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

Vol. VIII, No. 5 October 1986 octobre

CONTENTS

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

THE STRUCTURE OF FREE PRODUCTS OF PRO-p-GROUPS

Wolfgang Herfort and Luis Ribes

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

1. THE RESULT

Let p be a fixed prime number, and let $A_1, A_2, \ldots, A_n$ be a finite number of pro-p-groups. Let $G = \coprod_{i=1}^{n} A_i$ be their free pro-p-product, i.e., their coproduct in the category of pro-p-groups. We are concerned here with a possible description of the closed subgroups H of G, along the lines of the Kurosh theorem for free products of abstract groups (cf. [6], for example). Our main result is the following:

Theorem Let H be a (topologically) finitely generated closed subgroup of G. Then $H = (\coprod_{i,j} A_i^{\alpha_{ij}} \cap H) \amalg F$, where F is a free pro-p-group, and for every i, α_{ij} runs through a complete set of double coset representatives of A_i and H in G.

The theorem is in fact more general than stated here: the number of factors A_i can be infinite, and their free product should then be understood in the appropriate manner (cf. [1], [3]).

If each of the free factors A_i is $\mathbb{Z}_p$ (the additive group of the ring of p-adic integers), then G is a free pro-p-group. In this case, our theorem reduces to a well-known result of Tate (cf. [2], or [7], Cor. 3, p. 1-37).

Our method of proof uses very heavily the fact that H is finitely generated, and we do not know whether the result is also valid for infinitely generated subgroups of G. An explicit mention of the problem we solve with our theorem can be found in Lubotzky [5].

2. THE PROOF

Our proof makes frequent use of two results:

Fact (I): The open subgroups of G, do admit a decomposition as a free product as in the Theorem (cf. [1]).

Fact (II): Every finite subgroup of G is contained in some conjugate of one of the free factors A_i of G (cf. [4], Th. 2).

The proof of the theorem is done in two steps. First we assume that each of the free factors A_i of G is a finite p-group. The second step is a delicate reduction to the finite free factors case. For the first step the basic result is the following:

Proposition Let H be a closed (topologically) finitely generated subgroup of the free pro-p-product $G = \coprod_{i=1}^{n} A_i$, where each A_i is a finite p-group. Let $\mathcal{M}$ be a maximal set of maximal finite subgroups of H such that if M_1, M_2 are in $\mathcal{M}$, then $M_1^h \cap M_2 = \{1\}$, for each h in H (M_1^h is the conjugate of M_1 by h). Then

i) $\mathcal{M}$ is a finite set, say $\mathcal{M} = \{M_1, \ldots, M_t\}$.

ii) The subgroup of H generated by the M_i's is the free pro-p-product $M = \coprod_{i-1}^{t} M_i$.

iii) There is a free pro-p-subgroup F of H such that $H = (\coprod_{i=1}^{t} M_i) \amalg F$.

Note that this Proposition allows a description of the free factors M_i, completely internal to H; in fact, even though it is not apparent from the statement, the same is true for the group F. The description does not need a reference to G, although of course the fact that G is a free product is essential for the proof.

<u>Sketch of the proof of the Proposition</u>. For different subgroups $M_1, \ldots, M_r \in \mathcal{M}$, one first proves the existence of an open normal subgroup U of G such that each M_i $(i = 1, \ldots, r)$ is a maximal finite subgroup of HU, and $M_i^a \cap M_j = \{1\}$, for all $a \in HU$, and all $i \neq j$. To find this U one has to appeal to both Facts (I) and (II). This implies that $R = \langle M_1, \ldots, M_r \rangle$ is in fact the free product $R = \coprod_{i=1}^{r} M_i$, and one also has that R is a free factor of HU. The finite generation of H implies then that $\mathcal{M}$ must be finite. To prove part (iii) one shows first that the open subgroup U of G can be chosen in such a way that H is a free factor of HU. Since HU is an open subgroup of G, Fact (I) can be used to decompose it as a free product; then one transforms this free decomposition so that it contains as explicit free factors each of the M_i $(i = 1, \ldots, t)$. To do this one uses the Hopfian property of the finitely generated group G: every endoepimorphism of G is an isomorphism. Then we have HU expressed as a free pro-p-product of M, some other finite groups and a certain free pro-p-group L. To finish the proof of the Proposition we use again the Hopfian property of G to transform L in such a way that H appears explicitly as being generated by M and a free factor of L, and hence H is their free pro-p-product.

It is worth stating separately the following consequence of the proof of the Proposition.

<u>Corollary</u> <u>If H and G are as in the Proposition above, then H is a free factor of an open subgroup of G.</u>

One then deduces the Theorem from the Proposition in the special case when each A_i is a finite p-group, using Fact (II) and the Hopfian property of the group G .

To complete the proof of the Theorem in the general case, when the factors A_i can be arbitrary pro-p-groups, we need the following reduction results:

Lemma 1 Let G be as in the Theorem. Then

$$G = \varprojlim_{U} \left(\coprod_{i=1}^{n} A_i/A_i \cap U \right)$$

where U runs through the open normal subgroups of G .

Lemma 2 Let I be a partially ordered set, $\{ G_i \mid \eta_{ij} , i,j \in I \}$ a projective system of pro-p-groups, and $G = \varprojlim_i G_i$ their projective limit. Assume that for each i in I , there is a finite indexing set N_i such that $G_i = \coprod_{n \in N_i} A_{in}$, where each A_{in} is a finite p-group. Moreover, assume $\{ N_i \mid \eta_{ij} , i, j \in I \}$ is a projective system of sets so that $\eta_{ij} (A_{in}) = A_{jm}$, where $\eta_{ij}(n) = m$. For each $\nu = (n(i)) \in N = \varprojlim_i N_i$, set $A_\nu = \varprojlim_i A_{in(i)}$. Let H be a closed (topologically) finitely generated subgroup of G . Then there is a finite subset M of N such that $H = (\coprod_{\mu \in M, k} A_\mu^{\alpha(\mu,k)} \cap H) \amalg F$, where for each μ , $\alpha(\mu,k)$ runs through a complete set of double coset representatives of A_μ and H in G , and where F is a free pro-p-group. Moreover if $\nu \in N \ M$, then $A_\nu^\alpha \cap H = \{1\}$, for all $\alpha \in G$.

The proof of Lemma 1 is straightforward. The proof of Lemma 2 uses the following ingredients: 1) The already known version of the Theorem in the case when the free factors are all finite; 2) The Hopfian property of finitely generated pro-p-groups; and

3) The pro-p version of Grushko's theorem: if $A = B \amalg C$ is a free pro-p-product, then the minimum number of topological generators for A is the sum of the minimum numbers of topological generators for B and C (cf. [5]).

The Theorem in its most general form now follows easily from Lemmas 1 and 2. The details will appear elsewhere.

REFERENCES

1. E. Binz, J. Neukirch and G.H. Wenzel, A subgroup theorem for free products of profinite groups, J. Algebra 19 (1971) 104-109.

2. A. Douady, Cohomologie des groupes compacts totalement discontinus, Séminaire Bourbaki, exposé 189, 1959-60.

3. D. Gildenhuys and L. Ribes, A Kurosh subgroup theorem for free pro-C-products of pro-C-groups, Trans. Amer. Math. Soc. 186 (1973) 309-329.

4. W. Herfort and L. Ribes, Torsion elements and centralizers in free products of profinite groups, J. reine u. angew. Math. 358 (1985) 155-161.

5. A. Lubotzky, Combinatorial group theory for pro-p-groups, J. Pure Appl. Math. 25 (1982) 311-325.

6. W. Magnus, A. Karras and D. Solitar, Combinatorial group theory, Interscience, New York, 1966.

7. J-P. Serre, Cohomologie Galoisienne, Lect. Notes in Math., No. 5, Berlin-Heidelberg-New York, 1965.

Institut für Numerische und Angewandte Mathematik
Technische Universität
A-1040 Vienna, Austria

and

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6, Canada

Received 26 May, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 5, October 1986 octobre

LOI DE RÉCIPROCITÉ, CRITÈRE DE PRIMALITÉ DANS $\mathbb{F}_q[t]$

Yves HELLEGOUARCH

Presenté par P. Ribenboim, M.S.R.C.

Abstract : This paper shows that elementary number théory methods extend to $\mathbb{F}_q[t]$ to give a simple reciprocity law for h-powers and primality criteria.. It is not always easy and I owe to John Boxall the trick in the demonstration of the recitrocity law.

1) Préliminaires

On considère l'anneau $\mathbb{F}_q[t]$ et on désigne par ℓ sa caractéristique, de sorte que : $q = \ell^e$, e entier ≥ 1.

Pour tout polynôme non nul $P \in \mathbb{F}_q[t]$ on pose : $|P| = q^{\text{degré}(P)}$

Si l'on ajoute $|0| = 0$, on voit que $|\ |$ est une valeur absolue sur $\mathbb{F}_q[t]$.

Dans toute la suite, h désignera un diviseur fixe de $q-1$.

Les lemmes qui suivent sont immédiats.

Lemme 1.- Soit $\mathcal{M}$ le monoïde multiplicatif des polynômes unitaires de $\mathbb{F}_q[t]$. Alors l'application :

$$\theta_h : P \longmapsto \frac{|P|-1}{h} + h\mathbb{Z}$$

est un morphisme de $\mathcal{M}$ dans $(\mathbb{Z}/_{h\mathbb{Z}},+)$. Si de plus q est impair, l'application :

$$\varepsilon_h : P \longmapsto \frac{|P|-1}{h} + 2\mathbb{Z}$$

est un morphisme de $\mathcal{M}$ dans $(\mathbb{Z}/_{2\mathbb{Z}})$.

Soit un entier $n > 1$, on pose : $q^n-1 = hs(n)$, et on considère les endomorphismes φ_h et $\varphi_{s(n)}$ de $\mathbb{F}^*_{q^n}$ définis par :

$$\begin{cases} \varphi_h & : x \longmapsto x^h \\ \varphi_{s(n)} & : x \longmapsto x^{s(n)} \end{cases}$$

<u>Lemme 2</u> : $\quad \operatorname{Ker} \varphi_h = \operatorname{Im} \varphi_{s(n)} := \mu_h \subset \mathbb{F}_q^*$, $\operatorname{Ker} \varphi_{s(n)} = \operatorname{Im} \varphi_h$.

<u>Définition 1</u> : Soit $P \in \mathcal{M}$ irréductible ; pour tout $X \in \mathbb{F}_q[t]$ non divisible par P, on pose :

$$\left(\frac{X}{P}\right)_h = \varphi_{s(n)}(\bar{X}) \in \mu_h$$

où n désigne le degré de P et $\bar{X}$ la classe de X dans $[\mathbb{F}_q[t]/(P)]^*$.

Le théorème suivant est immédiat.

<u>Théorème 1</u>.- <u>Soit</u> $\lambda \in \mathbb{F}_q^*$ <u>et</u> $N \in \mathcal{M}$, <u>on pose</u> :

$$\lambda^{\theta_h(N)} := \left\{\lambda^{s(n)+h\nu} \ ; \ \nu \in \mathbb{Z}\right\} = \lambda^{s(n)} <\lambda^h>$$

<u>où</u> n <u>désigne le degré de</u> N.

1) <u>L'application</u> $N \longrightarrow \lambda^{\theta_h(N)}$ <u>est un morphisme de</u> $\mathcal{M}$ <u>dans</u> $\mathbb{F}_q^* /<\lambda^h>$.

2) <u>Si</u> P <u>est irréductible, on a</u> : $\left(\frac{\lambda}{P}\right)_h \in \lambda^{\theta_h(P)}$.

3) <u>Si</u> $(h,s(1)) = 1$, <u>alors</u> $\left(\frac{\lambda}{P}\right)_h$ <u>est caractérisé par cette inclusion</u>.

<u>Lemme 3</u>.- <u>Si</u> N_n <u>désigne la norme</u> $\mathbb{F}_{q^n}^* \longrightarrow \mathbb{F}_q^*$, <u>on a</u> : $\varphi_{s(n)} = \varphi_{s(1)} \circ N_n$.

<u>Preuve</u> : Si $\alpha \in \mathbb{F}_{q^n}^*$, on a :

$$N(x) = x^{1+q+\dots+q^{n-1}} = x^{\frac{q^n-1}{q-1}} = x^{\frac{s(n)}{s(1)}}$$

d'où :

$$\varphi_{s(n)}(x) = x^{s(n)} = \varphi^{s(1)}[N(x)]$$

Dans la suite, on posera $s(1) := s$.

2) <u>Loi de réciprocité</u>

On suppose toujours que $q-1 = hs$.

<u>Théorème 2</u>.- <u>Soient</u> P et $Q \in \mathcal{M}$, <u>irréductibles et distincts.</u>

1) <u>On a</u> :

$$\left(\frac{P}{Q}\right)_h : \left(\frac{Q}{P}\right)_h = (-1)^{s\,\deg(P).\deg(Q)}$$

2) <u>Si</u> q <u>est impair, on a</u> :

$$\left(\frac{P}{Q}\right)_h : \left(\frac{Q}{P}\right)_h = (-1)^{\frac{|P|-1}{h}\cdot\frac{|Q|-1}{h}} = (-1)^{\varepsilon_h(P)\varepsilon_h(Q)}$$

<u>Preuve</u> : On pose $m = \text{degré}(P)$, $n = \text{degré}(Q)$.

1) Soient $\alpha_1,\dots,\alpha_m$ les racines de P dans $\mathbb{F}_{q^m}$, on a :

$$N(Q) = \prod_{i=1}^{m} Q(\alpha_i) := R(P,Q)$$

et d'après le lemme 3 :

$$\varphi_{s_n}(Q) = \varphi_s[N(Q)] \equiv [R(P,Q)]^s \pmod P$$

et comme la réduction mod P est injective sur $\mathbb{F}_q^*$:

$$\left(\frac{Q}{P}\right)_h = [R(P,Q)]^s$$

2) De même :

$$\left(\frac{P}{Q}\right)_h = [R(Q,P)]^s$$

3) Comme il est bien connu que :

$$R(P,Q) : R(Q,P) = (-1)^{mn}$$

la première partie est démontrée.

4) Pour la seconde partie, on remarque que :

$$\frac{|P|-1}{h} = \frac{q^m-1}{h} = \left(\frac{q-1}{h}\right)(q^{m-1}+\dots+1)$$
$$\equiv sm \pmod 2$$

On a donc :

$$(-1)^{\frac{|P|-1}{h}\cdot\frac{|Q|-1}{h}} = (-1)^{(sm)(sn)} = (-1)^{smn}$$

3) Symbole de Jacobi

A partir de maintenant, on suppose que q est impair et que h et s sont premiers entre eux.

Soit $N = P_1 \ldots P_r \in \mathcal{M}$, où les $P_i \in \mathcal{M}$ sont irréductibles et non nécessairement distincts, et soit $X \in \mathbb{F}_q[t]$.

