are convergence spaces and $\mathcal{U}(A) = \{x \mid (x \in U(X)) \wedge \exists y((y \in A) \wedge (x \to y))\}$.

DEFINITION 1. A map $f: X \to Y$ is <u>perfect</u> if whenever $\mathcal{U} \in U(X)$, $\mathcal{U} \to y \in Y$, then for each $\mathcal{V} \in U(X)$ such that $f(\mathcal{V}) = \mathcal{U}$, there exists some $x \in f^{-1}(y)$ such that $\mathcal{V} \to x$.

REMARK 1. In Definition 1, it is important to note that f is NOT assumed to be continuous nor surjective in contrast to (5).

For $A \subset X$, a filter base F on X is <u>A-compact</u> if for each $\mathcal{U} \in U(F) = \{x \mid (x \in U(X)) \wedge (F \subset x)\}$ there exists some $a \in A$ such that $\mathcal{U} \to a$ and let $S(\mathcal{U}(A))$ be the set of all choice sets determined by $\mathcal{U}(A)$. Using filter base theory and Definition 1

1. This research was partially supported by a grant from the U.S. Naval Academy Research Council.

AMS(MOS) subject classification (1970). Primary 54A05,54C10 the next characterizing results are obtained.

THEOREM 1. For a space X and nonempty $A \subset X$ a filter base $\mathcal{F}$ on X is A-compact iff for each $S \in S(\mathcal{U}(A))$ there exists a nonempty finite $S_f \subset S$ and some $F \in \mathcal{F}$ such that $F \subset \bigcup S_f$.

THEOREM 2. Let $f: X \to Y$. Then f is perfect iff whenever $\mathcal{U} \in U(Y)$, $f(X) \in \mathcal{U}$ and $\mathcal{U} \to y \in Y$, then $f^{-1}(\mathcal{U})$ is $f^{-1}(y)$-compact.

Using the result that if $\mathcal{F} \in F(X)$, then $U(f^{-1}(\mathcal{F})) = \bigcup\{U(f^{-1}(\mathcal{U})) \mid \mathcal{U} \in U(\mathcal{F})\}$, Theorem 2 can be extended to all nontrivial filters on f(X).

THEOREM 3. Let $f: X \to Y$. Then f is perfect iff whenever $\mathcal{F} \in F(X)$, $\mathcal{F} \cap f(X)$ and $\mathcal{F} \to y \in Y$, then $f^{-1}(\mathcal{F})$ is $f^{-1}(y)$-compact.

Recall that the adherence operator "a_q" on F(X) is defined by $a_q(\mathcal{F}) = \{x \mid (x \in X) \wedge \exists y((y \in U(X)) \wedge (\mathcal{F} \subset y) \wedge (y \to x))\}$.

THEOREM 4. A map $f: X \to Y$ is perfect iff for each $\mathcal{F} \in F(X)$ if follows that $a_p(f(\mathcal{F})) \subset f(a_q(\mathcal{F}))$.

Various concepts such as q-closed subsets of X, the length of the decomposition series for X, weak-continuity and their relation to perfectness are investigated. Let $\hat{q}$ be the pretopological modification and $\lambda(q)$ the topological modification for a convergence function q (4).

THEOREM 5. If $\hat{q} = \lambda(q)$ and $\hat{p} \neq \lambda(p)$, then there does not exist a weakly-continuous and perfect surjection from (X,q) onto (Y,p).

A subset $B \subset X$ is <u>almost-compact</u> (6) if B is X-compact. Perfect maps (resp. surjections) inversely map compact (resp. almost-compact) subsets of the codomain onto compact (resp. almost-compact) subsets of the domain. Indeed, even though they are not in general (convergence space) continuous, perfect maps are closed and have compact point inverses. Thus they have the same property as do topologically (not necessarily continuous) perfect maps as defined in (3) (7). This property does NOT, however, characterize perfect maps as is the case for topological spaces (7).

<u>Example 1.</u> Let (X,q) be pseudotopological and not pretopological. Since (X,q) and $(X,\hat{q})$ have the same closed sets and each $x \in X$ is both q and $\hat{q}$-compact, then the identity map $I:(X,q) \to (X,\hat{q})$ is closed with compact point inverses. However, there exists some $\mathcal{U} \in U(X)$ and $x \in X$ such that $\mathcal{U}$ is $\hat{q}$-convergent to x but is not q-convergent to x. Consequently, I is not perfect.

It is well-known that for a topological space if f is a continuous map from a Hausdorff space into a locally compact space and for each compact $K \subset Y$, $f^{-1}(K)$ is compact, then f is perfect.

THEOREM 6. <u>Let $\mathcal{B} \subset P(Y)$ be such that for each $\mathcal{U} \in U(Y)$ there exists some $B \in \mathcal{B}$ such that $B \in \mathcal{U}$. If $f:X \to Y$ is weakly--continuous and for each $B \in \mathcal{B}$, $f^{-1}(B)$ is almost-compact and Y is Hausdorff, then f is perfect.</u>

The last major results deal with product spaces where for two maps $f:X \to Y$, $g:X \to Z$, we define $(f,g):X \to Y \times Z$ by $(f,g)(x)=$

$= (f(x),g(x))$ for each $x \in X$. Using the known result that for each $A \subset Y \times Z$, $(f,g)^{-1}(A) \subset f^{-1}(P_1(A)) \cap g^{-1}(P_2(A))$, where P_1, P_2 are the projections, the next proposition is obtained. Moreover, numerous corollaries and theorems follow from this result.

THEOREM 6. If $f:(X,q) \to (Y,p)$ is perfect and the map $g:(X,q) \to (Z,s)$ is weakly-continuous into Hausdorff Z, then $(f,g):X \to (Y \times Z, p \times s)$ is perfect.

REFERENCES

(1) R. F. Dickman, Jr. and J. R. Porter, θ-perfect and θ-absolutely closed functions, Illinois J. Math. 21(1977),42-60.

(2) R. A. Herrmann, Perfect maps on convergence spaces,preprint.

(3) S. Iliadis and S. Fomin, The method of centred systems in the theory of topological spaces, Uspeki Mat. Nauk 21(1966), 47-76.

(4) D. Kent, Convergence functions and their related topologies, Fund. Math. 54(1964), 125-133.

(5) D. Kent and G. D. Richardson, Open and proper maps between convergence spaces, Czechoslovak Math. J. 23(1973),15-23.

(6) Vinod-Kumar, Compactifications of convergence spaces, Notices Amer. Math. Soc. 24(1977), A-262.

(7) G. T. Whyburn, Directed families of sets and closedness of functions, Proc. Nat. Acad. Sci (USA), 54(1965),688-692.

MATHEMATICS DEPARTMENT, U.S. NAVAL ACADEMY, ANNAPOLIS,MD.21402

December 22, 1978

Quadratic Spaces Over Finite Fields And Codes

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

1. Spheres. Let F be a field of characteristic not 2 and V a finite dimensional quadratic space over F. V may be singular and the inner product of two vectors A and B of V is denoted by AB, while A^2 stands for AA. If $c \in F$, the set of vectors $\{A: A \in V \text{ and } A^2 = c\}$ is called the sphere of radius c of V and is denoted by S_c or $S_c(V)$. If F is finite, S_c contains only finitely many vectors and this number of vectors is called the cardinality of S_c and is denoted by $|S_c|$. The following theorem says that these cardinalities determine the isometry class of V [4].

Theorem 1. Let F be finite and V and W two finite dimensional quadratic spaces over F which may be singular. These spaces are isometric if and only if $|S_c(V)| = |S_c(W)|$ for all $c \in F$; i.e., if and only if spheres of the same radius have the same cardinality.

