

1 Feb/85	Memoir: Polytopes, Kaleidoscopes, Pythagoras and the future H.S.M. Coxeter F.R.S.C.	107
<hr/>		
5 July/84	On the operator equation $A_1 \times A_2 - B_1 \times B_2 = Q$ T. Masumdar	115
9 Aug/84	C^* algebras associated with Denjoy homeomorphisms of the circle I. F. Putnam	121
14 Nov/84	Universally integrally closed domains D. E. Dobbs	127
3 Dec/84	Le groupe des automorphismes du p-groupe de Sylow du groupe symétrique de degré p^n ; resultats P. Lentoudis	133
2 Jan/85	On the classification of noncommutative tori S. Disney, G.A. Elliot, A. Kumjian, I. Raeburn	137
2 Jan/85	Petits degrés de transcendance par la methode de Schneider en une variable M. Waldschmidt	143
2 Jan/85	Elliptic operators and realtive K-homology groups on manifolds with boundary K. Wojciechowski	149
8 Jan/85	On Pell numbers which are sums of not fewer than four squares N. Robbins	155
31st Jan/85	An easy proof for Schur's Inequality J. L. Levy	159
13 Feb/85	L'entropie topologique d'un groupe d'iteration J. Weitkämper	161
	Mailing Addresses	167

Memoirs - Mémoires

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

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

POLYTOPES, KALEIDOSCOPIES, PYTHAGORAS AND THE FUTURE

H.S.M. Coxeter

F.R.S.C.

In 1932, when I was a Rockefeller Foundation fellow at Princeton University, the celebrated Professor S. Lefschetz jokingly called me 'Mr. Polytope' because I had long been specially interested in the figures which he insisted were simply 'polyhedra' in space of any number of dimensions. The word *polytope* was coined in 1882 by Reinhold Hoppe and became established in Europe after the publication of P.H. Schoute's *Mehrdimensionale Geometrie, I (Die linearen Räume)* in 1902, *II (Die Polytope)* in 1905.

A *convex polytope* is simply defined as the convex hull of a finite set of points, and a *polytope* is, roughly speaking, any shape that shares the combinatorial properties of a convex polytope. However, my own interest has been restricted to highly symmetrical polytopes, such as the five platonic solids and their analogues in higher spaces. One remarkable feature of the symmetry groups of such polytopes is that they have presentations involving only a few,

easily remembered, relations. Another feature is that these groups are kaleidoscopic: generated by reflections. Although finite reflection groups had already been used by E. Cartan and H. Weyl in their investigation of simple Lie groups, my own contribution, during my visit to Princeton, was the complete enumeration of these kaleidoscopes in terms of a graphical notation in which each reflection (or mirror) is represented by a dot, and two dots are linked whenever the reflections do not commute (i.e., whenever the mirrors are not perpendicular). A link is marked q if the product of the two reflections is a rotation of period q (so that the angle between the mirrors is π/q), but for convenience the mark is omitted when $q = 3$ (the value that is found to arise most frequently). For further details, see my paper, *Groups whose fundamental regions are simplexes*, J. London Math. Soc. 6 (1931), 132-136, and my book, *Regular Polytopes* (first ed., Methuen, London, 1948; third ed., Dover, New York, 1973).

The graphical notation was adopted by Ernst Witt [*Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe*, Abh. Math. Sem. Hansisch. Univ. 14 (1941), 289-322] with the slight innovation of replacing a link marked 4 by a repeated link, so that the symmetry group of an ordinary cube is



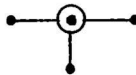
In 1946, the same symbols were used (with the same meaning) by E.B. Dynkin [*Classification of the simple Lie groups*, Rec. Math. (Mat. Sbornik) N.S. 18 (60), 347-352] and then they became widely known as *Dynkin graphs*.

Meanwhile, I saw that such a graph can be modified so as to provide a symbol for the polytope whose vertices are the images of a suitable point in the corresponding kaleidoscope. The idea is to insert a ring round the dots representing those mirrors on which the 'suitable point' does not lie. Thus the symbols



denote, respectively, the tetrahedron, octahedron, truncated tetrahedron, cuboctahedron and truncated octahedron; see my *Regular Complex Polytopes* (Cambridge University Press, 1974), pp. 18, 76.

The 4-dimensional regular polytope



is particularly interesting because its 24 vertices, with their coordinates expressed as quaternions, are the 24 unities in Adolf Hurwitz's arithmetic of *integral* quaternions.

The 6-dimensional uniform polytope



is interesting for a quite different reason. Its 27 vertices, like the 4 vertices of a square, are a *two-distance set*: any two of them belong either to an edge or to a diagonal, $\sqrt{2}$ times as long. P.H. Schoute observed in 1910 that this distinction between two distances resembles the behaviour of the 27 lines on the general cubic surface: any two of them are either skew or intersecting [*Convexity and its Applications*, ed. P.M. Gruber and J.M. Wills, Birkhäuser, Basel, 1983, pp. 111-119].

After 1952, when J.A. Todd and G.C. Shephard extended the theory of kaleidoscopes from Euclidean to unitary spaces, I realized that the graphical notation can be applied to *complex* kaleidoscopes by marking each dot with the period of the indicated reflection whenever this period is greater than 2. For dots representing reflections R and S , an unmarked link joining them now indicates the relation $RSR = SRS$, which is different from $(RS)^3 = 1$ when the period of the reflections exceeds 2. For instance,



is the group $SL(2,3)$ of order 24, and



is a complex 4-dimensional group of order 155,520 [see *Regular Complex Polytopes*, p. 134 and the frontispiece].