Définition 2.- On pose :

$$\begin{cases} \left(\frac{X}{N}\right)_h := \left(\frac{X}{P_1}\right)_h \cdots \left(\frac{X}{P_r}\right)_h, & \text{si } (X,N) = 1 \\ \left(\frac{X}{N}\right)_h := 0 & , \text{ sinon} \end{cases}$$

Théorème 3

1) Si $\lambda \in \mathbb{F}_q^*$, alors $\left(\frac{\lambda}{N}\right)_h$ est caractérisé par :

$$\left(\frac{\lambda}{N}\right)_h \in \lambda^{\theta_h(N)}$$

2) Si M et $N \in \mathcal{M}$, on a :

$$\left(\frac{M}{N}\right)_h : \left(\frac{N}{M}\right)_h = (-1)^{\frac{|M|-1}{h}\cdot\frac{|N|-1}{h}} = (-1)^{\varepsilon_h(M)\varepsilon_h(N)}$$

Preuve :

1) Si $\lambda \in \mu_h$, on a :

$$\left(\frac{\lambda}{N}\right)_h := \left(\frac{\lambda}{P_1}\right)_h \cdots \left(\frac{\lambda}{P_r}\right)_h = \lambda^{\theta_h(P_1)+\ldots+\theta_h(P_r)}$$

$$= \lambda^{\theta_h(P_1\ldots P_r)}$$

2) Si $\lambda \in \mathbb{F}_q^*$, alors $\lambda^s \in \mu_h$ et on a :

$$\left(\frac{\lambda}{N}\right)_h^s = \left(\frac{\lambda^s}{N}\right)_h = \lambda^{s\theta_h(P_1\ldots P_k)}$$

Comme $(s,h) = 1$, on en déduit que :

$$\left(\frac{\lambda}{N}\right)_h \in \lambda^{\theta_h(P_1\ldots P_h)}$$

3) La deuxième partie se montre par bilinéarité.

<u>Proposition 1</u>.- <u>Soit</u> $N \in \mathcal{M}$. <u>Pour que</u> N <u>soit une puissance</u> $h^{\text{ième}}$<u>, il faut et il suffit que pour tout</u> $X \in \mathbb{F}_q[t]$ <u>premier à</u> N <u>et tel que</u> $0 < |X| < |N|$, <u>on ait</u> :

$$\left(\frac{X}{N}\right)_h = 1$$

<u>Preuve</u> : On utilise le théorème chinois.

4) <u>Critères de primalité</u>

Ces critères ne prétendent pas remplacer celui de Berlekamp.

<u>Définition 3</u>.- Soit $B \in \mathbb{F}_q[t]$, $B \neq 0$.
Un polynôme $N \in \mathcal{M}$ sera dit "pseudo-premier en base B" lorsque l'on a :

$$B^{|N|-1} \equiv 1 \pmod N$$

<u>Exemple</u> : Si $\phi_n(X)$ désigne le polynôme cyclotomique d'ordre n, et si $B \in \mathcal{M}$, $B \notin \mu_n$, alors $\phi_n(B)$ est un polynôme pseudo-premier en base B.

Supposons N pseudo-premier en base B, on pose : $|N|-1 = h^{\nu}\sigma$, $0 < \nu$ et $(h,\sigma) = 1$.

Posons encore :

$$\begin{cases} B_o = B^{\sigma} \\ B_1 = B_o^h \\ \vdots \\ B_{\nu} = B_{\nu-1}^h \end{cases}$$

Il est clair que $B_{\nu} \equiv 1 \pmod N$. On appellera alors "indice de N" le plus petit entier ρ tel que $B_{\rho} \equiv 1 \pmod N$.

Définition 4 : Si N est pseudo-premier en base B, on dira que N est h-pseudo-premier fort en base B, ssi :

- soit $\rho = 0$
- soit il existe $\zeta \in \mu_h$ tel que $B_{\rho-1} \equiv \zeta \pmod{N}$.

Proposition 2.- On suppose que N est pseudo-premier d'indice $\rho > 0$ en base B. Alors si N n'est pas h-pseudo-premier fort en base B, deux au moins des p.g.c.d. $(N, B_{\rho-1} - \zeta)$ ne sont pas triviaux lorsque ζ parcourt μ_h.

La démonstration de cette proposition repose sur le lemme suivant :

Lemme 4.- $[\mathbb{F}_q[t]/(P^\nu)]^*$ est somme directe de $[\mathbb{F}_q[t]/(P)]^*$ et d'un ℓ-groupe.

Définition 5.- (C'est ici seulement qu'on utilise l'hypothèse que q est impair et que $(h,s) = 1$).

On dira que $N \in \mathcal{M}$ est un h-pseudo-premier eulérien en base B ssi :

$$B^{\frac{|N|-1}{h}} \equiv \left(\frac{B}{N}\right)_h \pmod{N}$$

Théorème 4.- Tout polynôme h-pseudo-premier fort en base B est h-pseudo-premier eulérien en base B.

Preuve : On écrit $N = P_1^{\alpha_1} \dots P_r^{\alpha_r}$.

1) C'est immédiat si $\rho = 0$.

2) Dans le cas général, on pose $|P_i| - 1 = h^\rho \tau_i$, avec $\tau_i \in \mathbb{N}$.

Le lemme 1 entraîne que : $\sigma h^{\nu-\rho} \equiv \Sigma \alpha_i \tau_i \pmod{h}$. Or :

$$\left(\frac{B_o}{P_i}\right)_h = \zeta^{\tau_i}$$

donc :

$$\left(\frac{B}{N}\right)_h = \prod_{i=1}^{r} \left(\frac{B}{P_i}\right)_h^{\alpha_i} = \zeta^{\frac{\Sigma \alpha_i \tau_i}{\sigma}} \equiv B_{\rho-1}^{h^{\nu-\rho}} \equiv B^{\frac{|N|-1}{h}} \pmod{N}$$

Received 23 June, 1986

Yves HELLEGOUARCH - Université de CAEN - FRANCE

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 5, October 1986 octobre

NOTE ON RINGS OF INTEGRAL-VALUED POLYNOMIALS

Fusao Shibata, Takasi Sugatani and Ken-ichi Yoshida

Presented by N.S. Mendelsohn, F.R.S.C.

Introduction. Let R be a Noetherian domain with quotient field K. Let $D(R)$ denote the ring of integral-valued polynomials $f(X) \in K[X]$ the polynomial ring in one variable X over K, such that $f(x) \in R$ for each $x \in R$. Most of the papers deal with Dedekind rings R, therefore are observed mainly the Dedekind-like properties of $D(R)$, see for instance [1], [2] and [4]. When R is assumed to be merely Noetherian, the ring $D(R)$ is more subtle. In fact it will be of interest to know when $D(R)$ is actually a proper overring of $R[X]$. In this note we will give some conditions for R to have the property $D(R) \neq R[X]$, in terms of depth one prime ideals of R. The following notation is fixed throughout this note. Let R, K, $R[X]$, $K[X]$ and $D(R)$ be as above. A polynomial of $D(R)$ not contained in $R[X]$ is said to be a special integral-valued polynomial of R. For a polynomial $f(X) \in R[X]$, C_f denotes the content ideal of $f(X)$. Our general reference for undefined terminology is [3].

First we recall the following fact of special integral-valued polynomials. The proof is straightforward.

LEMMA 1. *A polynomial* $f(X) \in K[X]$ *is a special integral-valued polynomial of* R *if and only if* $f(X)$ *can be written in the form* $f(X) = g(X)/a$, *where* a *is a nonzero nonunit of* R *and* $g(X) \in R[X]$ *satisfies that* $g(x) \in aR$ *for each* $x \in R$ *and* $C_g \not\subset aR$.

THEOREM 2. *For a Noetherian domain* R, *the following statements are equivalent.*

(1) $D(R) \neq R[X]$.

(2) *There exists a depth one prime ideal* p *of* R *such that* R/p *is a finite field*.

(3) *There exists a depth one prime ideal* p *of* R *such that* $D(R_p) \neq R_p[X]$.

(4) *There exists a prime ideal* p *of* R *such that* $D(R_p) \neq R_p[X]$.

PROOF. (1) $\Rightarrow$ (2): Assume (1). By Lemma 1, we have a nonzero nonunit $a \in R$ and a polynomial $g(X) \in R[X]$ such that $g(x) \in aR$ for each $x \in R$ and $C_g \not\subset aR$. Let $S = R/aR$, and let $\bar{g}(X) = a_nX^n+\ldots+a_0$ be the image of $g(X)$ in $S[X]$ under the natural homomorphism. Then $\bar{g}(X)$ vanishes on S, but is not a zero polynomial of $S[X]$. Now consider the primary decomposition of the ideal aR: $aR = q_1 \cap \ldots \cap q_s \cap Q_1 \cap \ldots \cap Q_t$, where $\sqrt{Q_j} = P_j$ $j = 1,\ldots,t$ are all of the maximal prime divisor of aR. Let $p_i = \sqrt{q_i}$ $i = 1,\ldots,s$. Since p_i, P_j are prime divisors of aR, they are of depth one. To establish (2), we want to show that at least one of R/p_i, R/P_j is a finite field. So we assume on the contrary that each of them is an infinite domain. Let $T = R/\cap_1^t P_j$, and let $u : S \to T$ be the natural surjection. Since T is a reduced ring with the minimal prime ideals $u(P_j)$ $j = 1,\ldots,t$, the total quotient ring F of T has the form $K_1 \times \ldots \times K_t$, where each K_j is the quotient field of R/P_j $j = 1,\ldots,t$. We let $v : T \to F$ be the natural injection. Let $A_j = \cup_0^n \{h \in K_j : h^e = 1\}$ $j = 1,\ldots,t$. Then it follows that there are nonzero elements $y_j \in K_j \smallsetminus A_j$ $j = 1,\ldots,t$. Now F is the total quotient ring of T, we can find a nonzero divisor $z \in T$ and elements $x_m' \in T$ such that $v(z)(y_1,\ldots,y_t)^m = v(x_m')$ $m = 0,\ldots,n$. Put $v(x_m') = (x_{1m},\ldots,x_{tm})$. Then $x_{jk} \neq x_{jm}$ for all $k \neq m$. As u being surjective, one obtains elements $x_m \in S$ such that $u(x_m) = x_m'$ $m = 0,\ldots,n$. Note that $\bar{g}(x_m) = 0$ for all $m = 0,\ldots,n$. Hence we have

$$\begin{bmatrix} 1 & x_0 & \cdots & x_0^{\,n} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & \cdots & x_n^{\,n} \end{bmatrix} \begin{bmatrix} a_0 \\ \vdots \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}.$$

Put

$$d = \begin{vmatrix} 1 & x_0 & \cdots & x_0^{\,n} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & \cdots & x_n^{\,n} \end{vmatrix}.$$

Since d is the Vandermonde's determinant, one can see that $vu(d) = (d_1,\ldots,d_t)$, where $d_j = \prod_{k<m}(x_{jk}-x_{jm})$ $j = 1,\ldots,t$. It then follows from the choice of x_{jm} that each $d_j \neq 0$. Hence d is not contained in any prime divisor of S. Thus d is a nonzero divisor of S, showing that $\bar{g}(X)$ is a nonzero polynomial. This is a contradiction. Hence (2) holds. (2) $\Rightarrow$ (1): Let p be a depth one prime ideal of R such that R/p is a finite field. Then it follows that $p = R :_R t$ for some $t \in K\setminus R$. Let $R/p = \{\bar{a}_1,\ldots,\bar{a}_n\}$, and let $a_i \in R$ be the pre-images of $\bar{a}_i$ $i = 1,\ldots,n$. The it can be seen easily that the polynomial $t\prod_1^n(X-a_i)$ is a special integral-valued polynomial of R, since for each $x \in R$, some $x-a_i \in p$. Thus (1) holds. (2) $\Rightarrow$ (3): Assume (2). Then for some depth one prime ideal p of R, R/p is a finite field, so trivially R_p/pR_p is a finite field. The above implication (2) $\Rightarrow$ (1) can be applied to obtain $D(R_p) \neq R_p[X]$. (3) $\Rightarrow$ (4): Trivial. (4) $\Rightarrow$ (2): If $D(R_p) \neq R_p[X]$ for some prime ideal p of R, then by (1) $\Rightarrow$ (2) above, we have a depth one prime ideal P of R such that $P \subseteq p$ and R_p/PR_p is a finite field. Hence in particular $P = p$ and R/P is a finite field. Hence (2) holds. Thus our theorem is completely proved.

The following is an immediate consequence of Theorem 2.

COROLLARY 3. (1) *If* R *contains an infinite field, then* $D(R) = R[X]$.
(2) *If* R *is normal, then* $D(R) \neq R[X]$ *if and only if there exists a height*

one prime ideal p *of* R *such that* R/p *is a finite field if and only if* R *has a valuation overring* V, *defining* R *such that the residue field of* V *is finite.*

REMARK. In the first statement of Corollary 3 the hypothesis R being Noetherian is superfluous, since the Vandermonde's determinant trick similar to the proof of Theorem 2 can be applied. This is certainly well-known, so we do not show the details.

If passing to the localization $(D(R))_p$ of $D(R)$ at a prime ideal p of R, we are naturally led to the following problem of when $D(R_p) = (D(R))_p$. We have partial results.

PROPOSITION 4. For every prime ideal p *of* R, $D(R_p) \subseteq (D(R))_p$ *holds.*

PROOF. Let p be a prime ideal of R. If $f(X) \in D(R_p)$, then $f(X) = g(X)/a$, where $g(X) \in R[X]$, $a \in R$. It then follows that $g(x) \in aR_p \cap R$ for each $x \in R$. On the other hand we have an element $t \in R \setminus p$ such that $t(aR_p \cap R) \subseteq aR$. Thus $tf(X) \in D(R)$. Hence $D(R_p) \subseteq (D(R))_p$.

PROPOSITION 5. If p *is a height one maximal ideal of* R, *then* $D(R_p) = (D(R))_p$. *In particular, if* R *is one-dimensional, then* $D(R_p) = (D(R))_p$ *for all prime ideals of* R, *and* $D(R) = \cap D(R_p)$, *the intersection taken over all prime ideals of* R.

PROOF. It is enough to prove the first statement, since the second statement is an immediate consequence of the first. Now one inclusion is Proposition 4. We show $D(R) \subseteq D(R_p)$ to complete the proof. Let $f(X) \in D(R)$. If $f(X) \in R_p[X]$, then we are done. So we assume $f(X) \notin R_p[X]$. Then we can find $g(X) \in R[X]$ and $a \in p$ such that $f(X) = g(X)/a$. Let $b \in R$ and $s \in R \setminus p$. Since R/p is a field, we can choose an element $t \in R$ such that $1-st \in pR_p$. But aR_p is a pR_p-primary ideal, so we may assume $1-st \in aR_p$. Thus $b/s = tb+ay$ for some $y \in R_p$. Since $g(X) \in R[X]$, it follows that $g(b/s) = g(tb+ay) \equiv g(tb) \mod aR_p$. Hence by assumption, $g(tb) \in aR$, and so $g(b/s) \in aR_p$. Thus $D(R) \subseteq D(R_p)$. With this the proof is complete.

REFERENCES

1. D. Brizolis, A theorem on ideals in Prüfer rings of integral-valued polynomials, Comm. Algebra 7(1979), 1065-1077.

2. R. Gilmer and W. W. Smith, Finitely generated ideals of the ring of integer-valued polynomials, J. Algebra 81(1983), 150-164.