Let F be finite and g an element of F which is not a square. It is immediate that the criterion of Theorem 1 is satisfied as soon as $|S_c(V)| = |S_c(W)|$ for $c = 0,1$ and g. Hence the theorem says that the isometry class of a quadratic space over a finite field is determined by three natural numbers. This agrees with the classical theory [1] where the isometry class of such spaces is determined by two natural numbers (dimension and rank) and one integer (± 1).

2. Codes. Let F be an arbitrary field which may be of characteristic 2, and V a finite dimensional vector space over F. Momentarily, V is not a quadratic space and we choose a basis $A_1, \ldots, A_n$ for V.

In coding theory, one studies the geometry of V relative to the fixed basis $A_1, \ldots, A_n$. Linear subspaces of V are now also called codes and the weight of a vector $A = c_1A_1 + \ldots + c_nA_n$ is the number of its nonzero coordinates c_i. If F is finite, one defines the weight enumerator of a code U as the integral polynomial

$$c_0 + c_1x + c_2x^2 + \ldots + c_nx^n,$$

where c_i is the numbers of vectors in U of weight i. See [3] for an exposition of coding theory.

Suppose now that F is the field consisting of 3 elements. Codes are then called ternary codes and they have been investigated in [2]. It now pays to make the vector space V into a quadratic space by declaring that the given basis $A_1, \ldots, A_n$ shall be orthonormal; i.e., $A_i^2 = 1$ for $i = 1, \ldots, n$ and $A_iA_j = 0$ if $i \neq j$. This makes V and all codes into quadratic spaces but, while V is nonsingular, codes may very well be singular. Theorem 1 makes the following theorem very easy to prove [4].

Theorem 2. If two ternary codes have the same weight enumerator, they are isometric.

3. Quadratic Spaces Over Arbitrary Fields. Theorem 1 applies only if the field F is finite, since otherwise the cardinality $|S_c|$ of the sphere S_c may be infinite. Hence we replace this cardinality by a natural number m_c, defined as follows.

Definition. Let F be a field which may be infinite, but is not of characteristic 2. Let V be a nonsingular, quadratic space over F of finite dimension n. If $c \epsilon F$, the natural number m_c is defined as the maximum number of mutually orthogonal vectors contained in the sphere S_c.

Clearly, $0 \leq m_c \leq n$ and m_0 is the usual Witt index of V. The basic question is: For what fields F does the function $c \mapsto m_c$ from F into the natural numbers completely characterize the isometry class of V?

It is easy to see that the function $c \mapsto m_c$ has this property if F is finite or real closed or algebraically closed. Probably this function, together with the discriminant of V, determines the isometry class of V also if F is a local algebraic number field or a Pythagorean field. In general this function may of course be restricted to 0, together with one element from every square class of F. A proper answer to the above basic question will undoubtedly constitute definite progress in the classification of quadratic spaces.

References.

[1] E. Artin, Geometric Algebra, Interscience Publishers, New York, N. Y., 1957.

[2] V. Pless, Symmetry codes over GF(3) and new five-designs, J. Comb. Theory, 12 (1972), 119-142.

[3] N.J.A. Sloane, Error-correcting codes and invariant theory: New applications of a 19th century technique, Amer. Math. Monthly, 84 (1977), 82-107.

[4] E. Snapper, Quadratic spaces over finite fields and codes, accepted for publication J. Comb. Theory.

Dartmouth College
Hanover, New Hampshire 03755
U.S.A.

Received January 3, 1979

Character formulas for the orthogonal groups over GF(2).II

J. S. Frame. Michigan State University

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

1. Generic characters. In this report we show more explicitly the construction given in Theorems 3.1 and 3.2 of [1] for the level 2 generic characters of each of the following infinite families of orthogonal groups over GF(2): $G_n = O_{2n+1}(2)$, $H_n = O_{2n}(2,+)$, and $K_n = O_{2n}(2,-)$. For each family of groups a generic character of level k and length L is a class function that assigns to each class C_ν a polynomial of degree $\leq 2k$ in z, such that for $z = 2^n$, $n \geq L$, the generic character of G_n (or H_n or K_n) becomes an absolutely irreducible complex (AIC) character of G_n (or H_n or K_n), whereas for $z = 2^n$, $n < L$, the generic character is the product of an AIC-character by either 1, -1, or 0.

We assign as label for each level k generic character a "degree symbol" (its value on class C_1) that is the product of a numerical factor f with 2-power numerator times a literal factor that is the product of 2k distinct factors a_{n-i}, b_{n-j}. We define

$$a_n = 2^n + 1,\ b_n = 2^n - 1,\ c_n = a_n b_n,\ 1_{n-j} = 1. \qquad (1.1)$$

Using 1's as placeholders for missing subscripts, we abbreviate by 2cal$b$/9 a level 2 degree symbol such as $2c_n a_{n-1} b_{n-3}/9$, whose value for n = 4 is $2(4^4-1)(2^3+1)(2-1)/9 = 510$. The length L of a generic character is defined as the number of symbols in its literal factor: for calb it is L = 4. (Note that for n = 3, $b_{n-3} = 2^{n-3}-1 = 0$, whereas $b_{n-3} < 0$ for n = 1 or 2.) Generic characters are called t-positive (t^+) or t-negative (t^-) according as their values on the transposition class t for $n \geq L$ are > 0 or < 0.

Explicit matrix formulas in §2 and §3 exhibit the details of Theorems 3.1 and 3.2 of [1]. Corresponding formulas have been obtained for all the generic AIC-characters of levels 3 and 4, including all their degree symbols, but lacking definitions for a few basic functions assigned to some classes whose elements have orders divisible by 4. For the classes C_λ of $G_2 \cong S_6$, the corresponding basic functions $\phi_\lambda^{(2)}$, defined in [1], are as follows.

$C_\lambda(G_2)$:	1	3_1	s	r	3_{11}	3_2	5_1;	t	3_1t	4_s^-	4_s^+			
$C_\lambda(S_6)$:	1^6	$1^3 3$	$1^2 2^2$	2^3	3^2	6	$1{\cdot}5$;	$1^4 2$	$1{\cdot}2{\cdot}3$	$1^2 4$	$2{\cdot}4$	(1.2)		
$\phi_\lambda^{(2)}$:	α^2	$\alpha\gamma$	β^2	α_2	γ^2	γ_2	ε;	$\alpha\beta$	$\gamma\beta$	δ	β_2			

2. The level 2 generic characters of G_n. In the matrix equations below, the character matrices of H_2 and K_2 are each multiplied by an adjusted basic vector B_{H2} or B_{K2} to furnish two vectors whose 9+7 components are each one of the 16 extended level 2 characters of G_2, each containing just one "derived" level 2 generic AIC-character of G_n as first constituent, and in some cases other lower level constituents. Each entry of the basic vectors B_{H2} and B_{K2} is a basic function $\phi_\lambda^{(2)}$ from (1.2) divided by the centralizer order $|H_2|/|C_\lambda(H_2)|$ or $|K_2|/|C_\lambda(K_2)|$ of an element of H_2 or K_2 in class C_λ of G_2. Of the 16 level 2 AIC-characters of G_n, $(n \geq 4)$, the nine t^+ characters are each derived from a character of H_2 and the seven t^- characters each from a character of K_2.

Class labels are shown under each column of the character matrices. The class label for an inner class (contained in subgroups H_2' or K_2') also labels (at the left) a self-associated character if the class splits in the subgroup, or a pair of associated characters otherwise, with a bar on top for the t^-

character of a pair. Degrees for G_4 are shown at the right.