In 1979, the University of Toronto honoured me with the degree of LL.D. and asked me to deliver the Convocation Address. Believing that real and complex kaleidoscopes could scarcely appeal to the nonmathematicians in the audience, I decided to talk instead about more familiar topics. As far as I know, the Address was nowhere printed in 1979; but some of its ideas still seem timely.

Convocation Address

Chancellor Moore, President Ham, my distinguished colleagues and fellow graduates, ladies and gentlemen:

I am profoundly honoured by the University's decision to confer on me this degree, the culmination of many benefits that I have received. I thank you, Derick Atkinson, for your generous citation. My career in Toronto has been so pleasant that, despite various temptations to move back to England or to the States, I have always preferred

to remain in this University, with its stimulating opportunities for the interaction of teaching and research. I have been fortunate in that, nearly all my life, I have been paid to do what I would have done anyway. One especially happy period was when I occupied an office in the middle of the University College Tower, looking out over the main campus towards this Convocation Hall, so that I could see everything that was going on without leaving my desk at the window.

My research has often been aided by the excellent Library, in which the collection of mathematical periodicals, going right back to the beginning of the 19th century, was built up by Dean Alfred T. DeLury, whom I remember well.

To you young graduates, who are going out into the wide world to make your fortunes, I would say: Choose a career that you can really enjoy, even if it doesn't bring you material wealth. It is sad to see people doing jobs that bore them, just to make money. And try to influence your governments to make the world a happier place for everyone. There is so much misery and senseless violence that we sometimes seem to be witnessing a breakdown of morality reminiscent of the decline and fall of the Roman Empire.

I would urge you all to remember that *your* generation may have the opportunity to undo some of the mistakes perpetrated by *my* generation: for instance, to restore the forests devastated by the pulp and paper companies, and to stop their loathsome habit of discharging mercury into our rivers and lakes. I was recently watching Cousteau's dramatic film about the Mediterranean Sea. He first shows the teeming life below the surface, fifty years ago, looking just like the Great Barrier Reef. Then he contrasts this with a picture of the same spot at the present time: a desert of filth with no life at all.

Some weeks ago, when first I was asked to address Convocation, I thought I would be very daring and speak out against the further development of nuclear power. But then came the disaster at 3-mile Island and various revelations of scandalous cover-ups, so that now such sentiments are no longer daring but almost commonplace. More and more people have begun to agree with the World Council of Churches that nuclear reactors are too dangerous. Apart from the hazard of leaks and the problem of waste disposal, the proliferation of nuclear technology is a very real danger. Just think what might happen if it came to be understood by some such despot as Idi Amin! As Ralph Nader said, 'We have only two choices: give up nuclear energy now, or wait till a major disaster occurs and give it up then.'

I am inclined to feel that we should simplify our lifestyle, accept a lower standard of living. This might even improve our health. I think we should abandon nuclear power in favour of absolutely harmless sources of energy such as windmills, and machines based on the ocean waves. One of my colleagues has made progress towards harnessing the tides in the Bay of Fundy; and already many buildings are heated almost entirely by the sun. In fact, the so-called 'energy crisis' could be overcome by

conservation. We all eat too much, drink too much, smoke too much, drive too fast, and junk our old automobiles instead of recycling the steel that they are made of. As for the direct use of oil, it has been demonstrated in Australia that cars, slightly modified, will go well on a mixture of gasoline and methanol. In view of the prevalence of lung cancer, a double benefit could be achieved by gradually giving up tobacco and growing instead certain plants that would produce vegetable substitutes for gasoline.

I believe you should try to persuade the Russians and Japanese to abandon the barbarous practice of *whaling*. Some critics say that the Greenpeace people are too sentimental when they oppose also the slaughter of baby seals, this being no more cruel than the slaughter of cattle. But I think even that should be gradually phased out. In view of the impending world famine, we should face the fact that each acre of farm land can feed more people if its crops are used directly for humans instead of being fed to cattle. Moreover, cruelty to animals has psychological connections with cruelty to human beings.

According to a recent issue of the *New Oxford Review* [April 1978] a papyrus found near Cairo turned out to be a collection of essays by some contemporaries of Jesus. 'The common thread running through ... was their despair of an evil world and their withdrawal from it in quest of a purer, ideal existence.'

Those of you who decide *against* doing anything practical may like to follow the example of those ancient idealists and escape, as I have done, into a different world, such as the world of mathematics. In the words of the late Professor G.H. Hardy of Oxford and Cambridge, of whom a characteristic snapshot can be seen in our departmental library,

'A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas. ... The mathematician's patterns, like the painter's or the poet's, must be beautiful; the *ideas*, like the *colours* or the *words*, must fit together in a harmonious way. Beauty is the first test; there is no permanent place in the world for ugly mathematics.' [G.H. Hardy, *A Mathematician's Apology*, Cambridge, 1940, pp. 24-25.]

J.L. Synge, who was the professor of Applied Mathematics when I first came to Toronto, put it this way:

'The northern ocean is beautiful, and beautiful the delicate intricacy of the snowflake before it melts and perishes, but such beauties are as nothing to him who delights in *numbers*, spurning alike the wild irrationality of life and the baffling complexity of nature's laws.'