3. H. Matsumura, Commutative algebra, W. A. Benjamin, New York, 1970.

4. D. L. McQuillan, On Prüfer domains of polynomials, J. Reine Angew. Math. 358 (1985), 162-178.

F. Shibata and K. Yoshida:

Department of Applied Mathematics
Okayama University of Science
Ridaicho, Okayama 700 JAPAN

T. Sugatani:

Department of Mathematics
Toyama University
Gofuku, Toyama 930 JAPAN

Received 26 June, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

AN ABSTRACT CHARACTERIZATION OF A FULL CLASS OF SURREAL NUMBERS

Norman L. Alling

Philip Ehrlich

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

Abstract: An axiomatic description of a full class of surreal numbers is given. It is shown that any two such classes have between them a unique order-preserving bijection that preserves birth-order. Since each of the classes of surreal numbers constructed to date is a full class of surreal numbers, the Main Theorem applies to any such pair.

0. Introduction. In On Numbers and Games [4] Conway defined his class No of surreal numbers. In [3] the authors gave a different, but very closely related, construction of a class No of surreal numbers. One can also construct a class of surreal numbers using as its basic object Conway's idea of the sign-expansion of a surreal number. (See [4, pp. 30-31] and [2] for details.) As we will see in another paper, the birth-order function in each of these constructions can be computed directly from the rank function. It certainly seems clear that these classes are essentially the same; however, to date this does not seem to have been proved.

This state of affairs resembles, to some degree, the status of the various constructions of the set of all real numbers: as Dedekind cuts in the rational numbers, as least upper bounds of bounded sets of rational numbers, as infinite decimals, ... Each of these constructions of the reals has its virtues. Once it has been shown that the field of all real numbers is, up to isomorphism, the only complete ordered field, one can pass freely back and forth between these various constructions, as need or inclination suggest. The Main Theorem has much the same impact on full classes of surreal numbers.

1. A Full Class of Surreal Numbers.

Let F be an ordered class. Given two subclasses L and R of F, we will write $L < R$ if given $x^L \varepsilon L$ and $x^R \varepsilon R$, then $x^L < x^R$. Following Conway, let a function b, called a birth-order function, be defined on F, and let it map F onto the class On of all ordinal numbers. Note first that since b maps F onto On, F is a proper class. Given $x, y \varepsilon F$, we will also follow Conway and say that x is simpler than y if $b(x) < b(y)$, x is as simple as y if $b(x) \leq b(y)$, ... $\{F, \leq, b\}$ will be said to satisfy Conway's Simplicity Theorem if the following holds.

(0) Given subsets L and R of F for which $L < R$, there exists a unique $x \varepsilon F$, with $L < \{x\} < R$, for which $b(x)$ is minimal. That is, for all $y \varepsilon F$ for which $L < \{y\} < R$, $b(x) \leq b(y)$. (Cf. [4, Theorem 11, p. 23].)

Assume that $\{F, \leq, b\}$ is such a triple and that it satisfies Conway's Simplicity Theorem (0). Let F" be a subclass of F. Given subsets L and R of F" for which $L < R$, we will call (L,R) a Conway cut in F". Let C(F") denote the class of all Conway cuts in F". Note that for each $(L,R) \varepsilon C(F")$, there is an element $x \varepsilon F$ (defined in (0)) which is uniquely determined by (L,R). We will define a function $\{\cdot|\cdot\}$ from C(F) into F by letting $\{L|R\}$ denote x. Since $\{\cdot|\cdot\}$ is not one-to-one x does not uniquely determine the Conway cut

(L,R). Given (L,R) and (L',R') in $C(F)$ such that $\{L|R\} = \{L'|R'\}$, we will call (L,R) and (L',R') equivalent. Clearly this is an equivalence relation on $C(F)$. Any $(L,R) \in C(F)$ for which $\{L|R\} = x$ will be called a Conway cut representation of x in $\{F,\leq,b\}$. We will call $(L,R) \in C(F'')$ timely if for all u in the union of L and R, $b(u) < b(x)$. Let $TC(F'')$ be the class of all timely Conway cuts in F''. Unless stated explicitly to the contrary, we will assume that all Conway cut representations are timely. Using Conway's notation and conventions [4, p. 4], we may also write $\{L|R\}$ as $\{x^L|x^R\}$, where x^L is a typical element in L and x^R is a typical element in R.

$\{F,\leq,b\}$ will be called a class of surreal numbers if, in addition to the properties that we have assumed for $\{F,\leq,b\}$, the following holds:

(1) given x and y in F, with $x = \{x^L|x^R\}$ and $y = \{y^L|y^R\}$, $x \leq y$ if and only if $x < y^R$ for all y^R, and $x^L < y$ for all x^L. (Cf. [4, p.4].)

Let $\{F,\leq,b\}$ be a class of surreal numbers. For each $\alpha \in On$, let $F(<,\alpha) = b^{-1}([0,\alpha))$, $F(\leq,\alpha) = b^{-1}([0,\alpha])$, and $F(=,\alpha) = b^{-1}(\{\alpha\})$.

(2) $\{F,\leq,b\}$ will be called full if $(L,R) \in C(F(<,\alpha))$, then $\{L|R\}$ is in $F(\leq,\alpha)$.

$\{No,\leq,b\}$, as defined in [3], is a full class of surreal numbers; as is Conway's class No [4]. The latter fact may be seen by consulting [4, p. 4], [4, pp. 15-17], Theorem 11 [4, p. 23], and [4, pp. 29-30]. Let $\{S,\leq,b\}$ denote the ordered class of all sign-expansions, as given by Conway [4, pp. 30-31]. Since Conway showed [4, p. 30] that the sign-expansion map $x \in No \to (x) \in S$ is an order-preserving bijection that preserves birth-order, $\{S,\leq,b\}$ is also a full class of surreal numbers. This can also be shown directly, by working on $\{S,\leq,b\}$ [2]. Finally, the <u>lexicographically ordered full binary tree of height</u> On (see [5, p. 216]) is another example. This follows almost immediately from the last result, and from Conway's Theorem 18 [4, p. 30].

Let $\{F,\leq,b\}$ be a full class of surreal numbers. Let $x\varepsilon F$, with $b(x) = \alpha$. Let $L = \{t\varepsilon F(<,\alpha): t < x\}$ and let $R = \{t\varepsilon F(<,\alpha): t > x\}$; then $L < \{x\} < R$. Let z be defined to be $\{L|R\}$. By (2) z is in $F(\leq,\alpha)$. Since the union of L and R is $F(<,\alpha)$, and since $L < \{z\} < R$ (0), $b(z) = \alpha$. Since $\{F,\leq,b\}$ satisfies Conway's Simplicity Theorem (0), $z = x$. Let (L,R) be called the <u>Cuesta Dutari cut representation</u> of x in $\{F,\leq,b\}$ (c.f., [3] and [4, p. 29]). Note that the Cuesta Dutari cut representation of x in $\{F,\leq,b\}$ is a timely Conway cut representation of x in $\{F,\leq,b\}$. Thus we have proved that

(3) (i) each $x\varepsilon F$ has a unique Cuesta Dutari cut representation in $\{F,\leq,b\}$;

(ii) hence $(L,R)\varepsilon TC(F) \to \{L|R\}\varepsilon F$ maps $TC(F)$ onto F.

2. <u>The Main Theorem.</u>

<u>Theorem.</u> <u>Assume that $\{F,\leq,b\}$ and $\{F',\leq',b'\}$ are full classes of surreal numbers. There exists a unique g of F onto F' such that for all $x \leq y$ in F, $g(x) \leq' g(y)$ in F', and $b(x) = b'(g(x))$, for all $x\varepsilon F$: i.e., such that g preserves order and birth-order.</u>

Proof. Let $\alpha\varepsilon On$. Assume that there exists a unique order-preserving map g_α from $F(<,\alpha)$ onto $F'(<',\alpha)$ such that $b = b'\cdot g_\alpha$ on $F(<,\alpha)$. Let (L,R) be the

Cuesta Dutari cut representation of $x \in F(=,\alpha)$ (3); then $(g_\alpha(L), g_\alpha(R))$, which we will define to be (L',R'), is in $C(F'(<',\alpha))$. Let $x' = \{L'|R'\}'$. By (2), x' is in $F'(\leq',\alpha)$. Since the union of L' and R' is $F'(<',\alpha)$, and since $L' <' \{x'\} <' R'$ (0), x' is not in $F'(<',\alpha)$; thus $b'(x') = \alpha$. As a result, we see that (L',R') is the Cuesta Dutari cut representation of x' in $\{F',\leq',b'\}$. Let g_α be extended to $g_{\alpha+1}$, by defining $g_{\alpha+1}(x)$ to be x', as constructed above, for each $x \in F(=,\alpha)$. Clearly $b = b' \cdot g_{\alpha+1}$ on $F(\leq,\alpha)$. Since (1) holds, $g_{\alpha+1}$ is an order-preserving map of $F(\leq,\alpha)$ into $F'(\leq',\alpha)$. Clearly $g_{\alpha+1}$ is unique. Let h_α be defined to be g_α^{-1}. Using the argument above we see that h_α extends to a unique order-preserving map $h_{\alpha+1}$ of $F'(\leq',\alpha)$ into $F(\leq,\alpha)$ such that $b' = b \cdot h_{\alpha+1}$ on $F'(\leq',\alpha)$. Clearly $g_{\alpha+1}$ and $h_{\alpha+1}$ are inverses of one another; thus $g_{\alpha+1}$ maps $F(\leq,\alpha)$ onto $F'(\leq',\alpha)$. By induction, the Theorem is proved.

Corollary. *There exists a unique order-preserving map, that preserves birth-order, which maps the class of Conway's surreal numbers [4] onto the class of surreal numbers constructed in [3].*

Let $\{F,\leq,b\}$ be a full class of surreal numbers. Let (L,R) and (L'',R'') be in $TC(F)$. L and L'' (resp R and R'') are *mutually cofinal* (resp. *mutually coinitial*) if for all $a \in L$ there exists $a'' \in L''$ such that $a \leq a''$, and for all $a'' \in L''$ there exists $a \in L$ such that $a'' \leq a$ (resp. if for all $c \in R$ there exists $c'' \in R''$ such that $c'' \leq c$, and for all $c'' \in R''$ there exists $c \in R$ such that $c \leq c''$).

Corollary. $\{L|R\} = \{L''|R''\}$ if and only if L and L'' are mutually cofinal and R and R'' are mutually coinitial.

Proof. Since this holds for $\{No, \leq, b\}$ [1, (2:0) and (2:1)] and since the Main Theorem is true, it holds for $\{F, \leq, b\}$.

References

1. N.L. Alling, Conway's Field of Surreal Numbers, Trans. Amer. Math. Soc. 287 (1985), 365-386.

2. -----------, Surreal Number Fields, Proceedings of the First International Symposium on Ordered Algebraic Structures, Heldermann Verlag, Berlin 1985.

3. ---------- and P. Ehrlich, An Alternative Construction of Conway's Surreal Numbers, submitted for publication.

4. J.H. Conway, On Numbers and Games, Academic Press, London, 1976.

5. S.F. Drake, Set Theory: An Introduction to Large Cardinals, North-Holland Publishing Co., Amsterdam, 1974.

Department of Mathematics
University of Rochester
Rochester, NY 14627
U.S.A.

Department of Philosophy
Brown University
Providence, RI 02912
U.S.A.

Received 9 July, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

ON THE SEPARATION OF MIDPOINT CONVEX SETS

Zs. Páles

Presented by J. Acsél, F.R.S.C.

ABSTRACT. In this note we show that the analogue of the theorem of Stone on the separation of disjoint convex sets is false if we replace "convex" by "midpoint convex".

Introduction. Let X be a linear space. The celebrated result of Stone [3] (see Holmes [1, p.7], Páles [2], Valentine [3, p.19]) reads as follows:

STONE'S THEOREM. Let A and B be disjoint convex subsets of the linear space X. Then there exist complementary convex sets A_o and B_o in X such that $A \subseteq A_o$ and $B \subseteq B_o$.

(Two sets A_o and B_o in X are complementary if they form a partition of X, that is $A_o \cup B_o = X$ and $A_o \cap B_o = \emptyset$.)

This result remains valid if we replace "convex" by "$\mathbb{F}$-convex" where $\mathbb{F}$ is an arbitrary subfield of $\mathbb{R}$ and we say that $A \subseteq X$ is $\mathbb{F}$-convex if $t \in \mathbb{F} \cap [0,1]$, $x,y \in A$ implies $tx+(1-t)y \in A$. The proof of this more general statement goes along the usual lines (see [1], [2], [3], [4]), therefore we can omit it.

Another natural concept for convexity is the Jensen-convexity or in other words, midpoint convexity: $A \subseteq X$ is called midpoint convex if $x,y \in A$ implies $(x+y)/2 \in A$.

The aim of this short note is to investigate the separation of midpoint convex sets and to show that the Stone theorem is false if we replace "convex" by "midpoint convex".

<u>Main result.</u> We shall need the following

LEMMA. <u>If</u> A <u>is a midpoint convex subset of the linear space</u> X <u>such that</u> $X\setminus A$ <u>is also midpoint convex then it is necessarily</u> $\mathbb{Q}$-<u>convex</u>.

P r o o f. Assume that A is not $\mathbb{Q}$-convex. Then there exist $p_o, q_o \in \mathbb{N}$ with $0 < 2p_o < q_o$ and $x_o, y_o \in A$ such that

$$u=(p_o/q_o)x_o+((q_o-p_o)/q_o)y_o \notin A. \tag{1}$$

Without loss of generality we can assume that q_o is minimal, that is

$$(p/q)x+((q-p)/q)y \in A \tag{2}$$

if $p,q \in \mathbb{N}$ with $0<p<q<q_o$ and $x,y \in A$ are arbitrary. (Then necessarily $q_o \geq 3$.) Consider now the element

$$v=((q_o-p_o)/q_o)x_o+(p_o/q_o)y_o.$$

If $v \notin A$ then, by (1) and by the midpoint convexity of $X\setminus A$, we have that

$$(u+v)/2 \notin A.$$

On the other hand

$$(u+v)/2= (x_o+y_o)/2 \in A,$$

since A is also midpoint convex. This contradiction shows that v must be in A. Now we can apply (2) for

$$x=v, \qquad y=y_o, \qquad p=p_o, \qquad q=q_o-p_o.$$

Thus we have that

$$A \ni (p_o/(q_o-p_o))v+((q_o-2p_o)/(q_o-p_o))u .$$

However this relation contradicts (1). This completes the proof of the Lemma.

To formulate our main result we need the concept of $\mathbb{Q}$- convex hull: If $A\subseteq X$ then the $\mathbb{Q}$-convex hull of A, written $co_{\mathbb{Q}}A$, is the intersection of all $\mathbb{Q}$-convex sets containing A, which is the set of all linear combinations

$$r_1a_1+ \dots +r_na_n$$

where $r_1,\dots,r_n\in\mathbb{Q}$ with $r_1,\dots,r_n>0$, $r_1+\dots+r_n=1$ and $a_1,\dots,a_n\in A$, $n\in\mathbb{N}$ are arbitrary.