H_2	Inner classes.						Outer.			B_{H2}		G_n degrees	G_4 degrees
1	1	1	1	1	1	1	1	1	1	$\alpha^2/72$		2cb1a/9+ba+1	1190+135+1
$\bar{1}$	1	1	1	1	1	1	-1	-1	-1	$\alpha\gamma/18$		2ca1b/9+ab+1	510+119+1
3_1	1	1	1	-1	1	-1	1	1	-1	$\beta^2/8$		caa/9	1275
$\bar{3}_1$	1	1	1	-1	1	-1	-1	-1	1	$\alpha_2/12$		cbb/9	595
s	4	1	0	0	-2	0	2	-1	0	$\gamma^2/18$	=	8bca/9 + ba	4200 +135
$\bar{s}$	4	1	0	0	-2	0	-2	1	0	$\gamma_2/6$		8acb/9 + ab	2856 +119
r	4	-2	0	2	1	-1	0	0	0	$\alpha\beta/12$		$\frac{8}{9}$c1c+ba+ab+1	3400+135+1
3_{11}	2	2	-2	0	2	0	0	0	0	$\gamma\beta/6$		cc/9	1785 +119
3_2	4	-2	0	-2	1	1	0	0	0	$\beta_2/4$		2cc/9	3570

C_λ: 1 3_1 s r 3_{11} 3_2; t 3_1t 4_s^+ $\qquad$ t^+ characters.

$K_2 \cong S_5$

								B_{K2}			
1	1	1	1	1	1	1	1	$\alpha^2/5!$		2ca1a/15+aa/3	918 + 51
$\bar{1}$	1	1	1	1	-1	-1	-1	$\alpha\gamma/6$		2cb1b/15+bb/3	238 + 35
3_1	5	-1	1	0	1	1	-1	$\gamma^2/8$		cba/3 + c/3	2975 + 85
$\bar{3}_1$	5	-1	1	0	-1	-1	1	$\varepsilon/5$	=	cab/3 + c/3	2295 + 85
s	4	1	0	-1	2	-1	0	$\alpha\beta/12$		8aca/15 +aa/3	2856 + 51
$\bar{s}$	4	1	0	-1	-2	1	0	$\gamma\beta/6$		8bcb/15 +bb/3	1512 + 35
5_1	6	0	-2	1	0	0	0	$\delta/4$		cc/5	3213

C_λ: 1 3_1 s 5_1 ; t 3_1t 4_s^- $\qquad$ t^- characters.

3. <u>The level 2 generic characters of H_n and K_n</u>. The product of the character matrix of $G_2 \cong S_6$ times the basic vector B_{G2} with entries $\phi_\lambda^{(2)}|C_\lambda(G_2)|/|G_2|$ is shown below as a vector having as entries the eleven t^+ extended level 2 characters of H_n $(n \geq 4)$, of which the first constituent is one of the 11 generic t^+ level 2 AIC-characters. Other constituents, if any, have lower levels. Corresponding extended characters of K_n, with degree symbols obtained from those of H_n by replacing a's by b's and b's by a's, are constructed by multiplying the character matrix of G_2 by a

basic vector $\bar{B}_{G2}$, obtained from B_{G2} by changing the signs of the outer class (last four) entries. The associate of each of the 11 t^+ level 2 generic characters of H_n and of K_n is its t^- product with the alternating character $\bar{1}$.

$G_2 \cong S_6$	Inner classes						.	Outer				B_{G2}		Characters of H_n
1	1	1	1	1	1	1	1	1	1	1	1	$\alpha^2/6!$		$4bc1la/45+2bla/3+1$
3_1	5	2	1	1	-1	1	0	-3	0	-1	-1	$\alpha\gamma/18$		$2bclb/9 + bb/3$
U	1	1	1	-1	1	-1	1	-1	-1	-1	1	$\beta^2/16$		$4bbbb/45$
V	5	-1	1	3	2	0	0	-1	-1	1	-1	$\alpha_2/48$		$4baab/9 + \frac{4}{3}1c + 1$
X	5	2	1	-1	-1	-1	0	3	0	1	-1	$\gamma^2/18$		$4bbaa/9 + 2bla/3$
Y	9	0	1	3	0	0	-1	3	0	-1	1	$\gamma_2/6$	=	$\frac{4}{5}baba+\frac{4}{3}1c+\frac{2}{3}bla+1$
3_{11}	5	-1	1	-3	2	0	0	1	1	-1	-1	$t/5$		$bca/9$
3_2	10	1	-2	-2	1	1	0	2	-1	0	0	$\alpha\beta/48$		$2bca/9$
5_1	9	0	1	-3	0	0	-1	-3	0	1	1	$\gamma\beta/6$		$bcb/5$
3_1s	10	1	-2	2	1	-1	0	-2	1	0	0	$\delta/8$		$4bbc/9 + bb/3$
s_2	16	-2	0	0	-2	0	1	0	0	0	0	$\beta_2/8$		$\frac{64}{45}1cc + \frac{4}{3}1c$
C_λ:	1	3_1	s	r	3_{11}	3_2	5_1;t	3_1t	4_s^-	4_s^+				

Character labels appear in the left column, and class labels below. Degrees of the 11 pairs of AIC level 2 characters for the groups H_4, K_4, H_5 and K_5 and corresponding class symbols are:

C_λ:	rr	3_1r	8_r^-	4_r^-	8_r^+	4_r^+	3_{11}	3_2	5_1	3_1s	4_st
H_4:	168	210	28	300	700	972	525	1050	567	700	1344
K_4:	0	714	204	476	204	476	357	714	1071	1020	1344
H_5:	2108	5270	666	6324	9300	14756	7905	15810	11067	13020	22848
K_5:	748	9350	2244	7700	5236	10692	6545	13090	15147	15708	22848

Reference

[1] J. S. Frame, Character formulas for the orthogonal groups over GF(2), Mathematical Reports, vol. 1, no.2 (1979), 99-102.

Michigan State University
East Lansing, Michigan

Received January 10, 1979

C. R. Math. Rep. Acad. Sci. Canada - Vol. 1 (1979) No. 3

There are atomic Nadel structures

M. Makkai*

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

§1. INTRODUCTION AND STATEMENT OF THE RESULT

In this note we describe in outline the construction of an example of a structure whose Scott sentence is of a certain singular character. The existence of such a so-called 'atomic Nadel structure' has been a recognized problem for at least five years; the author first heard of it from Leo Harrington in late 1973.

Scott sentences have been linked with fundamental problems concerning the number of non-isomorphic countable models of a theory (cf. e.g. [5]). G. Sacks (unpublished) and M. Nadel [6] recognized the importance of measuring the complexity of the Scott sentence in terms of admissible sets. Our problem originates directly in Nadel's work [6].

Let M be an arbitrary countable structure. For a finite tuple $\vec{a}$ of elements in M, $sh(\vec{a})$ is defined to be the least ordinal α such that for all $\vec{b}$ in M, $\vec{b} \equiv^{\alpha} \vec{a}$ (equivalence with respect to formulas of quantifier-rank $\leq \alpha$) implies $\vec{b} \sim \vec{a}$ (i.e. there is an automorphism of M mapping $\vec{b}$ to $\vec{a}$). The Scott height of M, $SH(M) = \sup\{sh(\vec{a}) : \vec{a}$ in $M\}$. For an admissible set A and $M \in A$, $SH(M) \leq ord(A)$; if equality holds, we call M a Nadel-structure (for A). $M \in A$ is A-Nadel iff it has no A-finite Scott-sentence [6]. M is A-atomic if $sh(\vec{a}) < ord(A)$ for all $\vec{a}$ in M. If $M \in A$, and the (conjunction of the) L_A - theory of M is a Scott-sentence, then M is A-atomic; hence the existence of A-atomic A-Nadel structures, for suitable A, is implied by

* The author's research was supported by a grant of NSERC of Canada.

THEOREM 1.1. For any A of the form A = HYP(x) (= the smallest admissible set containing x), with x an infinite subset of ω , there is an A-finite structure M without an A-finite Scott-sentence but such that $Th_A(M)$ is a Scott sentence for M.

We should remark that the result was expected, though maybe with a less 'elementary' construction than ours. Steel's work [7] on the Vaught conjecture concerning linear orders shows that a linear order cannot be an atomic Nadel structure. For an A-atomic Nadel-structure the function $\vec{a} \longmapsto sh(\vec{a})$ is not A-recursive; this is the stumbling block created by these structures for carrying over certain results from finitary logic to admissible fragments, noticed early on by many people.