One who regarded numbers as his personal friends was the extraordinary Indian genius Ramanujan, whom Hardy introduced to his colleagues in England for a tantalizingly brief period of glory. Ramanujan professed to have obtained his theorems by direct inspiration from a goddess. Be that as it may, these theorems filled many note-

books which kept more orthodox mathematicians busy for some twenty years, gradually proving that they are correct. When he was dying of tuberculosis, his friend Hardy visited him and raised the question whether any numbers are uninteresting. 'Take for instance, the number of the taxi that brought me here', said Hardy, 'surely the number 1729 is completely dull'. 'Not at all', replied Ramanujan, 'It is the smallest number that can be expressed in two distinct ways as the sum of two cubes!'

You see, $1729 = 1728 + 1$; 1728 is $12 \times 12 \times 12$, the cube of 12, and 1 is the cube of 1; also one thousand is the cube of 10, and 729 is the cube of 9.

A still more elementary bit of arithmetic occurred to me some years ago when I opened the New English Bible at the fifth chapter of Genesis and read:

'Methuselah was 187 years old when he begot Lamech. ... He lived 969 years and then he died. Lamech was 182 years old when he begot a son. He named him Noah [Genesis 5: 25, 28]. ... The Lord said to Noah, "Go into the ark, you and all your household ... In *seven days*' time I will send rain over all the earth for forty days and forty nights, and I will wipe off the face of the earth every living thing that I have made" [Genesis 7: 1, 4, 5]. Noah ... was 600 years old when the waters of the flood came upon the earth. [Genesis 7: 6].

From the fact that $187 + 182 + 600 = 969$, I deduced that the year when Methuselah died was the same as the year of the deluge. Accordingly I wondered whether Noah had been so callous as to let his grandfather drown instead of pulling him into the ark. I wrote up this thought as a mini-paper for the *Mathematical Gazette* [55, June 1971, p. 312]. As a result, several letters came to the Editor. Of these, my favourite is the letter from Dr. Michael Shimshoni of the Weizmann Institute of Science in Rehovoth, Israel, who pointed out that my arithmetical observation had already been made 15 centuries ago in the Babylonian Talmud [Tract Sanhedrin, p. 108]. Concerning the 'seven days', the commentator Rashi wrote: 'These were the seven days of mourning for the righteous Methuselah. The Lord wished to honour him and delayed the punishment. Compute the years of Methuselah and you will find that they ended when Noah was six hundred years old.'

It thus becomes clear that Methuselah simply died of old age, and his grandson mourned him for seven days, before the rain began to fall. Dr. Shimshoni added the remark that many Jews still have seven days of great mourning for close relatives (the 'shiva').

Methuselah, like all his ancestors, must have been a vegetarian. For God had said to Adam [Genesis 1: 29], 'I give you all plants that bear seed ... and every tree bearing fruit ... they shall be yours for food.'

In this connection, I might mention the prophet Daniel and his three friends who later walked in the burning fiery furnace (so elegantly set to music by Benjamin Britten). Daniel asked their Babylonian guard, 'Give us only vegetables to eat and water to drink' [Daniel 1: 12].

Soon after that time another notable example was the mathematical philosopher Pythagoras, who was born in Samos (an island off the west coast of Turkey). While he was studying in Egypt, he was taken prisoner and spent twelve years in Babylon. He was released through the intercession of Democedes the royal physician. Thus after an absence of 34 years Pythagoras returned to his native Samos where his mother Phartenis was still waiting for him [Tons Brunés, *The Secrets of Ancient Geometry*, 1, Copenhagen 1987, p. 238]. She accompanied him to Crotona, in southern Italy, where he founded his famous school. Men and women came in great numbers to listen to him. One of the most attentive was Theano, the beautiful daughter of his host Milo. Pythagoras married her, although she was very young. We know that she wrote a biography of her husband, but unhappily it is lost [W.W.R. Ball, *A Short Account of the History of Mathematics*, Dover, New York, 1960, p. 20].

His greatest contribution to mathematics is the introduction of *rigour*: the notion that a theorem needs not only a *statement* but a logically developed *proof*. A famous instance is his proof that the square root of 2 is *irrational*, which means that it is not the ratio of two whole numbers, such as 5 over 3. He said, let us make the tentative assumption that $\sqrt{2} = a/b$: a fraction in its 'lowest terms' (such as 5/3, not 10/6). This would imply $a^2/b^2 = 2$, or $a^2 = 2b^2$, which shows that a^2 is even. Since the square of an odd number is odd, this implies that a *itself is even*, say $a = 2c$. From $a^2 = 2b^2$ and $a = 2c$, we easily deduce $b^2 = 2c^2$. By the same reasoning again, this implies that b *is even*. Thus a and b are *both even*, contradicting our tentative assumption that the fraction a/b is in its lowest terms. Therefore our tentative assumption must be wrong: $\sqrt{2}$ cannot be expressed as a fraction a/b .

This proof amply satisfies Hardy's criterion for beauty: it combines a very high degree of *unexpectedness* with *inevitability* and *economy*. It is just as fresh and significant today as when Pythagoras first thought of it, 25 centuries ago.

His interest in *ratio* led naturally to an interest in *music*. Still today, both music and mathematics help to unite the various races of mankind; for both are written in a universal notation, the same for the Japanese, Russians, Arabs and ourselves.