THEOREM. Let A and B be disjoint midpoint convex subsets in X. Then there exist complementary midpoint convex subsets A_o and B_o in X such that $A\subseteq A_o$ and $B\subseteq B_o$ if and only if the intersection of the $\mathbb{Q}$-convex hulls of A and B is empty.

P r o o f. If A_o and B_o exist then, by the Lemma, we have that they are also $\mathbb{Q}$-convex sets. Since then $co_{\mathbb{Q}}A\subseteq A_o$ and $co_{\mathbb{Q}}B\subseteq B_o$ further $A_o\cap B_o=\emptyset$ hence $co_{\mathbb{Q}}A\cap co_{\mathbb{Q}}B=\emptyset$.
On the other hand, if $A^*=co_{\mathbb{Q}}A$ and $B^*=co_{\mathbb{Q}}B$ have empty intersection then, applying the Stone theorem for $\mathbb{Q}$-convex sets, we can find complementary $\mathbb{Q}$-convex sets A_o and B_o in X such that $A^*\subseteq A_o$ and $B^*\subseteq B_o$. Thus the proof is complete.

EXAMPLE. Let A be the set of all dyadic rational numbers, i.e.

$$A=\{p/2^n \mid p\in\mathbb{Z},\quad n\in\mathbb{N}\cup\{0\}\}$$

and let $B=\{1/3\}$. Then A and B are disjoint midpoint convex sets, but $co_{\mathbb{Q}}A=\mathbb{Q}$ which shows that A and B cannot be separated by complementary midpoint convex sets.

This example shows that the Stone theorem is false if we replace "convex" by "midpoint convex".

REFERENCES

[1] R. Holmes, Geometric functional analysis and its applications, Springer Verlag, New York-Heidelberg-Berlin, 1975.

[2] Zs. Páles, A Stone-type theorem for Abelian semigroups, submitted to Arch. Math..

[3] M. H. Stone, Convexity (mimeographed lecture notes), prepared by Harley Flanders, University of Chicago, Chicago, 1946.

[4] F. A. Valentine, Convex sets, McGraw-Hill Book Company, New York-San Francisco-Toronto-London, 1964.

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

Received 17 July, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

MIXED HODGE STRUCTURE IN ALGEBRAIC K-THEORY AND CYCLIC HOMOLOGY

Andrew J. Nicas

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

Abstract. Let C be a chain algebra which carries the structure of a multiplicative mixed Hodge complex as defined by Deligne. Then the Hochschild and cyclic hyperhomology of C have natural mixed Hodge structures and the Connes-Gysin sequence is an exact sequence of mixed Hodge structures. This result is applied to show that the reduced Waldhausen K-theory of a simply connected quasi-projective variety has a mixed Hodge structure and also that for any quasi-projective variety the reduced algebraic K-theory of the fundamental group-ring modulo a power of the augmentation ideal has a mixed Hodge structure.

Deligne defined the notion of a mixed Hodge structure (MHS) in [2] and proved that every quasi-projective variety over $\mathbf{C}$ has a natural MHS on its cohomology. The homotopy Lie algebra of a pointed topological space (X,x) is the graded Lie algebra $g_*(X,x)$ where $g_0(X,x)$ is the Malcev Lie algebra associated with $\pi_1(X,x)$ and, when $k \geq 1$,

$$g_k(X,x) = \begin{cases} \pi_{k+1}(X,x) \otimes \mathbf{Q} & \text{if } (X,x) \text{ is a nilpotent space} \\ 0 & \text{otherwise} \end{cases}$$

In [5] Morgan showed that the homotopy Lie algebra of every smooth quasi-projective variety over $\mathbf{C}$ has a natural MHS. Hain [4] extended these results to arbitrary quasi-projective varieties. Waldhausen [6] defined the algebraic K-theory of a topological space. His functor, $A(X)$, which depends on the homotopy type of X is important because of its relationship to pseudo-isotopy theory. We prove

Theorem. Let X be a simply connected quasi-projective variety over $\mathbf{C}$. Then for $j \geq 1$ the reduced Waldhausen K-theory $\pi_j\tilde{A}(X)$ has a natural MHS.

A related result is that the homology of the free loop space of such a space has a natural MHS. There is an analogue to the above theorem in the non-simply connected case:

Theorem. Let X be a quasi-projective variety over $\mathbf{C}$ and $x \in X$ a basepoint. Let $\pi = \pi_1(X,x)$, and $J = \text{kernel } (\mathbf{Z}\pi \to \mathbf{Z})$, the augmentation ideal. Then for $s \geq 0$ and $j \geq 1$ the reduced K-theory $\tilde{K}_j(\mathbf{Z}\pi/J^{s+1})$ has a natural MHS.

The theorems corresponding to the above two theorems are also valid in the Kähler case. The proof of these results proceeds via the cyclic homology of Connes [1] and uses the results of Goodwillie [3] concerning the relationship between the K-theory of simplicial rings and cyclic homology. The following result establishes the connection between Hodge theory and cyclic homology.

Theorem. Let $((C^E,W^E), (C,W,F))$ be a multiplicative mixed Hodge complex defined over a field E, $\mathbf{Q} \subset E \subset \mathbf{R}$. Then for each n the Hochschild and cyclic hyperhomology $HH_n(C)$ and $HC_n(C)$ have MHS's defined over E; furthermore, the Connes-Gysin sequence

$$\cdots \to HH_n(C) \xrightarrow{I} HC_n(C) \xrightarrow{S} HC_{n-2}(C) \xrightarrow{B} HH_{n-1}(C) \to \cdots$$

is an exact sequence of MHS's over E, where I, S, and B have type $(0,0)$.

The analogous result is also true in the relative case. In order to prove this theorem the notion of a multi-graded mixed Hodge complex (MHC) is introduced generalizing Deligne's definition. The total complex of a multi-graded MHC is shown to be again an MHC; furthermore, the complexes used to define Hochschild and cyclic homology can be given the structure of a multi-graded MHC under the hypotheses of the above theorem.

Acknowledgements. The author was supported by an NSERC University Research Fellowship and operating grant. I am very grateful to R. Hain for explaining his version of Hodge theory to me. I would also like to thank the Institute for Advanced Study and the Institut des Hautes Etudes Scientifiques for their hospitality during the year 1985-86 when this work was done.

References

1. A. Connes, Non-commutative differential geometry, Pub. Math. IHES 62 (1986), 257-360.
2. P. Deligne, Théorie d'Hodge II and III, Pub. Math. IHES 40 (1971), 5-58 and 44 (1975), 5-77.
3. T. Goodwillie, Algebraic K-theory and cyclic homology, to appear in Ann. of Math.
4. R. Hain, Mixed Hodge structures on homotopy groups, Bull. Amer. Math. Soc. 14 (1986), 111-114.
5. J. Morgan, The algebraic topology of smooth algebraic varieties, Pub. Math. IHES 48 (1978), 137-204.
6. F. Waldhausen, Algebraic K-theory of topological spaces I, Proc. Symp. Pure Math. 32 (1978), 35-60.

Department of Mathematics
University of Toronto
Toronto, Ontario M5S 1A1
Canada

Received July 18, 1986.

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

A SOLUTION TO BAGEMIHL'S CONJECTURE

Joseph Zaks

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

Abstract

Bagemihl gave in 1956 an example of eight tetrahedra in E^3 in which every pair meet in a 2-dimensional set; he also showed that the maximum number of such tetrahedra is at most 17. Baston proved in 1965 that $m \leq 9$. Both of them conjectured that $m = 8$. The conjecture had been repeatedly raised in the literature, in particular by Klee in 1969.

We have an affirmative solution to Bagemihl's conjecture, based on Baston's work, using combinatorics and computer search of all decompositions of the complete graph K_9 on nine vertices into certain collections of complete bipartite subgraphs.

A family of tetrahedra in E^3 is called neighborly [5, 6, 8] if every two of them meet in a 2-dimensional set. Let m denote the maximum number of tetrahedra in a neighborly family in E^3 . Bagemihl [1] proved that $8 \leq m \leq 17$ and conjectured that $m = 8$. Baston [2] showed that $8 \leq m \leq 9$ and conjectured that $m = 8$. The conjecture that $m = 8$ was mentioned in [3, 5] and in particular in [6], and in [7, 9]; extensions of these results can be found in [7-11].

To settle Baston's Conjecture affirmatively, suppose on the contrary that there exists a neighborly family $F = \{P_1, \ldots, P_9\}$ consisting of nine tetrahedra. Let $\{H_1, \ldots, H_t\}$ be the collection of all the planes which contain facets of members of F . The Baston matrix $B(F) = (b_{ij})$ is defined [2, 7, 10, and in variant form in 13] by

$$b_{ij} = \begin{cases} 1 & \text{if } H_j \text{ contains a facet of } P_i \text{ and } P_i \subset H_j^+ , \\ -1 & \text{" " " " " " " } P_i \subset H_j^- , \\ 0 & \text{otherwise,} \end{cases}$$

$1 \le i \le n$, $1 \le j \le t$, and where H_j^+ and H_j^- denote the two closed half-spaces determined by H_j .

Let x_{ij} , $i \le j$, denote the number of columns of $B(F)$ which contain precisely i non-zero terms of one sign and precisely j non-zero terms of the opposite sign.

The following properties hold:

(1) $j \ge 4$ implies that $x_{ij} = 0$,

(2) $x_{3,3} = 0$,

(3) $\sum (i+j)x_{ij} = 36$,

(4) $\sum ijx_{ij} = 36$,

(5) $0 \le x_{0,1} \le 2$,

(6) $K_9 = \sum_{i,j\ge 1} x_{ij}K_{i,j}$ (i.e., the complete graph K_9 decomposes into x_{ij} copies of complete bipartite graphs $K_{i,j}$, for all i, j),

(7) $\sum_{i,j\ge 1} x_{ij} \ge 8$.

(8) Each vertex of K_9 appears in at most four components in the decomposition given in (6).

Properties (1), (2) and (5) are due to Baston [2]; (3) and (4) were shown in [8], and they are equivalent to Baston's equations involving his "surplus". (6) was mentioned, in a variant form, in [11], and the idea is to look at the rows of B(F) as vertices, and to connect row i to row j by an edge whenever there exists a column k in $B(F)$, such that $b_{ik} \cdot b_{jk} = -1$. (7) follows from (6) by the Graham-Pollak [4] Theorem. (8) follows from the fact that every P_i has four facets, hence every row of $B(F)$ has four non-zero terms.

The Diophantine system (1-5) has 24 possible solutions; two of them were shown by Baston [2] to be impossible.

We treat all the remaining cases, and show that each one of them is impossible. There are various reasons, and we describe them in brief.

One case is shown to violate (6) and (7). A few other cases are impossible, due to the fact that the tetrahedra are dissected by the planes $H_1, \ldots, H_t$ into too many bounded pieces (more than the maximum possible number of bounded pieces determined by t planes in E^3).

For all the remaining cases, we analyze the possible combinations of types of tetrahedra in F, where a tetrahedron is said to be of type (p,q,r,s) if it touches p other members of F on one facet, q on another facet, etc; the possible types are (3, 3, 2, 0), (3, 3, 1, 1), (3, 2, 2, 1) and (2, 2, 2, 2) (assuming $p \geq q \geq r \geq s$). We extend Baston's observation that the value of $x_{2,2}$ puts some restrictions on the possible types.

For all these remaining cases, we have produced by computer all the possible decompositions of K_9, while trying to avoid repetitions (up to permutations of the vertices or the members of F). We proved directly, in each such an output, that the $0, \pm 1$ matrix, corresponding to the given decomposition of K_9, is not the Baston matrix of F.

The last reason of impossibility, used extensively by Baston, is actually a well-known lemma in linear programming, used in the simplex method; it states, in general, that "If $Q = \{x \in E^d \mid Ax^T \leq b^T\}$, where A is a $k{\times}d$-matrix, b is a k-vector, and A has a non-negative (or non-positive) column, then $Q = \emptyset$ or else Q is unbounded". Thus, given a $0, \pm 1$ matrix representing a decomposition of K_9, we consider the possible signs of the coefficients in the equations of the planes H_i, assuming the matrix is the Baston matrix $B(P)$ of F; since all the P_i's are non-empty, the contradiction obtained is by showing that one of the tetrahedra is necessarily unbounded.

The detailed proof, including the description of the algorithms used, will appear elsewhere.

References

1. Bagemihl, F., A conjecture concerning neighboring tetrahedra, Amer. Math. Monthly 63 (1956), 328-329.
2. Baston, V.J.D., some properties of polyhedra in Euclidean space, Pergamon Press, Oxford, 1965.
3. Danzer, L., Grünbaum, B. and Klee, V., Helly Theorem and its Relatives, Amer. Math. Soc. Proc. Symp. Pure Math. 7 (1963), 101-180.
4. Graham, R.L. and Pollak, H.O., On the addressing problem for loop switching, Bells Sys. Tech. J. 50 (1971), 2495-2519; see also Vol. 303 of Springer Lecture Notes in Math., Springer, New York, (1973), 99-110.
5. Grünbaum, B., convex Polytopes, J. Wiley & Sons, New York, 1967.
6. Klee, V., Can nine tetrahedra form a neighboring family?, Amer. Math. Monthly 76 (1969), 178-179.

7. Perles, M.A., At most 2^{d+1} neighborly simplices in E^d, Proc. Conf. Convexity and Graph Theory, Israel, 1981, Ann. Discrete Math. 20 (1984), (M. Rosenfeld ans J. Zaks, ed.), 253-254.

8. Zaks, J., Bounds of neighborly families of convex polytopes, Geometriae Dedicata 8 (1979), 279-296.

9. Zaks, J., Neighborly families of 2^d d-simplices in E^d, Geometriae Dedicata 11 (1981), 505-507.

10. Zaks, J., Arbitrarily large neighborly families of symmetric convex polytopes, Geometriae Dedicata (to appear).

11. Zaks, J., How does a complete graph split into bipartite graphs and how are neighborly cubes arranged? Amer. Math. Monthly 92 (1985), 568-571.

Received July 21, 1986

Dept. of Mathematics
University of Haifa
Mount Carmel, Haifa 31999
Israel.

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No. 5, October 1986 octobre

Derivative Estimates for the Navier-Stokes equations in three space dimensions

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

Abstract. On a smoothly bounded three-dimensional domain Ω let $u(x,t)$ be a vector solution of the Navier-Stokes equations for $t > 0$, vanishing on the boundary and smooth except on a singular set of low dimension. Then the $L^2(\Omega)$ norm of $D_t^r D_x^s u$ is integrable to the power $2(4r+2s-1)^{-1}$ over every finite time interval $(0,T)$, where r or s is positive, and $\max_{x \in \Omega} |D_t^r D_x^s u|$ is integrable over $(0,T)$ to the power $(2r+s+1)^{-1}$; $r,s = 0,1,2,...$

1. Introduction. Let $x_i (i = 1,2,3)$ be Cartesian coordinates in R^3 and $u_i(x,t)$ velocity components, $p(x,t)$ pressure for a viscous incompressible Navier-Stokes flow: $u_{i,t} + u_k u_{i,k} = -p_{,i} + \nu \Delta u_i$, $u_{i,i} = 0$, where ν is the constant viscosity and Δ the Laplacian operator. The summation convention is used, and subscript comma, or ∇ or D to denote derivatives. For $t = 0$ let $u(x,0) = u_0(x) \in L^2(\Omega)$ where $x \in \Omega$ a smoothly bounded domain of R^3 with compact boundary $\partial\Omega$, or a suitable three- dimensional manifold. Let $u_i(x,t) = 0$ for $x \in \partial\Omega$, $t > 0$ and consider solutions $u_i(x,t)$ smooth except on a singular set of low dimension [2,9,10]. Constants $C = C(\nu,\Omega,\partial\Omega)$ will in general be different at each occurrence.