§2. ABOUT THE PROOF.

All the work takes place within the confines of a deceptively simple structure. Let M_o be the linear ordering of order-type $(\omega^*+\omega)\cdot\omega$, or equivalently for our purposes, the disjoint sum $\coprod_{\ell\in\omega} Z_\ell$, with each Z_ℓ being an isomorphic copy of the linear ordering of all integers. The structure for 1.1 will be an expansion of M_o (hence, in particular, will have the same underlying set as M_o).

THEOREM 2.1. For any A-finite expansion M of M_o, the L_A-theory of M is a Scott sentence.

THEOREM 2.2. For A=HYP(x), x infinite $\subset\omega$, there is an expansion of M_o that is a Nadel structure for A.

Clearly, these two results imply 1.1. The main part of the work is the proof of 2.2; it uses, among others Dinchlet's theorem on primes in arithmetic progressions. We sketch a proof of 2.1.

Let $M_o^{(n)}$ $(M^{(n)})$ be the substructure of M_o (of M) with universe $\bigcup_{\ell<n} Z_\ell$. The automorphism group of $M_o^{(n)}$ is isomorphic to Z^n, the n-fold direct power of Z, the additive group of integers. For $s = \langle s_o,\ldots,s_{n-1}\rangle \in Z^n$, let $\bar{s}$ be the automorphism of $M_o^{(n)}$ defined by $\bar{s}(\langle a,\ell\rangle) = \langle a+s_\ell,\ell\rangle$ (where $a \longmapsto \langle a,\ell\rangle$ is a fixed isomorphism of $(Z,<)$ onto Z_ℓ). Let $T_n(M)$ be the set of $s\in Z^n$ such that $\bar{s}$ is an automorphism of $M^{(n)}$. Introducing the partial ordering $s \trianglelefteq t \Leftrightarrow s$ is an initial segment of t, we make $T = T(M) = \bigcup_{n<\omega} T_n(M)$ into a tree. Let $r_T(s)$ stand for the usual foundation-rank of s in T; in particular, $r_T(s)$ is an ordinal iff the subtree $\{t\in T: t \triangleright s\}$ is well founded, $r_T(s) = \infty$ otherwise.

LEMMA 2.2. (i) Let $n<\omega$ and $\vec{a}$ a finite tuple $\langle a_o,\ldots,a_{m-1}\rangle$ of elements of $M^{(n)}$ such that for all $\ell<n$ there is $i<m$ with $a_i\in Z_\ell$. Suppose that $\vec{a} \equiv^{\omega.2+\alpha} \vec{b}$ (in M). Then there is a unique $s\in T_n(M)$ such that $s(\vec{a}) = \vec{b}$ and $r_T(s) \geq \alpha$.

(ii) Suppose $s\in T_n(M)$, $\bar{s}(\vec{a}) = \vec{b}$. Then $r_T(s) \geq \omega.\alpha$ implies that $\vec{a} \equiv^{\alpha} \vec{b}$.

Let now M be an A-finite expansion of M_o; we'll show that M is A-atomic. Let $n<\omega$. Clearly $T_n = T_n(M)$ is a subgroup of the group Z^n, moreover it is easy to see that $T_n^\alpha = \{s\in T_n: r_T(s)\geq\alpha\}$ is a subgroup as well, for any α. Note that $T_n^\alpha \supset T_n^\beta$ if $\alpha<\beta$ and $T_n^\alpha \neq T_n^\beta$ if, in addition, there is s with $r_T(s) = \alpha$. Now use the elementary fact that every chain of properly decreasing subgroups of Z^n is of length $<\omega^2$. It follows that there is an ordinal $\nu=\nu_n < \omega^2$ such that the set X of ordinals $\alpha(\neq\infty)$ with the property that there is $s\in T_n$ with $r_T(s) = \alpha$ is of order-type ν. What is important for us is that ν is A-finite. Consider the sequence $\langle\alpha_\eta: \eta<\nu\rangle$

such that $X = \{\alpha_\eta : \eta<\nu\}$ and $\eta<\eta'<\nu \Rightarrow \alpha_\eta<\alpha_{\eta'}$. One can show that the function $\eta \mapsto \alpha_\eta$ $(\eta<\nu)$ is A-recursive. By Σ-replacement, there is $\alpha<\mathrm{ord}(A)$ such that $\alpha_\eta<\alpha$ for all $\eta<\nu$. It follows that for all $s\in T_n$, $r_T(s)\geq\alpha$ implies that $r_T(s) = \infty$. Now, let $\vec{a}$ be as in 2.3(i). We claim that $sh(\vec{a})\leq\omega.2+\alpha$ (in M). Indeed, if $\vec{a} \equiv^{\omega.2+\alpha} \vec{b}$, then by 2.3 (i) we have $s\in T_n$ with $\bar{s}(\vec{a}) = \vec{b}$ and $r_T(s)\geq\alpha$, hence $r_T(s) = \infty$. But this means that there is a path f through s in the tree T. Clearly, f gives rise to an automorphism $\bar{f}$ of M with $\bar{f}(\vec{a}) = \vec{b}$, hence $\vec{a} \sim \vec{b}$. This shows $sh(\vec{a})\leq\omega.2+\alpha$, and hence $sh(\vec{a}) < \mathrm{ord}(A)$; the same inequality for an arbitrary $\vec{a}$ is now an easy consequence. We have shown that M is A-atomic.

We now use the easily seen fact that the Scott sentence of M_o has no uncountable model. By the main theorem of [2], and using the atomicity of M, we readily conclude that $Th_A(M)$ must be a Scott sentence for M. This proves 2.1.

REFERENCES

[1] J. Barwise, Admissible Sets and Structures, Springer-Verlag, 1975.

[2] J. Gregory, Uncountable models and infinitary elementary extensions, J. Symbolic Logic 38 (1973), 460-470.

[3] H.J. Keisler, Model Theory for Infinitary Logic, North-Holland Publishing Co., 1971.

[4] M. Makkai, Admissible sets and infinitary logic, Chapter A.7 in Handbook of Mathematical Logic, ed. J. Barwise, North-Holland Publishing Co., 1977.

[5] M. Morley, The number of countable models, J. Symbolic Logic 35 (1970), 14-18.

[6] M. Nadel, Scott sentences and admissible sets, Annals Math. Logic 7 (1974), 267-294.

[7] J. Steel, On Vaught's conjecture, in: Lecture Notes Math., No. 689 Springer 1978, 193-208.

[8] M. Makkai, There are atomic Nadel structures, American Math. Society Notices 25 (1978), Abstract *78T-E82, p. A604.

McGill University
Montreal, Canada

Received January 15, 1979

ON THE MONEY-COUTTS CONFIGURATION OF NINE ANTI-TANGENT CYCLES

J. F. Rigby

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

Let a, b, c be three cycles in general position in the inversive plane, and let x be any cycle anti-tangent to b and c. Let y be one of the two (at most) cycles anti-tangent to c, a, x; let z be anti-tangent to a, b, y; let x' be anti-tangent to b, c, z (figure 1). The Tyrrell-Powell theorem [2] states that we can at this stage choose one of the two cycles y' anti-tangent to c, a, x', and then one of the two cycles z' anti-tangent to a, b, y', <u>in such a way that z' is anti-tangent to x also</u>.