Unhappily, Pythagoras's most devoted followers, the 'Pythagoreans', made the foolish decision to become a secret society, careful not to reveal their knowledge to outsiders. Eventually the ordinary people became so enraged that they murdered him and many of his disciples. Thus the Red Brigades of present-day Italy had their counterparts in 500 B.C.

No talk by a professor would be complete without a story about absent-mindedness, such as the one about the man who met a friend and said 'I can't quite remember, was it *you* who died, or your brother?'

Among the authentic instances, I like best the story told against himself by my Dutch friend the late Salomon van Oss. This is more-or-less the way he told it. (Remember that in Europe a street-car is called a 'tram'.)

'One day I was getting into a tram. A glass window happened to show a reflected image of myself. I said, "Oh, I am already in." So I got out.'

For telling this story I must apologize to Rien, my wife, who has already heard it *ad nauseam*.

In closing, I would express to her my profound gratitude for watching over me with loving care throughout most of my life, tolerating my peculiarities and encouraging all my best efforts. Sometimes I have gone against her advice and been sorry; more often I have followed her advice and been glad.

The best that I can wish for each of you is that you may have as full and happy a life as I have had and am still having.

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

ON THE OPERATOR EQUATION $A_1XA_2 - B_1XB_2 = Q$

Tapas Mazumdar

Presented by P.G. Rooney, F.R.S.C.

ABSTRACT. An analytic treatment of the existence and uniqueness of the solution X of $A_1XA_2 - B_1XB_2 = Q$ is given in a Hilbert space setting, where the linear operators A_1, A_2, B_1, B_2, Q may all be unbounded.

1. We will give an analytical treatment of the existence and uniqueness of the solution X of the equation, $A_1XA_2 - B_1XB_2 = Q$, in a Hilbert space setting. (Compare [1, 2, 3] for other analytic approaches). To describe our problem precisely, let H be a complex Hilbert space with inner product $(\cdot, \cdot)_H$ and norm $|\cdot|_H$. $V^1 \subset H$ is a complex normed linear space, and $A_1, B_1 \in L(V^1, H)$. A_2, B_2 are linear maps: $V^2 \rightarrow V^2$ where V^2 is a complex pre-Hilbert space. For $i = 1, 2$, the norm in V^i is denoted by $|\cdot|_i$.

Let $\omega = L(V^2, V^1)$ and $\mathfrak{X} = L(V^2, H)$, with their respective norm topologies. Of concern is the problem of existence of a unique solution $X = X_Q \in \omega$ or \mathfrak{X} of the equation

$$(A_1XA_2 - B_1XB_2)\phi = Q\phi \quad \forall \quad \phi \in V^2, \quad \dots \quad (1)$$

for a given $Q \in \mathfrak{X}$; we will present sufficient conditions, and our method of approach will be valid whether A_1, A_2, B_1, B_2 and Q are bounded or unbounded linear operators in H . In what follows $\|Q\|$ will denote the norm of Q in \mathfrak{X} , and \mathbb{N} will denote the set of natural numbers, $1, 2, 3, \dots$.

As an accessory to proving the main result appearing in the next section, we present the following theorem (which may be recast in a familiar

algebraic format using the concepts of Kronecker or direct product and diagonal dominance of matrices, cf. [2]).

Theorem 1. Assume that H, V^1, V^2 are all finite-dimensional spaces with $V^1 = H$ (set equality). Also assume that the one-sided coercivity property holds, i.e. \exists a constant $\beta > 0$ such that \forall nonzero $X \in \omega, \exists$ a $\phi_X \in V^2$ such that $|(A_1 X A_2 - B_1 X B_2)\phi|_H > \beta \|X\|_\omega \|\phi_X\|_2$. Then, (1) has a unique solution $X_Q \in \omega$ with $\|X_Q\|_\omega \leq \beta^{-1} \|Q\|$.

Proof. Since $\dim V^2 < \infty$, we will have $A_2, B_2 \in L(V^2, V^2)$. Then we can define a linear map $U: \omega \rightarrow \mathfrak{X}$ by $(U(X))\phi = (A_1 X A_2 - B_1 X B_2)\phi$. By the coercivity property it follows that $\|U(X)\|_{\mathfrak{X}} > \beta \|X\|_\omega$ for all nonzero X . Hence, U is a bijection, with $\|U^{-1}\| \leq \beta^{-1}$. $X_Q = U^{-1}(Q)$ completes the existence proof. The uniqueness readily follows from the coercivity assumption. Q.E.D.

2. Henceforth, H, V^1, V^2 will all be infinite-dimensional. We will make the transition from the finite dimensional result of Theorem 1 to infinite dimensions by assuming that V^2 is generated by an orthonormal basis $\{b_i | i \in \mathbb{N}\}$ formed of eigenvectors of both A_2 and B_2 ; $A_2 b_i = \lambda_i b_i$ and $B_2 b_i = \mu_i b_i \forall i \in \mathbb{N}$. This implies commutativity of A_2, B_2 , as is assumed in [3]. However, unlike [3], we do not assume commutativity of A_1, B_1 . The subspaces of V^2 and H generated by $\{b_i | 1 \leq i \leq n\}$ and $\{Qb_i | 1 \leq i \leq n\}$ are respectively denoted by V_n^2 and $[Qb_i]_{i=1}^n$.