That singularities wherein momentum locally overwhelms viscosity might occur was first pointed out by Leray [8]. The actual existence of such singular solutions is close to being established through the work of Ladyzhenskaya [7] and Scheffer [9,10,11], while the low dimension and the finite bound over time of the singular set have been established [7,8,9]. Our estimates over an arbitrary finite time interval therefore characterize all suitable solutions including singular solutions as well as behaviour when $t \to 0+$ [6]. Here smooth shall mean C^∞, while $s = (s_1,s_2,s_3)$ is a 3-index labelling space derivatives.

2. The Main Results. Let $\|u\|_p = \|u(x,t)\|_p = (\int_\Omega |u|^p dV)^{1/p}$ where $1 \le p \le \infty$. These norms are functions of time t, and are in turn contained in spaces $L^q(0,T)$ for fractional values of q.

Theorem *Let $u_i(x,t)$ be a Navier-Stokes flow in a bounded three dimensional domain Ω, u being smooth except on a singular set. Over any finite time interval $(0,T)$ we have, for $r,s_j = 0,1,2,...;$ $s = s_1+s_2+s_3$,*

$$\|D_t^r D_x^s u\|_2 \in L^{2(4r+2s-1)^{-1}}(0,T)$$

for r or $s_j > 0$, and

$$\max_{x \in \Omega} |D_t^r D_x^s u| = \|D_t^r D_x^s u\|_\infty \in L^{(2r+s+1)^{-1}}(0,T).$$

The proof will be outlined after a brief discussion of the special case of a three dimensional closed manifold.

3. Closed manifolds. If there is no boundary, as for a periodic parallelepiped or 3-torus, or R^3 with sufficiently rapid decrease at infinity, the problem can be simplified. The case $r = 0$ for the 3-torus has been established [3,5]. Assuming this, we use $\Delta p = -u_{k,j}u_{j,k}$ to obtain

$$\Delta u_{i,t} = -\Delta(u_k u_{i,k}) + (u_{k,j}u_{j,k})_{,i} + \nu\Delta\Delta u_i.$$

As we can freely integrate by parts on a manifold without boundary, estimates for Δu_i imply those for the second space derivatives $D_k D_j u_i$. For $s \geq 2$ the result now follows by induction on r, since all terms on the right of the above equation, or any further differentiated form of it, will have the same integrability behaviour in consequence of standard embedding inequalities. Thus we can use the equation as a finite difference template, or molecule, in the (r,s) lattice, with s decreasing two steps as r increases by one. The cases $s = 0$ and $s = 1$ remain and can be treated by an induction on r with estimates similar to the second part of the main proof described below.

4. Estimate of the scalar potential. A vector field $u \in L^2(\Omega)$ has orthogonal solenoidal and gradient parts [7, p 23]. Let $\Delta u_i = \bar{\Delta} u_i + f_{,i}$ where the Stokes operator term $\bar{\Delta} u_i$ is solenoidal and has vanishing normal component on $\partial\Omega$. For the scalar potential f, we have

Lemma 1. $\|\nabla f\|_2^2 \leq C\|\nabla u\|_2(\|\bar{\Delta} u\|_2 + C_1\|\nabla u\|_2).$

Outline of proof: Let $N = N(P,Q) = N(Q,P)$ be the harmonic Neumann function for Laplace's operator on Ω; thus $\frac{\partial N}{\partial n_Q} = 0$ on $\partial\Omega$ while $\Delta N = \delta - \frac{1}{V}$ with $V = \int_\Omega 1\, dV$ [4, p 280]. As u is solenoidal, $\Delta f = (\Delta u_i)_{,i} - (\bar{\Delta} u_i)_{,i} = 0$ so f is harmonic, with $\frac{\partial f}{\partial n} = \Delta u_i n_i$ on $\partial\Omega$. Hence $f = \int_{\partial\Omega} N\Delta u_i n_i dS = \int_{\partial\Omega} K\Delta u_i n_i dS$ where $K = N - G$ is the Bergman kernel of Ω and G the Green's function which vanishes on $\partial\Omega$ [1, p 275]. By the Gauss and Green integral theorems,

$$f = \int_\Omega (K\Delta u_i)_{,i} dV = \int_\Omega K_{,i}\Delta u_i dV = \int_{\partial\Omega} K_{,i}\frac{\partial u_i}{\partial n} dS = \int_{\partial\Omega} K_{,\alpha}\frac{\partial u_\alpha}{\partial n} dS,$$

Here α runs through tangential indices only since $u_{n,n} = 0$ on $\partial\Omega$ by the solenoidal relation $u_{i,i} = 0$ and the boundary condition $u = 0$ on $\partial\Omega$. Now it can be shown that the kernels $K_{,\alpha}(P,Q)$ and $\frac{\partial K_{,\alpha}}{\partial n}(P,Q)$ define bounded operators on $L^2(\partial\Omega)$, their leading singular terms being of Calderon-Zygmund type.

Thus $\|\nabla f\|_2^2 = \int_{\partial\Omega} f\frac{\partial f}{\partial n}dS \le \|f\|_{2,\partial}\|\frac{\partial f}{\partial n}\|_{2,\partial}$ where the subscript ∂ denotes integration over the boundary. Hence we find, by the above $L^2(\partial\Omega)$ boundedness property,

$$\|\nabla f\|_2^2 \le C\|\frac{\partial u_\alpha}{\partial n}\|_{2,\partial}^2 = C\int_{\partial\Omega}\left[\frac{\partial u_\alpha}{\partial n}\right]^2 dS \le C\int_\Omega |D_j u_\alpha|\,\{|D_j D_k u| + |D_j u|\}dV.$$

By an estimate of Ladyzhenskaya [7, p 20] we now have

$$\|\nabla f\|_2^2 \le C\|\nabla u\|_2\{\|\Delta u\|_2 + \|\nabla u\|_2\} \le C\|\nabla u\|_2\{\|\bar{\Delta} u\|_2 + \|\nabla f\|_2 + \|\nabla u\|_2\}$$

and the lemma follows after use of Young's inequality, in the form $ab \le \varepsilon a^2 + C(\varepsilon)b^2$.

5. A quadruple sequence of estimates. We use

Lemma 2. Let $a > 1$, $F(t) \ge 0$, $F(t) \in L^p(0,T)$, $G(t) \ge 0$ and, for $0 \le t \le T$, $F'(t) + G(t) \le KF(t)^{a+p}$. Then $G(t) \in L^{p(a+p)^{-1}}(0,T)$.

The proof is omitted; see [5] where the method is introduced.

We carry out an induction on r simultaneously for $D_t^r u$, $D_t^r\nabla u$ and $D_t^r\bar{\Delta}u$, using four sequences of estimates formed by differentiating the Navier-Stokes equations r times with respect to t and multiplying by $D_t^r u_i$, $D_t^r\bar{\Delta}u_i$, $D_t^{r+1}u_i$ and $D_t^{r+1}\bar{\Delta}u_i$, respectively. Each estimate is expressed by an inequality, and is numbered by its reciprocal time exponent or index or order of singularity:

1 $\quad D_t\|u\|_2^2 + 2\nu\|\nabla u\|_2^2 = 0$

3(a) $\quad D_t\|\nabla u\|_2^2 + \nu\|\bar{\Delta}u\|_2^2 \le C\|\nabla u\|_2^6$

3(b) $\quad \nu D_t\|\nabla u\|_2^2 + \|u_t\|_2^2 \le C\|\nabla u\|_2^3\|\bar{\Delta}u\|_2$

5(a) $\quad \nu D_t\|\bar{\Delta}u\|_2^2 + \|\nabla u_t\|_2^2 \le C\|\bar{\Delta}u_t\|_2\|\nabla u\|_2^{3/2}\|\bar{\Delta}u\|_2^{1/2}$

5(b) $\quad D_t\|u_t\|_2^2 + \nu\|\nabla u_t\|_2^2 \le C[\|u_t\|_2^{10/3} + \|\nabla u\|_2^{10}]$

7(a) $\quad D_t\|\nabla u_t\|_2^2 + \nu\|\bar{\Delta}u_t\|_2^2 \le C[\|\nabla u_t\|_2^{14/5} + \|\bar{\Delta}u\|_2^{14/3} + \|\nabla u\|_2^{14}]$

7(b) $\quad \nu D_t\|\nabla u_t\|_2^2 + \|u_{tt}\|_2^2 \le C[\|\nabla u_t\|_2^2\|\nabla u\|_2\|\bar{\Delta}u\|_2 + \|\nabla u\|_2^2\|\nabla u_t\|_2\|\bar{\Delta}u_t\|_2]$

9(a) $\quad \nu D_t\,\|D_t\bar{\Delta}u\|_2^2 + \|D_t^2\nabla u\|_2^2 \le C\|D_t^2\bar{\Delta}u\|_2\,(\|\nabla u\|_2\|D_t\nabla u\|_2^{1/2}\|D_t\bar{\Delta}u\|_2^{1/2} + \|D_t\nabla u\|_2\|\nabla u\|_2^{1/2}\|\bar{\Delta}u\|_2^{1/2})$

. . . . . .

$$(4r+1)(b)\ D_t\|D_t^r u\|_2^2+\nu\|D_t^r\nabla u\|_2^2 \le C[\|D_t^r\|_2^2\|\nabla u\|_2\|\bar{\Delta}u\|_2+\sum_{j=1}^{r-1}\|D_t^r u\|_2\|D_t^j\nabla u\|_2\|D_t^{r-j}\nabla u\|_2^{1/2}\|D_t^{r-j}\bar{\Delta}u\|_2^{1/2}]$$

$$(4r+3)(a)\ D_t\|D_t^r\nabla u\|_2^2 + \nu\|D_t^r\bar{\Delta}u\|_2^2 \le C[\|D_t^r\nabla u\|_2^2\|\nabla u\|_2(\|\nabla u\|_2^3 + \|\bar{\Delta}u\|_2)$$
$$+ \sum_{j=1}^{r-1}\|D_t^j\nabla u\|_2^2\|D_t^{r-j}\nabla u\|_2\|D_t^{r-j}\bar{\Delta}u\|_2]$$

$$(4r+3)(b)\ \nu D_t\|D_t^r\nabla u\|_2^2 + \|D_t^{r+1}u\|_2^2 \le C \sum_{j=0}^{r} \|D_t^j\nabla u\|_2^2\|D_t^{r-j}\nabla u\|_2\|D_t^{r-j}\bar{\Delta}u\|_2$$

$$(4r+5)(a)\ \nu D_t\|D_t^r\bar{\Delta}u\|_2^2 + \|D_t^{r+1}\nabla u\|_2^2 \le C\ \|D_t^{r+1}\bar{\Delta}u\|_2 \sum_{j=0}^{r} \|D_t^j\nabla u\|_2\|D_t^{r-j}\nabla u\|_2^{1/2}\|D_t^{r-j}\bar{\Delta}u\|_2^{1/2}$$

. . . . .

The estimate of $\|\nabla u\|_2$ from 1 is well known. Adding 3(a) and 3(b) we obtain after use of Young's inequality:

3: $(1 + \nu)D_t\|\nabla u\|_2^2 + \tfrac{1}{2}\nu\|\bar{\Delta}u\|_2^2 + \|u_t\|_2^2 \le C\|\nabla u\|_2^6$.
Hence by Lemma 2, $G_3(t) = \tfrac{1}{2}\nu\|\bar{\Delta}u\|_2^2 + \|u_t\|_2^2 \in L^{1/3}(0,T)$ as is $\|\nabla u\|_2^6 = F_3(t)^3$.

From 5(b) and 3(a) multiplied by $3\|\nabla u\|_2^4$ we find

5: $D_t[\|u_t\|_2^2 + \|\nabla u\|_2^6] + \nu[\|\nabla u_t\|_2^2 + 3\|\nabla u\|_2^4\|\bar{\Delta}u\|_2^2] \le C[\|u_t\|_2^{10/3} + \|\nabla u\|_2^{10}] \le C[\|u_t\|_2^2 + \|\nabla u\|_2^6]^{5/3}$
so by Lemma 2, $G_5(t) = \|\nabla u_t\|_2^2 + 3\|\nabla u\|_2^4\|\bar{\Delta}u\|_2^2 \in L^{1/5}(0,T)$, as is the right side $F_5(t)^{5/3}$.

From 7(a), 7(b), 5(a) multiplied by $\frac{5}{3}\|\bar{\Delta}u\|_2^{4/3}$ and 3(a) multiplied by $5\|\nabla u\|_2^8$ we get

$$7: D_t[(1 + \nu)\|\nabla u_t\|_2^2 + \|\bar{\Delta}u\|_2^{10/3} + \|\nabla u\|_2^{10}] + \nu\|\bar{\Delta}u_t\|_2^2 + \|u_{tt}\|_2^2 + 5\nu\|\nabla u\|_2^8\|\bar{\Delta}u\|_2^2 + \frac{5}{3}\|\bar{\Delta}u\|_2^{4/3}\|\nabla u_t\|_2^2$$
$$\le C[\|\nabla u_t\|_2^{14/5} + \|\bar{\Delta}u\|_2^{14/3} + \|\nabla u\|_2^{14}] \le C[\|\nabla u_t\|_2^2 + \|\bar{\Delta}u\|_2^{10/3} + \|\nabla u\|_2^{10}]^{7/5}.$$

Thus by Lemma 2, $G_7(t) = \nu\|\bar{\Delta}u_t\|_2^2 + \|u_{tt}\|_2^2 + 5\|\nabla u\|_2^8\|\bar{\Delta}u\|_2^2 + \frac{5}{3}\|\bar{\Delta}u\|_2^{4/3}\|\nabla u_t\|_2^2 \in L^{1/7}(0,T)$ as is the right hand side $F_7(t)^{7/5}$.

This pattern is maintained, so proceeding inductively we deduce the estimates for $\|\nabla u\|_2$, $\|\bar{\Delta}u\|_2$, $\|u_t\|_2$, $\|\nabla u_t\|_2$, $\|\bar{\Delta}u_t\|_2$, $\|u_{tt}\|_2$, $\cdots$ and the corresponding triple sequence of higher time derivatives $\|D_t^r\nabla u\|_2$, $\|D_t^r\bar{\Delta}u\|_2$, and $\|D_t^{r+1}u\|_2$. At each stage we use the preceding inequalities multiplied by well-determined factors that raise their reciprocal indices to the new level. Each relation is homogeneous with index equal to its numerical label.