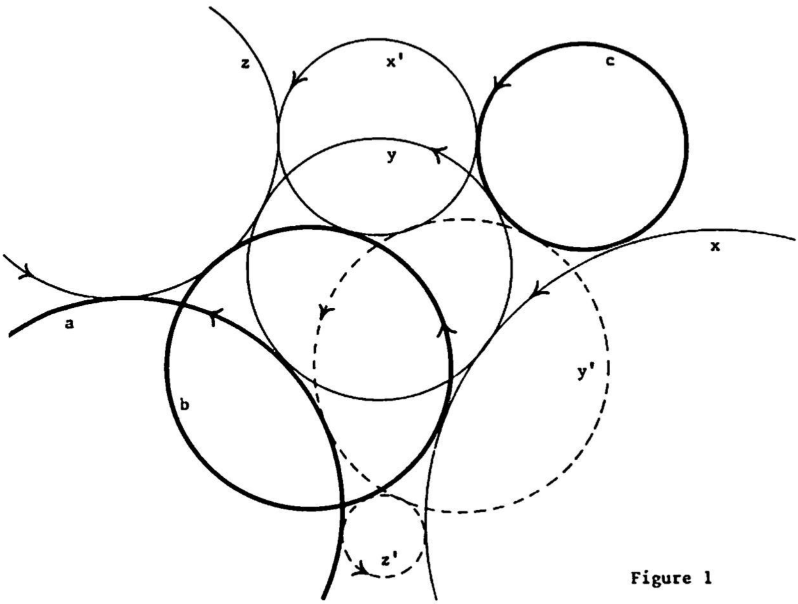

Figure 1

This gives us a configuration of nine anti-tangent cycles, whose existence was first conjectured by G. B. Money-Coutts (see [1] and [2]). Further properties of this configuration are given below.

The unique circle orthogonal to three mutually anti-tangent cycles will be called their orthocircle.

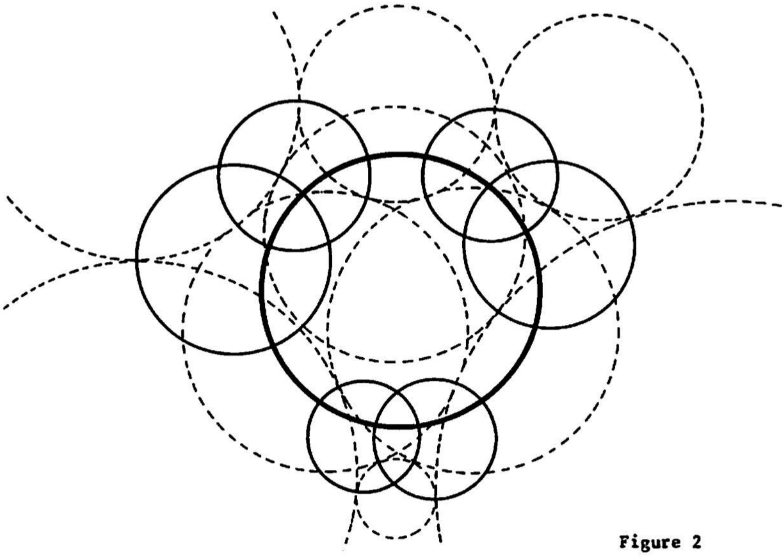

Figure 2

THEOREM 1. The six orthocircles determined by a Money-Coutts configuration have a common orthogonal circle (possibly imaginary?) (figure 2).

If four cycles are anti-tangent as in figure 3, it is easily proved by inversion that their four points of contact are concyclic, on the auxiliary circle of the four cycles.

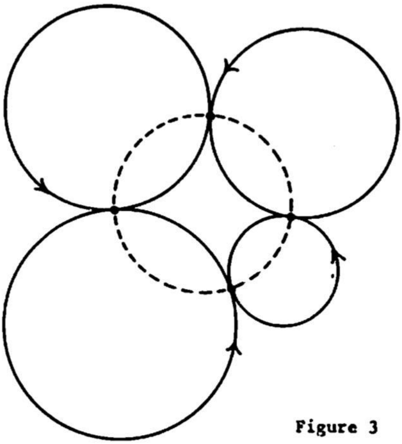

Figure 3

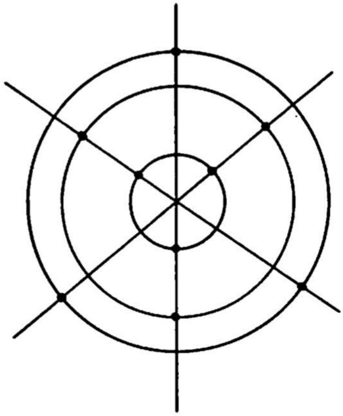

Figure 5

THEOREM 2. <u>The nine auxiliary circles determined by a Money-Coutts configuration meet by fours in nine points, as shown in figure 4 on the next page, four of these points lying on each circle</u>.

THEOREM 3. <u>If nine circles meet by fours in nine points as in figure 4, then the nine points lie by threes on three coaxal circles, and also by threes on three circles of the orthogonal coaxal system, as in figure 5</u>.

We do not require in theorem 3 that the nine circles should be derived from a Money-Coutts configuration, but in theorem 4 (a converse of theorems 2 and 3) we show that they must be.

THEOREM 4. <u>Starting with any three general circles from each of two orthogonal coaxal systems, we can choose (in 32 ways) nine of their 18 points of intersection such that these nine points lie by fours on nine circles, and these circles are the auxiliary circles of a unique Money-Coutts configuration</u>.

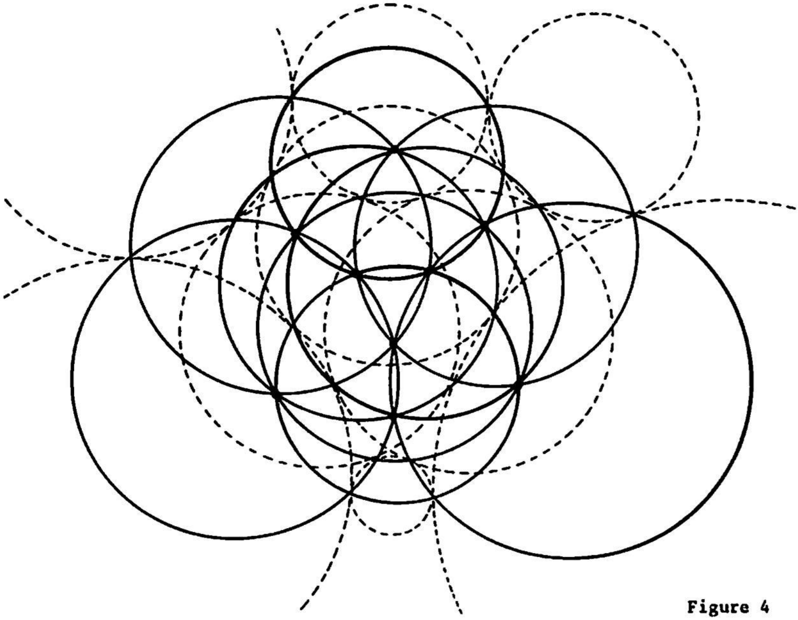

Figure 4

REFERENCES

1. C. J. A. Evelyn, G. B. Money-Coutts and J. A. Tyrrell, The seven circles theorem and other new theorems (Stacey International, London, 1974).