We next assume that \exists a subsequence N' of N such that $\forall n \in N' \exists$ a finite dimensional subspace $V^1(n)$ of V^1 containing $A_1[V^1(n)]$, $B_1[V^1(n)]$ and $[Qb_i]_{i=1}^n$. Since $\dim(V^1(n)) < \infty$, \exists a constant $c(n) > 0$ such that $|v|_1 \leq c(n)|v|_H \quad \forall v \in V^1(n)$. Considered as a subspace of H , $V^1(n)$ will be denoted by $H(n)$. For all $n \in N'$, let $\omega(n) = \{X \text{ restricted to } V_n^2 \mid X \in \omega, Xb_i = 0 \quad \forall i > n, Xb_i \in V^1(n) \quad \forall i \leq n\}$ with its norm topology. Also, $\forall n \in N'$, we define $A_{1,n}, B_{1,n} \in L(V^1(n), H(n))$, $A_{2,n}, B_{2,n} \in L(V_n^2, V_n^2)$ and $Q_n \in L(V_n^2, H(n))$ as the restrictions of the operators A_1, B_1, A_2, B_2 and Q respectively. We clearly have $A_{2,n}[V_n^2] \subset V_n^2$. In the rest of the paper these notations and assumptions will remain implicit; only convenience will dictate any explicit mention of them.

We now have an easy consequence of Theorem 1.

Lemma 2. In addition to the assumptions made so far in this section, also assume that

$$\left. \begin{array}{l} \forall n \in N', \exists \text{ a constant } \beta_n > 0 \text{ such that } \forall \text{ nonzero} \\ Y \in \omega(n), \exists \text{ a } \phi_Y \in V_n^2 \text{ satisfying:} \\ | (A_1YA_2 - B_1YB_2)\phi_Y |_H > \beta_n \| Y \|_{\omega(n)} |\phi_Y|_2. \end{array} \right\} \dots \dots (2)$$

Then, $\forall n \in N', \exists$ a unique $Y_n \in \omega(n)$ such that

$$(A_{1,n}Y_nA_{2,n} - B_{1,n}Y_nB_{2,n})\phi = Q_n\phi \quad \forall \phi \in V_n^2. \quad \square \dots \dots (3)$$

Now we are ready to present our main result.

Theorem 3. Assume the spectral condition that $\forall i \in N$, the linear operator $\lambda_i A_i - \mu_i B_i: H \rightarrow H$ has a continuous inverse T_i defined on its image, with norm $\|T_i\|$. Also assume that (i) $\sum_{i=1}^{\infty} \|T_i\|^2 = M_2^2 < \infty$, or (ii)

\exists positive numbers p , $(\gamma_i)_{i=1}^{\infty}$ with $p > 1$ such that $\sum_{i=1}^{\infty} [\gamma_i \|T_i\|]^p = M_p^p < \infty$ and $\sum_{i=1}^{\infty} [\gamma_i^{-1} |Qb_i|_H]^q = M_q^q < \infty$. Then (2) is true, and \exists a unique solution $X_Q \in X$ of (1) provided the ϕ 's are restricted to only finite dimensional elements of V^2 . If, in addition, V^2 is dense in H , $A_1: H \rightarrow H$ is closable with closure \bar{A}_1 , and $B_1 \in L(H, H)$, then this X_Q uniquely satisfies:

$$(\bar{A}_1 X_Q A_2 - B_1 X_Q B_2)\phi = Q\phi \quad \forall \quad \phi \in V^2. \quad \dots \quad (4)$$

Proof. The uniqueness part is easy. If X_Q, Y_Q are two solutions of (1), then, because each b_i is an eigenvector of A_2 and B_2 we obtain from (1) by replacing ϕ by b_i : $(\lambda_i A_1 - \mu_i B_1)(X_Q - Y_Q)b_i = 0$. Operating by T_i we have, $(X_Q - Y_Q)b_i = 0 \quad \forall \quad i \in \mathbb{N}$. Hence, $X_Q = Y_Q$.

The various steps in the long existence proof may be briefly described as follows (the details will appear elsewhere):

First, (2) is proved by contradiction. If we deny its validity for an $m \in \mathbb{N}'$, then \exists a sequence $(Y_i)_{i=1}^{\infty}$ of nonzero elements of $\omega(m)$ such that $\forall i \in \mathbb{N}$, $|(A_1 Y_i A_2 - B_1 Y_i B_2)\phi|_H \leq 2^{-i} \|Y_i\|_{\omega(m)} |\phi|_2 \quad \forall \phi \in V_m^2$. Replace ϕ in turn by b_j for all $j \leq m$ and use the results to show that if $v \in V_m^2$ is arbitrary with $|v|_2 = 1$, then we get $|Y_i v|_1 \leq 2^{-i} c(m) \|Y_i\|_{\omega(m)} \sum_{j=1}^{\infty} \|T_j\|$. Choosing i judiciously according as condition (i) or condition (ii) in the theorem holds, we arrive at the contradiction, $\|Y_i\|_{\omega(m)} \leq \frac{1}{2} \|Y_i\|_{\omega(m)}$. This proves (2).