From Lemma 1 we also deduce $\|\nabla f\|_2 \in L^1(0,T)$ so that $\|\Delta u\|_2^2 = \|\bar{\Delta}u\|_2^2 + \|\nabla f\|_2^2 \in L^{1/3}(0,T)$, and similar relations for $f_t, f_{tt}, \cdots$. An estimate of Ladyzhenskaya [7, p 21] now shows that $\|D_x^2u\|_2 \in L^{2/3}(0,T)$, and similar results follow inductively for the higher time derivatives $D_t^r D_x^2 u$. Induction on r now yields the main result for all $r = 0,1,2,...$ in the cases $s = 0,1,2$.

6. Tangential derivatives. In a suitable local coordinate system, the higher tangential derivatives of u will also vanish on the boundary. Hence for each tangential derivative $D_\alpha^s u$ we may carry out a similar induction over r yielding estimates for $\|\nabla D_\alpha^s u\|_2$, $\|\tilde{\Delta} D_\alpha^s u\|_2$, $\|D_\alpha^s u_t\|$,... and their higher time derivatives. We note that the necessary commutation of D_α^s and Δ in the equations gives rise to lower order terms with coefficients depending on boundary curvature. These terms can be accomodated without change in the integrability results; for reasons of space we omit details here.

7. Higher order normal derivatives. From the preceding stages we obtain the main integrability result for all space and time derivatives of normal order at most two in suitable local boundary coordinates. For derivatives of normal order three or more the result now follows inductively and in an elementary way from the incompressibility and vorticity relations. Thus $u_{i,i} = 0$ implies, if the boundary is $x_3 = 0$, that $D_3^3 u_3 = -D_3^2(D_1 u_1 + D_2 u_2)$, and similarly for higher normal derivatives of u_3 in a boundary coordinate neighbourhood.

The vorticity equations $\omega_{i,t} + u_k \omega_{i,k} = \omega_k u_{i,k} + \nu\Delta\omega_i$ are solved for the viscosity term so that, for example, $\nu\Delta\omega_2 = \nu\Delta(u_{3,1} - u_{1,3}) = \omega_{2,t} + u_k\omega_{2,k} - \omega_k u_{2,k}$. This yields a relation for $D_3^3 u_1$ in terms of normal derivatives of lower order; and similarly for $D_3^3 u_2$ and their higher normal derivatives.

To estimate the product terms we may note, for example, that $\max|u| \in L^1(0,T)$ while $\|\omega_{i,k}\|_2 \in L^{2/3}(0,T)$ so that $\|u_k\omega_{i,k}\|_2 \in L^{2/5}(0,T)$. In general the reciprocal index of the maximum of any derivative term exceeds that of its $L^2(0,T)$ norm by $\frac{3}{2}$. Hence all product terms in these estimates turn out to have the requisite index values.

After estimating $D_3^3 u_i, D_3^4 u_i, \cdots$ we may likewise estimate all mixed derivatives $D_3^{s_1} D_\alpha^{s_\alpha} u_i$, $(\alpha = 1,2)$ and higher time derivatives $D_t^r D_3^3 u_i, ... D_t^r D_1^{s_1} D_\alpha^{s_\alpha} u_i$, and so on. This will complete the induction proof on the indices r and $s = (s_1, s_2, s_3)$ for the norms $\|D_t^r D_x^s u\|_2$. The main result for the maximum norms follows from the $\frac{3}{2}$ allowance described above. Note that from the vorticity equations higher order space derivatives are calculated using higher time derivatives, in effect by a template with $2r + s$ constant.

8. Acknowledgement.

Thanks are due for support of this work through NSERC operating grant A3004.

References

1. S. Bergman and M. Schiffer, *Kernel functions and Elliptic Differential Equations in Mathematical Physics,* Academic Press, New York (1953), xiii + 432 pp.
2. L. Caffarelli, R. Kohn and L. Nirenberg, *Partial Regularity of suitable weak solutions of the Navier-Stokes equations.* Comm. Pure and Applied Math. 35 (1982), 771-831.
3. G.F.D. Duff, *L^2 estimates and integrals for solutions of the Navier-Stokes equations on a three-dimensional closed manifold,* Kyoto Math. J., to appear.
4. G.F.D. Duff and D. Naylor, *Differential Equations of Applied Mathematics,* Wiley, New York, (1966) xi + 423 pp.
5. C. Foias, C. Guillopé and R. Temam, *New a priori estimates for Navier-Stokes equations in dimension 3,* Comm. in P.D.E. 6(1981), 329-359.
6. J.G. Heywood, *The Navier-Stokes Equations - On the Existence, Regularity and Decay of Solutions,* Indiana Univ. Math. J. 29 (1980), 639-681.
7. O.A. Ladyzhenskaya, *The Mathematical Theory of Viscous Incompressible Flow,* Trans. New York, 2nd ed. (1969), xviii + 224 pp.
8. J. Leray, *Sur le mouvement d'un liquide visqueux emplissant l'espace.* Acta Mathematica 63 (1934), 193-248.
9. V. Scheffer, *The Navier-Stokes equations on a bounded domain,* Comm. Math. Phys. 73 (1980), 1-42.
10. V. Scheffer, *Boundary regularity for the Navier-Stokes equations in a half-space.* Commun. Math. Phys. 85 (1982), 275-299.
11. V. Scheffer, *A Solution to the Navier-Stokes Inequality with an Internal Singularity.* Commun. Math. Phys. 101 (1985), 47-85.

Department of Mathematics
University of Toronto
Toronto, Ontario
M5S 1A1

Received 31 July, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

THE DIFFEOMORPHISM GROUP OF THE IRRATIONAL ROTATION C*-ALGEBRA

George A. Elliott, F.R.S.C.

A complete description is given of the automorphisms of the smooth irrational rotation algebra, in the case that the rotation has generic Diophantine properties.

1. As pointed out by Brenken in [3], there is a natural homomorphism of the group of automorphisms of the irrational rotation C^*-algebra, A_θ, into $GL(2,Z)$, namely, the action on K_1. (By [12], $K_1(A_\theta) \cong Z^2$. A_θ denotes the C^*-algebra generated by unitaries u_1 and u_2 such that $u_2 u_1 = e^{2\pi i\theta} u_1 u_2$; by [9], A_θ is simple if θ is irrational.)

Brenken showed that the image of this homomorphism contains $SL(2, Z)$, and asked whether it is equal to $SL(2, Z)$. What he showed was that the homomorphism takes a certain canonical subgroup of $\mathrm{Aut}\, A_\theta$, consisting of the substitutions $u_i \mapsto u_1^{n_{1i}} u_2^{n_{2i}}$, $(n_{ij}) \in SL(2, Z)$, isomorphically onto $SL(2, Z)$. (A slightly different embedding of $SL(2, Z)$ in $\mathrm{Aut}\, A_\theta$ was described simultaneously by Watatani in [14].) It follows that, if the homomorphism can be shown to map $\mathrm{Aut}\, A_\theta$ into $SL(2, Z)$, then $\mathrm{Aut}\, A_\theta$ is the semidirect product of a closed normal subgroup by $SL(2, Z)$.

Brenken showed in [4] that certain interesting automorphisms of A_θ, for instance, those which fix the canonical generator u_1, do give rise to matrices with determinant $+1$.

In [8] and [5] it was shown that any diffeomorphism of A_θ gives rise to a matrix in $SL(2, Z)$. By a diffeomorphism of A_θ is meant an automorphism of the dense *-algebra A_θ^∞ of smooth elements of A_θ with respect to the canonical action of T^2. Since Brenken's (or Watatani's) copy of $SL(2, Z)$ in $\mathrm{Aut}\, A_\theta$ is contained in $\mathrm{Aut}\, A_\theta^\infty$, it follows that at least $\mathrm{Aut}\, A_\theta^\infty$ is the semidirect product of a normal subgroup by $SL(2, Z)$.

The purpose of the present note is to give a description of this normal subgroup, i.e., the kernel of the action of $\mathrm{Aut}\, A_\theta^\infty$ on $K_1(A_\theta^\infty)$, in the case that θ has generic Diophantine properties. By [2], this is the case that every derivation of A_θ^∞ is an inner perturbation of the canonical derivation corresponding to some one-parameter subgroup of T^2.

Denote by $U(A_\theta^\infty)$ the unitary group of A_θ^∞, and by $U(A_\theta^\infty)^0$ the connected component of the identity. Denote by $PU(A_\theta^\infty)^0$ the quotient of $U(A_\theta^\infty)^0$ by its centre (which is the scalar multiples of the identity, if θ is irrational). For the present purpose, let us take the group $PU(A_\theta^\infty)^0$ as a basic object, even though its structure could possibly be analysed further, in the way that the unitary group of a simple unital approximately finite-dimensional C^*-algebra was analysed in [10]. (Is it simple ?)

Denote by $T^2 \rtimes SL(2, Z)$ the semidirect product of $T^2 = R^2/Z^2$ by the canonical action of $SL(2, Z)$. It is immediate that the canonical action of T^2 on A_θ^∞ (by the substitutions $u_i \mapsto \lambda_i u_i$, $(\lambda_1, \lambda_2) \in T^2$) is compatible with Brenken's (or Watatani's) action of $SL(2, Z)$ on A_θ^∞, in the sense that these actions extend to an action of $T^2 \rtimes SL(2, Z)$ on A_θ^∞. In this way one obtains an action of $T^2 \rtimes SL(2, Z)$ on $PU(A_\theta^\infty)^0$.

Theorem. *If θ is irrational and has generic Diophantine properties, then*

$$\mathrm{Aut}\, A_\theta^\infty \cong PU(A_\theta^\infty)^0 \rtimes (T^2 \rtimes SL(2, Z)).$$

2. The proof of Theorem 1 is based on the following fact, which can be read off from the solution of the Yang-Mills problem for a finitely generated projective module over A_θ^∞ given by Connes and Rieffel in [7]. It is a simple reformulation of their result, in the special case that the module is A_θ^∞ itself. (It is also equivalent to any other single special case of their result.)

Theorem. *Let $\theta \in R$ be arbitrary, and let h_1 and h_2 be skew-symmetric elements of A_θ^∞ with canonical trace zero, such that the derivations*

$$\delta_1 + \mathrm{ad}\, h_1, \quad \delta_2 + \mathrm{ad}\, h_2$$

of A_θ^∞ commute. Here δ_1 and δ_2 denote the canonical derivations arising from the standard basis of the Lie algebra of T^2. There exists $u \in U(A_\theta^\infty)$, unique up to a scalar multiple, such that

$$h_1 = u^{-1}\, \delta_1(u), \quad h_2 = u^{-1}\, \delta_2(u).$$

Necessarily, $u \in U(A_\theta^\infty)^0$.

Proof. The existence of $v \in U(A_\theta^\infty)$ such that $h_i - v^{-1}\, \delta_i(v) \in C$ is a direct reformulation of Theorem 5.7 of [7], with $\Lambda = A_\theta^\infty$ (i.e. with Λ free of rank one and d equal to one).

This is seen as follows – of course we must use the language of [7] (and [6]). With A_θ^∞ considered as a right module over itself, the Grassmannian connection for δ is δ itself (since $\delta(1) = 0$). To avoid confusion, though, let us denote it by ∇. Since ∇_1 and ∇_2 (i.e. δ_1 and δ_2) commute, ∇ has curvature zero. If left multiplication by h_i is written just as h_i, then $\nabla + h$ is another connection for δ, the curvature of which is $\delta_1(h_2) - \delta_2(h_1) + [h_1, h_2]$. The condition that the derivations $\delta + \mathrm{ad}\, h_1$ and $\delta_2 + \mathrm{ad}\, h_2$ commute is just that $\delta_1(h_2) - \delta_2(h_1) + [h_1, h_2] = 0$. Thus, this condition, restated, is that also the connection $\nabla + h$ has curvature zero. Hence by Theorem 5.7 of [7], there exists a unitary endomorphism v such that $(\nabla + h) - v^{-1}\nabla v$ is constant. Since $v^{-1}\nabla v = \nabla + v^{-1}\delta(v)$, as follows from $[\nabla, v] = \delta(v)$, this says that $h - v^{-1}\delta(v)$ is constant, which means $h_i - v^{-1}\delta_i(v) \in \mathbf{C}$.

Now let us deduce the conclusion of the theorem. By [12], the classes of u_1 and u_2 generate $\mathrm{K}_1(A_\theta)$, so we may choose $n_1, n_2 \in \mathbf{Z}$ so that, with $w = u_1^{n_1} u_2^{n_2}$, the class of wv in $\mathrm{K}_1(A_\theta)$ is zero. Note that $w^{-1}\delta_i(w) \in \mathbf{C}$. Hence

$$(wv)^{-1}\delta(wv) = v^{-1}w^{-1}\delta(w)\,v + v^{-1}\delta(v) = w^{-1}\delta(w) + v^{-1}\delta(v),$$

and so also $h_i - (wv)^{-1}\delta_i(wv) \in \mathbf{C}$. Set $wv = u$. Since the class of u in $\mathrm{K}_1(A_\theta)$ is zero, by Theorem 2.1 of [13] (compare §4.4 of [1]) we have $\tau(u^{-1}\delta_i(u)) = 0$, where τ denotes the T^2-invariant trace on A_θ. Since $\tau(h_i) = 0$ by hypothesis, and $h_i - u^{-1}\delta_i(u) \in \mathbf{C}$, $h_i - u^{-1}\delta_i(u) = 0$ as desired.

To prove that u is unique up to a scalar multiple, note that from $u^{-1}\delta(u) = z^{-1}\delta(z)$ follows, successively, $(uz^{-1})^{-1}\delta(uz^{-1}) = 0$, $\delta(uz^{-1}) = 0$, $uz^{-1} \in \mathbf{C}$.

Finally, since the class of u in $\mathrm{K}_1(A_\theta)$ is zero, by Theorem 8.3 of [11] we have $u \in \mathrm{U}(A_\theta)^0$, and hence $u \in \mathrm{U}(A_\theta^\infty)^0$ (compare Theorem 2.1 of [13]).

3. **Proof of Theorem 1.** It remains to show that the kernel of the canonical homomorphism

$$\mathrm{Aut}\, A_\theta^\infty \to \mathrm{SL}(2, \mathbf{Z})$$

is isomorphic to $\mathrm{PU}(A_\theta^\infty)^0 \rtimes \mathrm{T}^2$. The canonical action of T^2 is easily seen to consist of outer automorphisms except for $\mathrm{Ad}\, u_1^{n_1} u_2^{n_2}$, $(n_1, n_2) \in \mathbf{Z}^2$. By 4.4 of [1] (an application of Theorem 2.1 of [13]), $u_1^{n_1} u_2^{n_2} \notin \mathrm{U}(A_\theta)^0$ if $(n_1, n_2) \neq (0, 0)$. Hence $\mathrm{Ad}(\mathrm{U}(A_\theta^\infty)^0)$ has trivial intersection with the action of T^2. The proof will be completed by showing that these two subgroups span the kernel.