2. J. A. Tyrrell and M. T. Powell, A theorem in circle geometry, Bull. London Math. Soc. 3 (1971), 70-74.

University College, Cardiff CF1 1XL, Wales

Received January 24, 1979

DERIVATIONS AND FUNCTIONAL EQUATIONS BASIC TO CHARACTERIZATIONS OF INFORMATION MEASURES

J. Aczél, F.R.S.C.

A fundamental characterization of the entropies of degree (or type) β

$$A\left(\sum_{k=1}^{n} p_k^{\beta}-1\right) \quad (\beta\neq 1) \qquad -A\sum_{k=1}^{n} p_k \log p_k \quad (\beta=1)$$

(Daróczy 1970, Aczél-Daróczy 1975) is based on solution of the functional equation

$$f(x) + (1-x)^{\beta} f\left(\frac{y}{1-x}\right) = f(y) + (1-y)^{\beta} f\left(\frac{x}{1-y}\right) \quad . \tag{1}$$

The equation

$$f_1(x) + (1-x)^{\beta} f_2\left(\frac{y}{1-x}\right) = f_3(y) + (1-y)^{\beta} f_4\left(\frac{x}{1-y}\right) \tag{2}$$

is a natural generalization of (1). It also has important applications to characterizations of divergences and inaccuracies of degree β (Rathie-Kannappan 1972, 1973) in the probabilistic information theory and of inset entropies of degree β (Aczél-Kannappan 1978) in the so called mixed theory of information. In both cases we have equations, similar to (1), for functions of more than one variable and, keeping the additional variable(s) constant, one arrives, since the constants turn out to be different in each member, to equations of the form (2). - Of course, it would be nice to reduce (2) to the equation (1). But immediately (2) can be reduced to

$$f(1-x) + (1-x)^{\beta} f\left(\frac{y}{1-x}\right) = f(y) + (1-y)^{\beta} f\left(1-\frac{x}{1-y}\right) \quad , \tag{3}$$

see Kannappan-Rathie 1975, Kannappan 1978. The first of these papers shows that (3) has the same solutions as (1) <u>if</u> f <u>is measurable</u>, while the second shows that (3) implies, <u>if</u> $\beta \neq 2$, $f(1-x) = f(x)$ (symmetry around $\frac{1}{2}$) and thus (1). Since there is no difference in (1) or (3) or in the general solutions (without any measurability conditions), symmetric around $\frac{1}{2}$

(4) $$f(x) = A[(1-x)^{\beta}+x^{\beta}-1] \qquad (\beta\neq 0,1)$$

of (1) [which are also the general measurable solutions of (3)], between the cases $\beta = 2$ and $\beta \neq 2$, it is natural to conjecture that the exclusion of the case $\beta = 2$ is caused by the method of proof rather than by intrinsic reasons and indeed, this conjecture was pronounced by Kannappan 1978, Aczél-Kannappan 1978. - However, I will disprove this conjecture here by giving a solution of (3), for $\beta = 2$, which does not satisfy (1). [As to the domain of validity of the equations (1), (2), and (3), it may be

(5) $$D = \{(x,y)\,|\,x>0,y>0,x+y<1\} \quad \text{or} \quad D = \{(x,y)\,|\,0\le x<1,0\le y<1,x+y\le 1\} \;;$$

in the latter case $0^{\beta} := 0$, by definition, in (4).]

It is known (see, e.g., Zariski-Samuel 1958) that there exist functions $d : R \to R$, not identically zero on $]0,1[$ and satisfying

(6) $$d(x+y) = d(x) + d(y) \quad \text{and} \quad d(xy) = xd(y) + yd(x) \quad \text{for all} \quad x,y\in R \;.$$

They are called derivations. Easy consequences of (6) are

$$d(1-t) = -d(t) \quad \text{and} \quad d(\tfrac{t}{s}) = \frac{sd(t)-td(s)}{s^2} \qquad (s\neq 0, t\in R) \;.$$

So

$$\begin{aligned} d(1-x) + (1-x)^2 d(\tfrac{y}{1-x}) &= -d(x) + (1-x)d(y) + yd(x) = (1-x)d(y) - (1-y)d(x) \\ &= d(y) - (1-y)d(x) - xd(y) = d(y) + (1-y)^2 d(1-\tfrac{x}{1-y}), \end{aligned}$$

that is, d satisfies (3), but not (1) for $\beta = 2$:

$$\begin{aligned} d(x) + (1-x)^2 d(\tfrac{y}{1-x}) &= d(x) + (1-x)d(y) + yd(x) \neq d(y) + (1-y)d(x) + xd(y) \\ &= d(y) + (1-y)^2 d(\tfrac{x}{1-y}) \end{aligned}$$

because

$$xd(y) \neq yd(x) \quad \text{since} \quad d(x) \not\equiv ax$$

($d(x) = ax$ does not satisfy the second equation (6) except if $a = 0$ in which case d is identically zero). Of course, also $x \mapsto f(x) = A[(1-x)^2 + x^2 - 1] + d(x)$ is a solution of (3) $\beta=2$ [but not of (1) if $d \neq 0$]. - These counter-examples are amazingly simple. The only reason I can imagine that none of the several mathematicians, who tried to prove the above conjecture, have found them, is that they thought that the conjecture is true. [As mentioned above, (4) is the only <u>measurable</u> solution of (3), also for $\beta = 2$ and indeed, all measurable derivations are identically zero.]

The situation was somewhat similar with another conjecture about (1). While the solution (4) of (1) has been found in the case $\beta \neq 1$ without any measurability or other regularity supposition, it was known (see Aczél-Daróczy 1975) that the function given by

(7) $$f(x) = -A[(1-x)\log(1-x) + x \log x] \quad (0 \log 0 := 0)$$

is only then the general solution of (1) if (symmetry around $\frac{1}{2}$ and) some regularity condition, such as measurability (Lee 1964) is supposed (else there are counter-examples). It was conjectured (Aczél-Daróczy 1975), that nonnegativity of f could serve as such a regularity condition instead of measurability. This too has been recently disproved (Daróczy-Maksa 1978) and the counter-example again is simple and involves derivations (and may also not have been found previously for the reason that most of those working on the subject had thought that the conjecture is true): If d is an arbitrary derivation, then

$$f(x) = -A[(1-x)\log(1-x) + x \log x] + \frac{d(x)^2}{x(1-x)}, \quad (A \geq 0)$$

is nonnegative, symmetric around $\frac{1}{2}$, and satisfies (1). (Of course, if f is supposed to be measurable, then (7) is the only symmetric solution). While it is not likely that the pathological solutions, involving derivations, would have practical applications, it is interesting to note that the exceptional cases $\beta = 1$ and $\beta = 2$ are the most useful for applications.

This research has been supported a.o. by a leave fellowship of the Social Sciences and Humanities Research Council of Canada.

REFERENCES

J. Aczél-Z. Daróczy	1975	On Measures of Information and their Characterizations. Academic Press, New York-San Francisco-London.
J. Aczél-Pl. Kannappan	1978	A mixed theory of information. III. Inset entropies of degree β. Information and Control 39.
Z. Daróczy	1970	Generalized information functions. Information and Control 16, 36-51.
Z. Daróczy-Gy. Maksa	1978	Talk presented at the Sixteenth International Symposium on Functional Equations, Sep. 3-10, 1978, Leibnitz, Austria.
Pl. Kannappan	1978	Note on generalized information function. Tôhoku Math. J. 30, 251-255.
Pl. Kannappan-P.N. Rathie	1975	On generalized information function. Tôhoku Math. J. 27, 207-212.
P.M. Lee	1964	On the axioms of information theory. Ann. Math. Statistics 35, 415-418.
P.N. Rathie-Pl. Kannappan	1972	A directed-divergence function of type β. Information and Control 20, 38-45.
P.N. Rathie-Pl. Kannappan	1973	An inaccuracy function of type β. Ann. Inst. Statist. Math. 25, 205-214.
O. Zariski-P. Samuel	1958	Commutative Algebra. I, Chapter II. Van Nostrand, Princeton, N.J.-Toronto-London-New York.

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

Received February 1, 1979

AN ELEMENTARY THEORY OF GROTHENDIECK'S RESIDUE SYMBOL

by Glenn W. Hopkins and Joseph Lipman[(1)]

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

INTRODUCTION. Grothendieck has defined an intriguing homomorphism, the "residue symbol", and listed some of its basic properties (cf. [5, pp. 195-199], and also [1]). This symbol has found application in several areas ([2], [3], [7], [10]). Unfortunately, Grothendieck's treatment is embedded in a formidable global duality theory, which makes detailed proofs inaccessible to many who may find the symbol itself quite useful.