Now consider the unique solutions Y_p, Y_q , given by Lemma 2, for every pair p, q of consecutive elements of \mathbb{N}' , with $p < q$. Consider (3) for $n = q$ and $n = p$ in turn. Put b_i for ϕ , $\forall i \leq p$, subtract and simplify.

to yield $Y_{p,q} b_i = Y_p b_i \quad \forall i \leq p$. This allows us to define an ascending sequence $\{X_p\}_{p \in \mathbb{N}^+}$ of elements of \mathcal{W} by $X_p b_i = Y_p b_i \quad \forall i \leq p$, and $X_p b_i = 0 \quad \forall i > p$. Then X_p satisfies (1) whenever $\phi \in V_p^2$. Moreover, if $\phi = \sum_{i=1}^{\infty} \alpha_i b_i \in V^2 \quad (\alpha_i \in \mathbb{C})$, then $X_p \phi = \sum_{i=1}^p \alpha_i T_i Q_p b_i$.

In the next part of the proof it is shown that the sequence $\{X_p\}_{p \in \mathbb{N}^+}$ converges to some $X_Q \in \tilde{\mathcal{X}} = L(\tilde{V}^2, H)$ in the weak operator topology of $\tilde{\mathcal{X}}$, where \tilde{V}^2 is the completion of V^2 . This is done by showing that $\forall \phi \in \tilde{V}^2$ and $\forall h \in H$, the sequence $\{(X_p \phi, h)_H\}_{p \in \mathbb{N}^+}$ is Cauchy in \mathbb{C} . Here, of course, we utilize conditions (i) or (ii), as the case may be. We actually obtain $\lim_{p \rightarrow \infty} (X_p \phi, h)_H = (X_Q \phi, h)_H$.

The last part of the proof consists of showing that this X_Q is indeed the solution sought.

3. Here we outline an example. Let $H = L^2([0, 2\pi] \times [0, 2\pi]; \mathbb{C})$. An orthonormal basis for H is $\{e_{i,j}\}_{i,j=0}^{\infty}$ where $e_{i,j}(x,y) = e_i(x) e_j(y)$, $e_0(\xi) = (2\pi)^{-\frac{1}{2}}$, $e_{2n-1}(\xi) = \pi^{-\frac{1}{2}} \sin n\xi$, $e_{2n}(\xi) = \pi^{-\frac{1}{2}} \cos n\xi$. With appropriate constants $\gamma_{p,q}$, we may define $b_{p,q} = \gamma_{p,q} e_{p,q}$ such that $\{b_{p,q}\}_{p,q=0}^{\infty}$ forms an orthonormal set in the Sobolev space H^3 . Let V^2 be the subspace of H^3 formed of all finite linear combinations over \mathbb{C} of the $b_{p,q}$'s. With $V^1 = H_0^2$, we define the various operators by

$$A_1 u = -a \partial_x^2 u + k_1 u, \quad B_1 u = -b \partial_y^2 u,$$

$$A_2 \phi = (\partial_x^2 + \partial_y^2) \phi - \frac{1}{2} \phi, \quad B_2 \phi = (\partial_x^4 + \partial_y^4) \phi + k_2 \phi,$$

where a, k_1, b, k_2 are positive constants. For Q we may take the one

defined by $Q(b_{p,q}) = (\text{const.}) \partial_y^2 b_{p,q}$ if p and q are both odd, and $Q(b_{p,q}) = 0$ otherwise. Here $\partial_x^2 u = (\partial^2 u)/(\partial x^2)$, all the derivatives being taken in the distributional sense.

It can be shown that all conditions to apply Theorem 3 are satisfied, and that equation (1) has a unique solution.

REFERENCES

1. P. Lancaster, Explicit solutions of linear matrix equations, *SIAM Review* 12 (1970), pp. 544-566.
2. P. Lancaster, "Theory of Matrices", Academic Press, New York, 1969.
3. G. Lumer and M. Rosenblum, Linear operator equations, *Proc. Amer. Math. Soc.* (1959), pp. 32-41.

Department of Mathematics and Statistics
Wright State University
Dayton, Ohio 45435

Received July 5, 1984

C*-ALGEBRAS ASSOCIATED WITH DENJOY HOMEOMORPHISMS OF THE CIRCLE

Ian F. Putnam

Presented by D.E. Handleman, F.R.S.C.

A homeomorphism of the circle without periodic points generates a free action of the integers on the circle. We consider the cross-product or transformation group C*-algebras associated with such actions. These homeomorphisms fall into two classes: rotations through an angle which is an irrational multiple of 2π , and the so-called Denjoy homeomorphisms. The irrational rotation C*-algebras have been studied in [6], [7] and [8]. Here, we investigate the general structure of the Denjoy C*-algebras and extend certain results about the irrational rotation C*-algebras to the Denjoy case.

We let \mathbb{R} denote the real numbers, S^1 , the circle, and $\pi: \mathbb{R} \rightarrow S^1$, the usual covering map. We use R_α to denote rotation through an angle of $2\pi\alpha$, that is, $R_\alpha(\pi(x)) = \pi(x + \alpha)$, for any $x \in \mathbb{R}$. We will use ϕ and ψ to denote homeomorphisms of the circle without periodic points, that is, for any $p \in S^1$, $\phi^n(p) = p$ only if $n = 0$.

From [3] and [4], we have the following dynamical information regarding ϕ :

- (a) $\rho(\phi)$, an irrational number between 0 and 1, called the rotation number of ϕ
- (b) an order-preserving, continuous function $h: S^1 \rightarrow S^1$ such that $h \circ \phi = R_{\rho(\phi)} \circ h$, called the semi-conjugacy for ϕ .
- (c) a unique minimal non-empty, closed, ϕ -invariant set $\Sigma \subseteq S^1$, and its complement Y , a maximal open, ϕ -invariant, proper subset of S^1 .
- (d) a unique ϕ -invariant probability measure μ on S^1 , given by $\mu(E) = \lambda(h(E))$, where $E \subseteq S^1$ is any Borel set, and λ is normalized

Lebesgue measure on S^1 . Moreover, $\text{supp}(\mu) = \Sigma$.