Let α be an automorphism of the *-algebra A_θ^∞ acting trivially on $K_1(A_\theta^\infty)$. Let us show that the derivations $\alpha^{-1}\,\delta_1\,\alpha$ and $\alpha^{-1}\,\delta_2\,\alpha$ are equal to $\delta_1 + \operatorname{ad} h_1$ and $\delta_2 + \operatorname{ad} h_2$ with $h_i = -h_i^* \in A_\theta^\infty$. By the hypothesis on θ, at least we have

$$\alpha^{-1}\,\delta_i\,\alpha \;=\; \delta_i' + \operatorname{ad} h_i$$

with $h_i = -h_i^* \in A_\theta^\infty$, where δ_1', δ_2' are real linear combinations of δ_1 and δ_2 (see [2]). Since the functionals

$$\delta \mapsto \tau(u_i^{-1}\,\delta(u_i))$$

defined on derivations of A_θ^∞ are zero on inner derivations, separate linear combinations of δ_1 and δ_2, and are unchanged if u_1 and u_2 are replaced by other unitaries in the same K_1 classes (see [13], [1]) – in particular, by the unitaries $\alpha(u_1)$ and $\alpha(u_2)$ –, and since τ is unique and therefore invariant under α, we have

$$\begin{aligned}
\tau(u_i^{-1}\,\delta_j'(u_i)) &= \tau(u_i^{-1}(\alpha^{-1}\,\delta_j\,\alpha - \operatorname{ad} h_j)\,(u_i)) \\
&= \tau(u_i^{-1}(\alpha^{-1}\,\delta_j\,\alpha)\,(u_i)) \\
&= \tau(\alpha(u_i)^{-1}\,\delta_j(\alpha(u_i))) \\
&= \tau(u_i^{-1}\,\delta_j\,(u_i)),
\end{aligned}$$

and hence $\delta_j' = \delta_j$, as asserted.

Finally, after adding scalars to h_1 and h_2 so that $\tau(h_i) = 0$, we conclude by Theorem 2 applied to the commuting derivations $\alpha^{-1}\,\delta_i\,\alpha = \delta_i + \operatorname{ad} h_i$ that, for some $u \in U(A_\theta^\infty)^0$,

$$h_i \;=\; u^{-1}\,\delta_i(u).$$

Equivalently, as a short calculation shows,

$$\alpha^{-1}\,\delta_i\,\alpha \;=\; (\operatorname{Ad}u)^{-1}\,\delta_i\,(\operatorname{Ad}u).$$

In other words, the automorphism $\alpha(\operatorname{Ad}u)^{-1}$ commutes with δ_1 and δ_2, and it follows that $\alpha(\operatorname{Ad}u)^{-1}$ is the canonical automorphism corresponding to some element of $\mathbf{T}^2$. ($u_1^{n_1}\,u_2^{n_2}$ is an eigenvector for δ_j with eigenvalue $2\pi i n_j$.) This shows that α is the product of automorphisms belonging to $\operatorname{Ad}(U(A_\theta^\infty)^0)$ or to the canonical action of $\mathbf{T}^2$, as desired.

4. **Remark.** It is known that the only invertible elements of the subalgebra A_θ^F of finite linear combinations of monomials in u_1 and u_2 are the nonzero scalar multiples of these monomials. (Totally order the group $\mathbf{Z}^2$ and define the degree of an

element of A_θ^F to tbe highest pair of exponents $(n_1, n_2) \in \mathbf{Z}^2$ appearing.)

Hence immediately we have in this case, for any $\theta \in \mathbf{R}$, the following simpler analogue of Theorem 1:

$$\mathrm{Aut}\, A_\theta^F \cong \mathbf{T}^2 \rtimes SL(2, \mathbf{Z}).$$

Acknowledgements

The author's research has been supported by an operating grant from the Natural Sciences and Engineering Research Council of Canada and by a travel grant from the Danish Natural Science Foundation.

References

1. O. Bratteli, G. A. Elliott, and R. H. Herman, *On the possible temperatures of a dynamical system,* Comm. Math. Phys. 74 (1980), 281-295.

2. O. Bratteli, G. A. Elliott, and P. E. T. Jorgensen, *Decomposition of unbounded derivations into invariant and approximately inner parts,* J. Reine Angew. Math. 346 (1984), 166-193.

3. B. Brenken, *Representations and automorphisms of the irrational rotation algebra,* Pacific J. Math. 111 (1984), 257-282.

4. B. Brenken, *Approximately inner automorphisms of the irrational rotation algebra,* C. R. Math. Rep. Acad. Sci. Canada 7 (1985), 363-368.

5. B. Brenken, J. Cuntz, G. A. Elliott, and R. Nest, *On the classification of noncommutative tori, III,* Operator Algebras and Mathematical Physics (Editors, P. E. T. Jorgensen and P. S. Muhly), Contemporary Mathematics 60, Amer. Math. Soc., 1986, to appear.

6. A. Connes, C^*-algèbres et géométrie différentielle, C. R. Acad. Sci. Paris 290, Série A (1980), 599-604.

7. A. Connes and M. A. Rieffel, *Yang-Mills for non-commutative two-tori,* Operator Algebras and Mathematical Physics (Editors, P. E. T. Jorgensen and P. S. Muhly), Contemporary Mathematics 60, Amer. Math. Soc., 1986, to appear.

8. J. Cuntz, G. A. Elliott, F. M. Goodman, and P. E. T. Jorgensen, *On the classification of noncommutative tori, II,* C. R. Math. Rep. Acad. Sci. Canada 7 (1985), 189-194.

9. E. G. Effros and F. Hahn, *Locally compact transformation groups and* C^*-*algebras*, Mem. Amer. Math. Soc. 75 (1967), (ii) + 92 pages.

10. P. de la Harpe and G. Skandalis, *Sur la simplicité essentielle du groupe des inversibles et du groupe unitaire dans une* C^*-*algèbre simple*, J. Funct. Anal. 62 (1985), 354-378.

11. M. A. Rieffel, *Projective modules over higher-dimensional non-commutative tori*, preprint, January 1986.

12. M. V. Pimsner and D. Voiculescu, *Exact sequences for K-groups and Ext-groups of certain crossed product* C^*-*algebras*, J. Operator Theory 4 (1980), 93-118.

13. W. Pusz and S. L. Woronowicz, *Passive states and KMS states for general quantum systems*, Comm. Math. Phys. 58 (1978), 273-290.

14. Y. Watatani, *Toral automorphisms on irrational rotation algebras*, Math. Japonica 26 (1981), 479-484.

Department of Mathematics
University of Toronto
Toronto, Ontario
Canada, M5S 1A1

Mathematics Institute
Universitetsparken 5
2100 Copenhagen Ø
Denmark

Received 31 July, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

A CROSS-SPECTRAL METHOD FOR SENSITIVITY ANALYSIS OF COMPUTER SIMULATION MODELS

A. Feuerverger, D.L. McLeish and R. Rubinstein

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

ABSTRACT. Cross-spectral analysis of system performance variables with score function sequences leads to a practical solution of the problem of sensitivity analysis for computer simulation models.

1. INTRODUCTION. Consider a computer simulation model driven by an input sequence X_t and resulting in an output sequence Y_t where $t = 0, \pm 1, \pm 2, \cdots$. The input sequence X_t is taken as independent identically distributed from density $f_\nu(x)$ where ν is a multidimensional real parameter, and the output sequence Y_t will normally settle (as $t \to \infty$) into steady state and become a stationary and ergodic process. One or more sample performance measures of the form $L_t = L_t(Y_t)$ are evaluated and we are interested not only in the steady state mean $l(\nu) = \lim_{t\to\infty} E_\nu L_t$ but also in the sensitivities (gradient, Hessian, etc.) $\nabla_\nu l(\nu)$, $\nabla_\nu^2 l(\nu)$. Examples of relevant stochastic systems are queuing and reliability networks. In the first case L_t might be the sojourn time of the t-th customer, and $f_\nu(x)$ the multivariate density of interarrival times, service times and routing probabilities. In the second case L_t might be the life of a reliability system while $f_\nu(x)$ describes the component lifetimes. In such systems $l(\nu)$ is generally not analytically tractable so that we have to resort to Monte Carlo simulation. Normally the system cannot have knowledge of the future and we write

$Y_t = Y_t(X_t, X_{t-1}, \cdots)$ and $L_t = L_t(Y_t) = L_t(X_t, X_{t-1}, \cdots)$. In typical applications, system operation is started from some initial state and left to run until stationarity is attained. Thereafter T consecutive observations are taken and we denote these as $(X_1, L_1), (X_2, L_2), \ldots, (X_T, L_T)$. In this simulation the value of ν is set at ν_o and due to the complexity of the system, it is costly to repeat the simulation at other values of ν. The value of $l(\nu_o)$ may be estimated by $\frac{1}{T}\sum_{t=1}^{T} L_t$ whose variance, under general conditions, is $O(T^{-1})$. The purpose of this note is to present an effective method by which the sensitivities may be estimated simultaneously from the same simulation run. Some relevant references are Rubinstein (1986), Ho and Cao (1983). One contribution of our new method lies in the substantial reduction in the asymptotic order of the variance achieved relative to the score function method (Rubinstein, 1986), namely from $O(T)$ to $O(B_T^{-1}T^{-1})$ for $B_T \to 0$ such that $B_T T \to \infty$.

2. MAIN RESULT. For simplicity we take ν here to be univariate and assume the process L_t is stationary. Application of the result to vector valued parameters ν and to a vector of performance measures L_t requires only considering the sequences L_t and S_t appearing in the theorem to be jointly stationary vector valued time series. Hereafter the parameter ν will be assumed to be set equal to its value in the simulation ν_o wherever it appears. Our key result requires a mixing type condition consistent with the physical requirement that the simulation system settles eventually into a steady state suitable for statistical analysis. Specifically, let F_{-M}^{t} be the σ-field $F_{-M}^{t} = \sigma\{X_{-M}, X_{-M+1}, \ldots, X_t\}$. It follows from the martingale convergence theorem (e.g. Doob, 1953, p. 331, Theorem 4.3) that the approximation to the function L_t based on a finite data set $X_{-M}, X_{-M+1}, \cdots, X_t$, say, approxi-

mates L_t arbitrarily closely as $M \to \infty$. More precisely, if L_t is measurable with respect to $F_{-\infty}^{t}$ and is square integrable, then

$$E_\nu[L_t | F_{-M}^{t}] \to L_t \quad \text{as } M \to \infty \tag{2.1}$$

where the convergence in (2.1) holds both with probability 1 and in expectation since the martingale on the left hand side of (2.1) is uniformly integrable since it has a bounded sequence of second moments. Now if we are to be able to approximate the sensitivity $\frac{\partial}{\partial \nu} l(\nu)$ also using only a finite data set, then clearly it is necessary that the convergence in (2.1) occur for the expectation of the derivative with respect to ν as well, i.e. that

$$0 = E_\nu \frac{\partial}{\partial \nu} L_t = \lim_{M \to \infty} E_\nu \{ \frac{\partial}{\partial \nu} E_\nu [L_t | F_{-M}^{t}] \}. \tag{2.2}$$

Our main result is the following

THEOREM. Let $\{X_t, L_t\}$ be the stationary stochastic system described above. Let $S_t = \dfrac{\partial \log f_\nu(X_t)}{\partial \nu}$ and assume that S_t and L_t are square integrable and that the covariances $\mathrm{cov}_\nu(L_t, S_{t-j})$ are absolutely summable in j. Assume that (2.2) holds and also that the derivative may be passed through the integral in

$$\frac{\partial}{\partial \nu} \int E_\nu[L_t | F_{-M}^{t}] \prod_{i=-M}^{t} f_\nu(x_i) d\underline{x}$$

for each M. Then

$$\frac{\partial}{\partial \nu} l(\nu) = f_{L,S}(0) \tag{2.3}$$

where $f_{L,S}(\lambda)$ is the cross-spectral density function of the stationary sequence $\{L_t, S_t\}$. It follows that for any sequence $B_t \to 0$ such that $B_T T \to \infty$, an estimator will exist having bias $O(B_T^2)$ and variance $O(B_T^{-1} T^{-1})$.

PROOF. From (2.2)

$$\frac{\partial}{\partial\nu}\, l(\nu) \tag{2.4}$$

$$= \lim_{M\to\infty} \frac{\partial}{\partial\nu} E_\nu\{E_\nu(L_t\,|F^t_{-M})\} \tag{2.5}$$

$$= \lim_{M\to\infty} \int \frac{\partial}{\partial\nu} E_\nu\{L_t|F^t_{-M}\}\prod_{-M}^{t} f_\nu(x_i)\, d\underline{x} \;+\; \int E_\nu\{L_t|F^t_{-M}\}\frac{\partial}{\partial\nu}\prod_{-M}^{t} f_\nu(x_i)\, d\underline{x}$$

$$= \lim_{M\to\infty} E_\nu\{\frac{\partial}{\partial\nu} E_\nu[L_t|F^t_{-M}]\} + E_\nu(L_t\sum_{-M}^{t} S_i) \tag{2.6}$$

$$= \sum_{j=-\infty}^{t} \mathrm{cov}_\nu(L_t, S_j) \tag{2.7}$$

$$= f_{L,S}(0)\,. \quad \square \tag{2.8}$$

The proof shows that the limit in (2.2) must exist under the other conditions of the theorem; (2.2) is only required to insure that this limit is 0. Concerning estimation of $f_{L,S}(0)$, see Brillinger (1975), Jenkins and Watts (1969). In particular (Brillinger, 1975, chapter 7) for any sequence $B_T \to 0$ such that $B_T T \to \infty$ an estimator will generally exist having bias $O(B_T)$ and variance $O(B_T^{-1}T^{-1})$; for symmetric weight functions the bias will be $O(B_T^2)$. Variance reducing techniques which take into account the onesidedness of the $f_{L,S}(\lambda)$ Fourier series (e.g. Bhansali and Karavellas, 1983) and as in Heidelberger and Welch (1981) may also be applied. Further terms in the Taylor expansion of $l(\nu)$ may be obtained by means of cumulant spectra (Brillinger and Rosenblatt, 1967), e.g. $\frac{\partial^2}{\partial\nu^2}\, l(\nu) = f_{L,S,S}(0,0)$ where $f_{L,S,S}(\lambda_1, \lambda_2)$ is the cross-bispectrum.

Control variates may be used to achieve further variance reduction. Suppose that we can find some simple function $\hat{L}_t$, say, of the past observations, which approximates reasonably closely the performance measure L_t and whose expectation is analytically calculable and differentiable. For example, we might take $\hat{L}_t$ to be a linear combination of functions $g_\nu(X_i)$ such that $\frac{\partial}{\partial\nu}E_\nu g(X_i)$

can be calculated analytically; or simply

$$\hat{L}_t = c(\nu) + \sum_{i=0}^{\infty} d_i(\nu) X_{t-i} \tag{2.9}$$

for nonrandom regression coefficients $c(\nu)$ and $d_i(\nu)$; or in the case of a GI/G/1 queue with L_t the sojourn time of a customer, $\hat{L}_t$ might be a weighted average of the difference between the service times and the interarrival times of a few of the preceding customers in the system. Then

$$\frac{\partial}{\partial \nu} l(\nu) = \frac{\partial}{\partial \nu} E_\nu (L_t - \hat{L}_t) + \frac{\partial}{\partial \nu} E_\nu \hat{L}_t = E_\nu \{(L_t - \hat{L}_t) \sum_{j=0}^{\infty} S_{t-j}\} + \frac{\partial}{\partial \nu} E_\nu \hat{L}_t \tag{2.10}$$

Thus we may estimate the cross spectral density function between $L_t - \hat{L}_t$ and S_j rather than L_t and S_j, the advantage being that judicious choice of $\hat{L}_t$ may result in a cross spectral density function that is flatter near the origin (for example, a preliminary simulation may be used and L_t regressed on the preceeding X_j). We may then use a spectral density estimator with wide window without substantially increasing the bias of the estimator while reducing its variance significantly.