We outline here an approach to residues which requires only basic commutative and homological algebra. The feasibility of such an approach was suggested by Cartier fifteen or twenty years ago. It is both more elementary and more general than the one in [5]. It should be noted however that the formalism of residues does take on more meaning in the context of duality, from which it arose.

1. BASIC DEFINITIONS. All rings are commutative. We consider a ring A, and a homomorphism of A-algebras $\pi: R \to B$ where, as an A-module, B is finitely generated and projective. Let $S = R \otimes_A B$, and let $\gamma: S \to B$ be the unique A-algebra homomorphism such that $\gamma(r \otimes b) = \pi(r)b$. For any integer $q \geq 0$ we have natural maps

$$\mathrm{Ext}_R^q(B,B) = \mathrm{Ext}_S^q(B,\mathrm{Hom}_A(B,B)) \xrightarrow{\tau} \mathrm{Ext}_S^q(B,\mathrm{Hom}_A(B,A)) \to \mathrm{Hom}_A(\mathrm{Tor}_q^S(B,B),A).$$

(τ exists because of a natural B-isomorphism

$$\mathrm{Hom}_A(B,B) \otimes_S B \xrightarrow{\sim} \mathrm{Hom}_A(B,A)$$

induced by the A-linear trace map $\mathrm{tr}_{B/A}: \mathrm{Hom}_A(B,B) \to A$.)

Let $\Omega = \Omega_{R/A}$ be the R-module of Kähler A-differentials, and let J be the kernel of γ. There exist natural isomorphisms of exterior powers

(1) Supported by National Science Foundation.

$$\Omega^q \otimes_R B = (\Lambda^q\Omega) \otimes_R B \xrightarrow{\sim} \Lambda^q(J/J^2) \qquad (q \geq 0)$$

and a natural homomorphism of graded B-algebras

$$\bigoplus_{q\geq 0} \Lambda^q(J/J^2) \longrightarrow \bigoplus_{q \geq 0} \mathrm{Tor}_q^S(B,B).$$

Combining all these maps, we obtain natural A-linear homomorphisms

$$\mathrm{Res}^q:\Omega^q \otimes_R \mathrm{Ext}_R^q(B,B) \to \mathrm{Tor}_q^S(B,B) \otimes_B \mathrm{Ext}_R^q(B,B) \to A \qquad (q \geq 0).$$

2. THE RESIDUE SYMBOL. Let $(f_1,\ldots,f_q)$ be a regular sequence in R. Suppose that B (as above) is R/I, where $I = (f_1,\ldots,f_q)R$. Then there are natural isomorphisms

$$\mathrm{Ext}_R^q(B,B) \xrightarrow{\sim} \mathrm{Hom}_B(\Lambda^q(I/I^2),B) \xrightarrow{\sim} B$$

so that Res^q gives an A-homomorphism

$$\mathrm{Res}_{R/A}:\mathrm{Hom}_B(\Lambda^q(I/I^2),\Omega^q/I\Omega^q) \to A.$$

For any $\omega \in \Omega^q$, let

$$\begin{bmatrix} \omega \\ f_1,\ldots,f_q \end{bmatrix} \in \mathrm{Hom}_B(\Lambda^q(I/I^2),\Omega^q/I\Omega^q)$$

be the map which takes $\bar{f}_1 \wedge\ldots\wedge \bar{f}_q$ ($\bar{f}_i = f_i \bmod I^2$) to $\omega \bmod I\Omega^q$. We have then defined the symbol

$$\mathrm{Res}_{R/A}\begin{bmatrix} \omega \\ f_1,\ldots,f_q \end{bmatrix} \in A.$$

The formulation and proof of properties of this symbol corresponding to those listed in [5] is now a (quite involved) exercise in algebra.

3. EXAMPLE. Assume further that R is a polynomial or power series ring in q variables over A, so that $\Omega^q/I\Omega^q \cong B$. Then the B-linear map

$$\mathrm{Hom}_B(\Lambda^q(I/I^2),\Omega^q/I\Omega^q) \to \mathrm{Hom}_A(B,A)$$

corresponding to $\mathrm{Res}_{R/A}$ is an isomorphism, whose inverse is the map θ which is the main object of study in [8]. Theorem (4.2) of loc. cit. can be restated as follows:

$$\operatorname{Res}_{R/A}\begin{bmatrix} df_1 \wedge df_2 \wedge \ldots \wedge df_q \\ f_1, f_2, \ldots, f_q \end{bmatrix} = \operatorname{tr}_{B/A}(1).$$

This is part of (R6) on p. 198 of [5]. Scheja and Storch derive some interesting corollaries, for example concerning equality of Kähler and Dedekind differents.

4. LOCAL RESIDUES. In algebraic or analytic geometry we consider the case when A is a field, R is a q-dimensional local ring containing A and whose residue field is finite over A, and $B = R/I$, where I is an ideal whose radical is the maximal ideal M of R. There is then a commutative diagram

$$\begin{array}{ccc} \Omega^q \otimes_R \operatorname{Ext}^q_R(B,R) & \longrightarrow & \Omega^q \otimes_R H^q_M(R) = H^q_M(\Omega^q) \\ \big\downarrow & & \big\downarrow \rho \\ \Omega^q \otimes_R \operatorname{Ext}^q_R(B,B) & \xrightarrow{\operatorname{Res}^q} & A \end{array}$$

(cohomology supported in M)

where ρ, the <u>local residue</u> (or <u>trace</u>) <u>map</u>, does not depend on I. This ρ is a basic component of duality theory. For example, if V is a d-dimensional irreducible variety over a perfect field A, there is a <u>dualizing sheaf</u> on V [6, Chapter III, §7] whose stalk at a closed point $v \in V$, with local ring R, is the following R-module of meromorphic q-forms:

$$\{\omega/r \mid \omega \in \Omega^q,\ 0 \neq r \in R, \text{ and } \rho(\omega \otimes \lambda) = 0 \text{ for all } \lambda \in H^q_M(R) \text{ with } r\lambda = 0\}.$$

This dualizing sheaf is constructed in [4, Théorème 4.1] by means of Grothendieck's machinery. With our definition of residues, a more digestible treatment, in the spirit of [7], is anticipated.

The curve case $q = 1$ is presented in [9, Chapter IV, §3]. The connection with the foregoing may be clarified by an example:

5. EXAMPLE. Let A be a field, and $R = A[[X]]$ the formal power series ring in one variable. Let $K = R[1/X]$ be the fraction field of R.

Here

$$H^1_M(\Omega) = \Omega \otimes_R K$$

and for any $h = a_0 + a_1X + a_2X^2 + \ldots$ in R, and $s > 0$, we find that

$$\rho(hdX/X^s) = \mathrm{Res}_{R/A}\begin{bmatrix} hdX \\ X^s \end{bmatrix} = a_{s-1} \text{ ,}$$

the coefficient of X^{-1} in h/X^s. This is of course the classical definition of the residue of hdX/X^s; as developed here, it is clearly independent of the choice of the "parameter" X (cf. [9, p. 25]).

REFERENCES

[1] A. Beauville, Une notion de résidu en géométrie analytique, Lecture Notes in Math. no. 205, Springer-Verlag, 1971, pp. 183-203.

[2] J. Carrell and D. Lieberman, Vector fields and Chern numbers, Math. Ann. 225 (1977), 263-273.

[3] J. Damon, The Gysin homomorphism for flag bundles: applications, Amer. J. Math. 96 (1974), 248-260.

[4] F. Elzein, Complexe dualisant et applications, Thèse de Doctorat d'État, Paris, 1977.

[5] R. Hartshorne, Residues and duality, Lecture Notes in Math. no. 20, Springer-Verlag, 1966.

[6] R. Hartshorne, Algebraic Geometry, Springer-Verlag, 1977.

[7] E. Kunz, Residuen von Differentialformen auf Cohen-Macaulay Varietäten, Math. Z. 152 (1977), 165-189.