- (e) $Q(\phi) = h(Y)$, with h as in (b) and Y as in (c). This defines $Q(\phi)$ up to rotation. It is countable and $R_{\rho(\phi)}$ -invariant. (The $T(\phi)$ defined in [4] is exactly the compliment of our $Q(\phi)$. Our definition will be much more convenient later on.)
- (f) $n(\phi)$, the number of disjoint $R_{\rho(\phi)}$ -orbits in $Q(\phi)$. The possible values of $n(\phi)$ are 0 (if $Q(\phi)$ is empty), 1, 2, ..., and \aleph_0 .

It was shown in [4] that $\rho(\phi)$ and $Q(\phi)$ characterize ϕ . For our purposes, it will be more useful to state the result in terms of transformation groups. We let (\mathbb{Z}, S^1, ϕ) denote the action generated by ϕ of the integers on the circle. The condition that ϕ have no periodic points means that this action is free.

In general, we say that two transformation groups, (G_1, X_1) and (G_2, X_2) are isomorphic if there is an isomorphism of topological groups $\xi: G_1 \rightarrow G_2$, and a homeomorphism $\eta: X_1 \rightarrow X_2$, such that, for $x \in X_1$ and $g \in G_1$, $\eta(g \cdot x) = \xi(g) \cdot \eta(x)$.

The results of [4] give us:

Theorem 1 Two free actions (\mathbb{Z}, S^1, ϕ) and (\mathbb{Z}, S^1, ψ) are isomorphic if and only if (i) $\rho(\phi) = \rho(\psi)$ or $\rho(\phi) = 1 - \rho(\psi)$, and (ii) $Q(\phi) \equiv Q(\psi)$ or $Q(\phi) \equiv -Q(\psi)$, where \equiv denotes equality up to rotation, and $-Q(\psi) = \{ \pi(-x) \mid \pi(x) \in Q(\psi) \}$.

We will denote by A_ϕ the transformation group C^* -algebra $C^*(\mathbb{Z}, S^1, \phi)$, which is also the cross-product C^* -algebra $C(S^1) \rtimes_{\phi} \mathbb{Z}$ (see [5]). Note that we also use ϕ to denote the automorphism of $C(S^1)$ induced by ϕ .

The existence of the unique ϕ -invariant probability measure on S^1 gives a unique normalized trace, denoted Tr , on A_ϕ (see [2]).

In [7], Rieffel showed explicitly the existence of non-trivial projections in the irrational rotation C^* -algebras, and computed their traces. The construction can be modified easily to any ϕ without periodic points, and the traces of these can be calculated. The results of [6] allow us to compute $K_0(A_\phi)$ as a group. Together, these results give us:

Theorem 2 $\text{Tr}_* : K_0(A_\phi) \rightarrow \mathbb{Z} + \rho(\phi)\mathbb{Z}$ is an isomorphism of ordered groups.

From [2], A_ϕ is simple if and only if ϕ is topologically ergodic, that is $\Sigma = S^1$. This is true if and only if ϕ is (topologically) an irrational rotation. This, in turn, is true if and only if $Q(\phi)$ is empty.

We now turn to the other case. Since such ϕ are referred to as Denjoy homeomorphisms, it seems reasonable to call the A_ϕ Denjoy C^* -algebras.

In this case, Σ is a Cantor set, and the maximal open, ϕ -invariant set Y gives a maximal ideal, denoted \mathcal{I} , in A_ϕ . The action of ϕ when restricted to Y , is very simple and so we can describe \mathcal{I} very concretely:

Theorem 3 (i) $\mathcal{I} = \{ x \in A \mid \text{Tr}(x^*x) = 0 \}$
 (ii) $\mathcal{I} \cong \bigoplus_{k=1}^{n(\phi)} C_0(I_k) \otimes \mathcal{K}(\mathcal{L}^2(\mathbb{Z}))$, where \mathcal{K} is the C^* -algebra of compact operators, and $I_k \subseteq S^1$ is an open interval, for each $k = 1, 2, \dots, n(\phi)$.

We denote by D_ϕ the C^* -algebra $C(\Sigma) \rtimes_\phi \mathbb{Z}$, obtained by restricting ϕ to Σ . The algebra D_ϕ is simple, since Σ is minimal. We have the short exact sequence: $0 \rightarrow \mathcal{I} \rightarrow A_\phi \rightarrow D_\phi \rightarrow 0$.

Since $\text{supp}(\mu) = \Sigma$, D_ϕ has a unique, faithful, normalized trace, also denoted Tr . Using the six-term exact sequence for K -groups obtained from the short exact sequence above, and the $*$ -isomorphism of part (ii) of Theorem 3, the set $Q(\phi)$ appears as the trace of certain elements of $K_0(D_\phi)$.

From this and Theorems 1 and 2, we obtain the following result, already known for the irrational rotation case:

Theorem 4 Two free actions (\mathbb{Z}, S^1, ϕ) and (\mathbb{Z}, S^1, ψ) are isomorphic as transformation groups if and only if A_ϕ and A_ψ are $*$ -isomorphic.