For a regenerative process, there is some random time τ such that L_t is independent of S_j; $j<t-\tau$. In this case $t-\tau$ is a regeneration time of the process. Then since $E(L_t S_{t-k}) = E(L_t S_{t-k} \mid k \leq \tau) \, P(k \leq \tau)$ we may estimate the cross-covariance using only terms L_t and S_j in the same regenerative cycle, further reducing the variance of the score function estimator to $O(T^{-1})$. Further details will be given elsewhere.

ACKNOWLEDGEMENTS. This research was supported by grants from the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

R.J. Bhansali and D. Karavellas, Wiener filtering, in Handbook of Statistics, Vol. 3, D.R. Brillinger and P.R. Krishnaiah, eds., 1-19, North Holland, Amsterdam, (1983).

D.R. Brillinger, Time Series: Data Analysis and Theory, Holt Rinehart and Winston, New York, (1975).

D.R. Brillinger and M. Rosenblatt, Asymptotic theory of estimates of K-th order spectra, in Advanced Seminar on Spectral Analysis of Time Series, Harris, B., Ed., 153-188, Wiley, New York, (1967).

J.L. Doob, Stochastic Processes, Wiley, New York, (1953).

P. Heidelberger and P.D. Welch, A Spectral Method for Confidence Interval Generation and Run Length Control in Simulations, Communications of the ACM, 24, (1981), 233-245.

Y.C. Ho and X. Cao, Perturbation Analysis and Optimization of Queuing Networks, Journal of Optimization Theory and Appl. 40, 4, (1983), 559-582.

G.M. Jenkins and D.G. Watts, Spectral Analysis and its Applications, Holden-Day, San Francisco, (1968).

R.Y. Rubinstein, Monte Carlo Optimization, Simulation and Sensitivity of Queuing Networks, Wiley, New York, (1986, in press).

Andrey Feuerverger
Department of Statistics
University of Toronto
Toronto, Ontario
Canada M5S 1A1

Don L. McLeish
Department of Statistics
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1

Reuven Rubinstein
Faculty of Industrial Engineering
and Management
The Technion
Haifa 32000
Israel

Received 6 August, 1986

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

Non-linear Operators and Ergodic Theory.

M.P. Heble and K. Sundaresan

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

We present here some ergodic theorems concerning a class of nonlinear operators in $L_p(\mu)$, $1 \le p < \infty$, known as composition operators. Let (X,Σ,μ) be a finite positive nonatomic measure space, and ϕ be a real valued function on $R \times X$ such that for $r \in R$, $\phi(r,\cdot)$ is a measurable function on X, and for t a.e. in X, $\phi(\cdot,t)$ is continuous on the real line. Further we assume $\phi(0,t) = 0$, t a.e. Such a function ϕ is called a Caratheodory function. Caratheodory functions determine nonlinear operators in $L_p(\mu)$ in a natural way. If ϕ is a Caratheodory function, it is verified that the function $\phi \circ f$ defined by $\phi \circ f(t) = \phi(f(t),t)$ is measurable if f is a measurable function. Further it is known that if $f \in L_p(\mu)$, then $\phi \circ f \in L_p(\mu)$, iff there exists a constant $b > 0$, and a function $c \in L_p(\mu)$, such that

(*) $$|\phi(r,t)| \le c(t) + b|r| \text{ for all } r \in R,$$

and for t a.e. in X. Thus if (*) holds the operator T defined by $Tf = \phi \circ f$ is a nonlinear operator in $L_p(\mu)$. The operator T acting on $L_p(\mu)$ into $L_p(\mu)$ is continuous, and maps bounded sets into bounded sets. Further the constant b in (*) may be chosen to be $\|T\| = \sup\{\|Tf\|_p \mid \|f\|_p \le 1\}$. We discuss here the individual and dominated ergodic theorems for a class of composition operators determined by Caratheodory functions ϕ, which are symmetric, nonnegative. Such a Caratheodory function ϕ is called convex (monotone increasing) if $\phi(\cdot,t)$ is convex (monotone increasing) on the positive half ray R^+.

The class of composition operators described above have been extensively studied in the literature, see Krasnosel'skii [3]. Our motivation for the study of the ergodic properties of this class of nonlinear operators arises out of the importance of this class of operators in the theory of nonlinear integral equations [3], on the one hand, and on the other hand, the importance of the individual and dominated ergodic theorems for linear contractions and isometries (cf. Akcoglu [1], A. Ionescu Tulcea [2]), in various branches of analysis.

For the rest of the discussion p is a fixed number, $1 \le p < \infty$. If ϕ is a Caratheodory function, then the sequence of functions $\{\phi^{(n)}\}_{n \ge 1}$, $\phi^{(1)} = \phi$, defined inductively by setting $\phi^{(n)}(r,t) = \phi(\phi^{(n-1)}(r,t),t)$, $n \ge 2$, are all Caratheodory functions.

In what follows as usual if $T : L_{p}(\mu) \to L_p(\mu)$ is a nonlinear operator we define the maximal operator T^* by $(T^*f)(t) = \sup_{n\geq 1}\left\{ \left| \frac{\sum_{i=0}^{n-1} T^i(f)(t)}{n} \right| \right\}$. The properties of a linear operator described in individual and dominated ergodic theorems, [2], are in a natural way extended to nonlinear operators.

Here we present the theorems providing sketches of proofs. The detailed proofs will be appearing elsewhere.

Theorem 1. If T is a composition in $L_p(\mu)$ determined by a monotonic increasing Caratheodory function ϕ then the individual ergodic theorem holds for T if $\|T\| < 1$.

Proof. Let $b = \|T\|$. As noted in the introduction there exists a function $c \in L_p(\mu)$, such that for t a.e. in X, and for all $r \in R$, $\phi(r,t) \leq c(t) + b|r|$. Let $f \in L_p(\mu)$, which without loss of generality may be assumed to be nonnegative, for the purpose of the proof here. Let $E_1 = \{t \mid \phi(f(t),t) \leq |f(t)|\}$, and $E_2 = \{t \mid \phi(f(t),t) > |f(t)|\}$. Then E_1, E_2 are disjoint measurable sets. From the properties of ϕ it is verified that

$$\frac{\sum_{i=0}^{n-1} T^i(f)}{n} = \frac{\sum_{i=0}^{n-1} T^i(f)\chi_{E_1}}{n} + \frac{\sum_{i=0}^{n-1} (T^i f)\chi_{E_2}}{n}.$$

Further it is shown that $\left\{ \sum_{i=0}^{n-1} \frac{(T^i f)(t)}{n} \right\}$ is decreasing bounded below by 0 (increasing bounded above by $\frac{c(t) + |f(t)|}{1-b}$) for $t \in E_1$ (for $t \in E_2$), completing the proof.

In general when $\|T\| = 1$, the conclusion in the preceding theorem is false, as shown by the following example.

Example 2. Let $X = [0,1]$, $\Sigma =$ the σ-algebra of Lebesgue measurable subsets of X, and μ be the restriction of Lebesgue measure to X. Let ϕ be the Caratheodory function defined by $\phi(r,t) = r^2$ if $0 \leq r \leq 1$, and $t \in X$, and $\phi(r,t) = (1 - 2t) + 2tr$, if $r \geq 1$, and $t \in X$. If T is the composition operator determined by ϕ, then T acts on $L_2(\mu)$ into $L_2(\mu)$. Further it is verified that $\|T\| = 1$. However when $f = 2\chi_{(1/2,1]}$, the means $\frac{\sum_{i=0}^{n-1} T^i(f)(t)}{n}$ fail to converge pointwise t a.e.

In the next proposition we consider the case $\|T\| > 1$, and ϕ is a convex Caratheodory function.

Proposition 3. If $T : L_p(\mu) \to L_p(\mu)$ is a composition operator determined by a convex Caratheodory function, and if $\|T\| > 1$, then the individual ergodic theorem does not hold for T.

Proof. The hypothesis implies that there are positive numbers a, and $\theta > 1$, and a measurable set F of positive measure such that for $t \in F$, $\phi(a,t) \geq \theta a$. Now the convexity of ϕ implies that, if $f = a\chi_F$, then $\dfrac{\sum_{i=0}^{n-1} T^i(f)(t)}{n}$ tends to ∞ as $n \to \infty$ for all $t \in F$.

Concerning the dominated ergodic theorem we have the following.

Theorem 4. If $T : L_p(\mu) \to L_p(\mu)$ is a composition determined by a convex Caratheodory function ϕ with $\|T\| < 1$, then the dominated ergodic theorem holds for T.

Proof. Using the inequality (*) with $b = \|T\|$, it is verified that for all $f \in L_p(\mu)$, with $\|f\| > 1$, $\|T^* f\| \leq \lambda \|f\|$, when $\lambda = \dfrac{1 + \|c\|}{(1-b)}$. Now appealing to the convexity of ϕ, it is shown that $\|T^* f\| \leq \lambda \|f\|$ for all $f \in L_p(\mu)$.

Remark. The preceding theorem does not extend to compositions determined by monotone increasing Caratheodory functions ϕ. For consider the measure space (X,Σ,μ) of example 2. Let ϕ be the caratheodary function $\phi(r,t) = \frac{1}{2} t r^{1/2}$, if $0 \leq r \leq 1$, and $t \in X$, and $\phi(r,t) = \frac{1}{2} t r$, if $r \geq 1$, and $t \in X$. Then it is verified that $\|T\| \leq \frac{1}{2}$, and if $F_r = [2r^{1/2}, 1]$, $0 < r < \dfrac{1}{4}$, then $\dfrac{\|T^*(r\chi_{F_r})\|}{\|r\chi_{F_r}\|} \to \infty$ as $r \to 0$. Hence T fails to satisfy the dominated ergodic property.

Finally we have the following characterization of compositions T in $L_p(\mu)$, determined by monotone increasing Caratheodory functions ϕ, for which the dominated ergodic theorem holds.

Theorem 5. Let $T : L_p(\mu) \to L_p(\mu)$ be a composition determined by a monotone increasing Caratheodory function ϕ. Then T has the dominated ergodic property iff the set of functions $\{e_r\}_{r \in R}$ is bounded in the Banach space $L_\infty(\mu)$, where for $r \in R$, $r \neq 0$, and $e_r(t) = \frac{1}{r} \lim_{n \to \infty} \phi^{(n)}(r,t)$, for $t \in X$.

The proof uses techniques similar to those involved in the proofs of Theorems 1 and 4.

References

(1) M.A. Akcoglu, *A pointwise ergodic theorem in* L_p spaces, Can. J. Maths. XXVII, 1075-1082.

(2) A. Ionescu Tulcea, *Ergodic properties of isometries in* L_p spaces, Bull. A.M.S. 70 (1964), 366-371.

(3) M.A. Krasnosel'skii, *Topological methods in the theory of nonlinear integral equations*, Macmillan, New York (1964).

Department of Mathematics
University of Toronto
Toronto, Canada M5S 1A1
and
Department of Mathematics
Cleveland State University
Cleveland, Ohio 44115, U.S.A.

Received 14 August, 1986

Mailing Addresses

1.	N.A. Alling	Department of Mathematics University of Rochester Rochester, NY 14627, U.S.A.
2.	G.F.D. Duff	Department of Mathematics University of Toronto Toronto, Ontario, Canada, M5S 1A1
3.	P. Ehrlich	Department of Philosophy Brown University Providence, RI 02912, U.S.A.
4.	G.A. Elliott	Mathematics Institute Universitetsparken 5 2100 Copenhagen Ø, Denmark
5.	A. Feuerverger	Department of Statistics University of Toronto Toronto, Ontario, Canada M5S 1A1
6.	M.P. Heble	Department of Mathematics University of Toronto Toronto, Ontario, Canada M5S 1A1
7.	Y. Hellegouarch	Départment de Mathématiques et de Mécanique Université de Caen 14032 Caen Cedex, France
8.	W. Herfort	Institute für Numerische und Angewandte Mathematik Technische Universität A-1040 Vienna, Austria
9.	D.L. McLeish	Department of Statistics University of Waterloo Waterloo, Ontario, Canada K2L 3G1
10.	A.J. Nicas	Department of Mathematics University of Toronto Toronto, Ontario, Canada M5S 1A1
11.	Zs. Páles	Department of Mathematics L. Kossuth University H-4010 Debrecen, Pf. 12, Hungary
12.	L. Ribes	Department of Mathematics and Statistics Carleton University Ottawa, Ontario, Canada K1S 5B6

13. R. Rubinstein — Faculty of Industrial Engineering and Management
The Technion
Haifa 32000, Israel

14. F. Shibata — Department of Applied Mathemtics
Okayama University of Science
Ridaicho, Okayama 700, Japan

15. T. Sugatani — Department of Mathematics
Toyama University
Gofuku, Toyama 930, Japan

16. K. Sundaresan — Department of Mathematics
Cleveland State University
Cleveland, OH 44115, U.S.A.

17. K. Yoshida — Department of Applied Mathematics
Okayama University of Science
Ridaicho, Okayama 700, Japan

18. J. Zaks — Department of Mathematics
University of Haifa
Mount Carmel, Haifa 31999, Israel

C.R. Math. Rep. Acad. Sci. Canada - Vol. VIII, No, 5, October 1986 octobre

THE STRUCTURE OF FREE PRODUCTS OF PRO-p-GROUPS

Wolfgang Herfort and Luis Ribes

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

1. THE RESULT

Let p be a fixed prime number, and let $A_1, A_2, \ldots, A_n$ be a finite number of pro-p-groups. Let $G = \coprod_{i=1}^{n} A_i$ be their free pro-p-product, i.e., their coproduct in the category of pro-p-groups. We are concerned here with a possible description of the closed subgroups H of G, along the lines of the Kurosh theorem for free products of abstract groups (cf. [6], for example). Our main result is the following:

Theorem Let H be a (topologically) finitely generated closed subgroup of G. Then $H = (\coprod_{i,j} A_i^{\alpha_{ij}} \cap H) \amalg F$, where F is a free pro-p-group, and for every i, α_{ij} runs through a complete set of double coset representatives of A_i and H in G.

The theorem is in fact more general than stated here: the number of factors A_i can be infinite, and their free product should then be understood in the appropriate manner (cf. [1], [3]).

If each of the free factors A_i is $\mathbb{Z}_p$ (the additive group of the ring of p-adic integers), then G is a free pro-p-group. In this case, our theorem reduces to a well-known result of Tate (cf. [2], or [7], Cor. 3, p. 1-37).

Our method of proof uses very heavily the fact that H is finitely generated, and we do not know whether the result is also valid for infinitely generated subgroups of G. An explicit mention of the problem we solve with our theorem can be found in Lubotzky [5].