[8] G. Scheja and U. Storch, Uber Spurfunktionen bei vollständigen Durchschnitten, J. Reine Angew. Math. 278/279 (1975), 174-190.

[9] J. -P. Serre, Groupes algébriques et corps de classes, Hermann, Paris, 1959.

[10] Y. L. Tong, Integral representation formulae and Grothendieck residue symbol, Amer. J. Math. 95 (1973), 904-917.

University of Mississippi
University, MS 38677, U.S.A.

Purdue University
W. Lafayette, IN 47907 U.S.A.

Received February 15, 1979

On n-dimensional Kloosterman sums

by

Robert A. Smith

Presented by J.H.H. Chalk, F.R.S.C.

For each integer $n \geq 1$, define a $\mathbb{Z}$-bilinear form on $\mathbb{Z}^n \times \mathbb{Z}^n$ into $\mathbb{Z}$ by $\underline{a} \cdot \underline{x} = a_1x_1 + \cdots + a_nx_n$, where $\underline{a} = (a_1, \ldots, a_n)$, $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. This induces a $\mathbb{Z}$-bilinear form on $\mathbb{Z}^n \times \mathbb{Z}^{n-1}$ into $\mathbb{Z}$ $(n \geq 2)$ if we embed $\mathbb{Z}^{n-1}$ into $\mathbb{Z}^n$ by $(x_1, \ldots, x_{n-1}) \mapsto (x_1, \ldots, x_{n-1}, 0)$. Also, define $N(\underline{x}) = x_1 \ldots x_n$. Let $q \geq 1$ be an integer. If each component of $\underline{a}$ is relatively prime to q, we say that $\underline{a}$ is <u>relatively prime</u> to q. If $x \in \mathbb{Z}$ is relatively prime to q, there exists an integer $\overline{x}$ satisfying $x\overline{x} \equiv 1 \bmod q$. Finally, we write $e_q(t) = e^{2\pi it/q}$.

The n-dimensional Kloosterman sum is defined as follows. For each $\underline{a} \in \mathbb{Z}^{n+1}$, define

$$K_n(\underline{a}\,;q) = \sum_{\underline{x} \bmod q}^{*} e_q\left(\underline{a} \cdot \underline{x} + a_{n+1}\overline{N(\underline{x})}\right),$$

where the summation condition means that each component of $\underline{x} \in \mathbb{Z}^n$ runs over a reduced set of residues mod q.

Recently, Deligne [1] established the last of the Weil Conjectures, the Riemann Hypothesis for algebraic varieties over finite fields. In [2], Deligne applies his work on the Weil Conjectures to deduce (among other things)

$$|K_n(\underline{a}\,;p)| \leq (n+1)p^{n/2}, \tag{1}$$

where p is any prime and $\underline{a}$ is relatively prime to p. The special case of (1) when $n = 1$ was established by Weil [5]. It is well-known that this special case implies

$$|K_1(a,b;q)| \le q^{\frac12}(a,b,q)^{\frac12}\, d(q) , \tag{2}$$

where (a,b,q) denotes the g.c.d. of a, b and q, and $d(q)$ denotes the number of divisors of q.

In [4], we establish the following two theorems, Theorem 2 being the n-dimensional analogue of (2). Indeed, since $K_n(\underline{a};q)$ is multiplicative in q, it suffices to assume $q = p^\alpha$, a prime power. Theorem 2 is therefore essentially a corollary of Theorem 1 and (1).

<u>THEOREM 1</u>. Suppose $\underline{a} \in \mathbf{Z}^{n+1}$ is relatively prime to p $(p > 2)$, and suppose $X^{n+1} \equiv N(\underline{a}) \bmod p$ is solvable. Assume p does not divide $n+1$. For each $\alpha \ge 2$, there exists an integer t satisfying $t^{n+1} \equiv N(\underline{a}) \bmod p^\alpha$. If $\alpha = 2\beta + \gamma$ where $\beta \ge 1$ and $\gamma = 0$ or 1, let $U = U_n(p^\beta) = \{1 \le u \le p^\beta : u^{n+1} \equiv 1 \bmod p^\beta\}$. Then

$$K_n(\underline{a};p^\alpha) = (p^\alpha)^{n/2}\, \varepsilon_n(p^\alpha, t) \sum_{u \in U} \left(\frac{u}{p}\right)^\gamma e_{p^\alpha}\big(t f_\gamma(u)\big) ,$$

where $f_0(u) = nu + \bar{u}^n$ and $f_1(u) = f_0(u) - \overline{2(n+1)}\, n\, u^{n+2}\big(1 - \bar{u}^{n+1}\big)^2$. In addition, $\left(\frac{u}{p}\right)$ denotes the Legendre symbol and $\varepsilon_n(p^\alpha, t)$ denotes a certain fourth root of unity depending on p^α, n and t.

Similar but more complicated results hold when p divides $n+1$ $(p > 2)$ and for $p = 2$.

<u>THEOREM 2</u>. For all $\underline{a} \in \mathbf{Z}^{n+1}$,

$$|K_n(\underline{a};q)| \le q^{n/2} (\underline{a};q)_n^{n/2}\, d_{n+1}(q) ,$$

where $(\underline{a};q)_n$ is a certain generalization of the g.c.d. of $\underline{a}$ and q (depending on n), and $d_{n+1}(q)$ denotes the number of representations of q

as a product of $n+1$ factors.

The following is an application of Deligne's estimate (1). For each Dirichlet character $\chi \bmod p$, define

$$W(\chi) = \sum_{x \bmod p} \chi(x) e_p(x) ,$$

the ordinary Gaussian sum. Since $W(\chi) \neq 0$ for all χ, define

$$\theta(\chi) = \frac{1}{2\pi} \arg W(\chi) ,$$

where "arg" is chosen to satisfy $0 \le \arg W(\chi) < 2\pi$ for all χ.

THEOREM 3. For any $0 \le \alpha < \beta \le 1$, let $N_p(\alpha, \beta)$ denote the number of characters $\chi \bmod p$ for which $\alpha \le \theta(\chi) \le \beta$. Then

$$N_p(\alpha, \beta) = (\beta-\alpha)p + O(p^{3/4}) , \qquad (p \to \infty)$$

where the implied constant in the O-term is independent of p. In particular, the arguments of the Gaussian sums $W(\chi)$ are uniformly distributed mod 1 as $p \to \infty$.

The proof depends on a theorem of Erdös and Turán on uniform distribution [3, p. 374]. Thus,

$$|N_p(\alpha, \beta) - (\beta-\alpha)p| \ll 1 + \frac{p}{m+1} + \sum_{1 \le n \le m} \frac{1}{n} |T_n(p)| ,$$

where $m \ge 1$ is arbitrary and

$$T_n(p) = \sum_{\chi \bmod p} e^{2\pi i n \theta(\chi)} .$$

Since $(p-1)K_{n-1}(\underline{e}; p) = p^{n/2} T_n(p) + (-1)^n (p^{n/2} - 1)$ with $\underline{e} = (1, 1, \dots, 1)$ (cf. [4]), Theorem 3 follows from (1) with $m = [p^{1/4}]$.

REFERENCES

1. P. Deligne, La conjecture de Weil I, Publ. Math. IHES 43 (1974), 273-307.

2. P. Deligne, Applications de la formule des traces aux sommes trigonométriques, (S.G.A. 4½) Springer Lecture Notes in Math. 569 (1977), 168-232.

3. P. Erdös and P. Turán, On a problem in the theory of uniform distribution I, II, Indag. Math. 10 (1948), 370-378 and 406-413.

4. R.A. Smith, On n-dimensional Kloosterman sums, J. Number Theory (to appear).

5. A. Weil, On some exponential sums, Proc. Nat. Acad. Sci. (U.S.A.) 34 (1948), 204-207.

University of Toronto
Toronto, Ontario
Canada M5S 1A1

Received March 2, 1979