In [8], Rieffel investigated the question of strong Morita equivalence for the irrational rotation C^* -algebras. While many of the results there are valid only for rigid motions (i.e. rotations), we are able to generalize the characterization of strong Morita equivalence, as follows:

Theorem 5 Let Φ and Ψ be homeomorphisms of the circle without periodic points. Then the C^* -algebras A_Φ and A_Ψ are strongly Morita equivalent if and only if there is $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $GL(2, \mathbb{Z})$ such that

(i) $\rho(\Psi) = \left\{ \frac{a \rho(\Phi) + b}{c \rho(\Phi) + d} \right\}$, where $\{ \cdot \}$ denotes fractional part, and

(ii) $\pi^{-1}(Q(\Psi)) \equiv \frac{1}{c \rho(\Phi) + d} \pi^{-1}(Q(\Phi))$, where \equiv denotes equality up to translation.

- Remarks
1. The semiconjugacy h defines an embedding $h^*: A_{R, \rho(\phi)} \rightarrow A_\psi$. The image of $A_{R, \rho(\phi)}$ has trivial intersection with ideal \mathcal{I} , so we also have an embedding $q \circ h^*: A_{R, \rho(\phi)} \rightarrow D_\psi$.
 2. In the case $n(\phi) = 1$, the algebra D_ϕ is similar to the C^* -algebra constructed by Cuntz in Remark 2.5 of [1].
 3. Both the Kasparov group $\text{Ext} \left(D_\phi, \bigoplus_{k=1}^{n(\phi)} C_0(I_k) \right)$ and the element of this group determined by $0 \rightarrow \mathcal{I} \rightarrow A_\psi \rightarrow D_\phi \rightarrow 0$, can be computed using the universal coefficient theorem. We also have methods of realizing the extension classes in more concrete terms, which we intend to include in the complete

publication of this material.

I would like to thank Marc Rieffel, under whose invaluable supervision this work was done. I would also like to thank Charles Pugh for many helpful conversations regarding homeomorphisms of the circle.

REFERENCES

1. J. Cuntz, K-theory for certain C^* -algebras. II, *J. Operator Theory*, 5, (1981), 101-108.
2. E.G. Effros and H. Hahn, Locally compact transformation groups and C^* -algebras, *Mem. Amer. Math. Soc.*, 75 (1967).
3. Y. Katznelson, Sigma-finite invariant measures for smooth mappings of the circle, *J. Anal. Math.*, 31 (1977), 1-18.
4. N.G. Markley, Homeomorphisms of the circle without periodic points, *Proc. Lon. Math. Soc.*, (3) 20 (1970), 688-698.
5. G.K. Pedersen, C^* -algebras and their automorphism groups, Academic Press, 1979.
6. M. Pimsner and D. Voiculescu, Exact sequences for K-groups and Ext-groups of certain cross-product C^* -algebras, *J. Operator Theory*, 4 (1980), 93-118.
7. M.A. Rieffel, C^* -algebras associated with irrational rotations, *Pac. J. Math.*, 93 (1981), 415-429.
8. M.A. Rieffel, The cancellation theorem for projective modules over irrational rotation C^* -algebras, *Proc. Lon. Math. Soc.*, (3), 47 (1983), 285-302.

Department of Mathematics,
University of California,
Berkeley, California, 94720,
U.S.A.

Received August 9, 1984

UNIVERSALLY INTEGRALLY CLOSED DOMAINS

David E. Dobbs

Presented by G. deB. Robinson, F.R.S.C.

Abstract. A characterization is given of the integral domains R , with quotient field K , such that S is integrally closed in $S \otimes_R K$ for each integral domain S which is an algebraic extension of R .

Integrality is one of the most important universal properties studied in commutative algebra (cf. [3, Lemma, page 160]). However, the property of being integrally closed is far from being universal. For instance, working inside the Gaussian numbers, we see that $\mathbb{Z}[2i]$ is not integrally closed in $\mathbb{Z}[2i] \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(i)$, although \mathbb{Z} is of course integrally closed in \mathbb{Q} . Let us say that an integral domain R , with quotient field K , is a universally integrally closed domain in case (the canonical image of) S is integrally closed in $S \otimes_R K$ for each commutative R -algebra S ; that is, in case the property that R is integrally closed (in K) holds and is preserved by arbitrary changes of

base, $R \rightarrow S$. This note presents two theorems characterizing these, and some related, integral domains.

THEOREM 1. For an integral domain R with quotient field K , the following are equivalent:

- (1) R is a universally integrally closed domain;
- (2) If S is an integral domain having R as a subring, then S is integrally closed in $S \otimes_R K$;
- (3) If S is an integral domain having R as subring such that the transcendence degree of S over R is 1, then S is integrally closed in $S \otimes_R K$;
- (4) If S is a commutative R -free R -algebra which is algebraic over, and contains R , then S is integrally closed in $S \otimes_R K$;
- (5) R is a field.

Proof. It is clear that (5) \Rightarrow (1), for if $R = K$, then the canonical map $S \rightarrow S \otimes_R K$ is an isomorphism. Moreover, the implications (1) \Rightarrow (2), (2) \Rightarrow (3), and (1) \Rightarrow (4) are trivial. We shall next prove the contrapositives of (3) \Rightarrow (5) and (4) \Rightarrow (5).

Choose a nonzero nonunit r in R and an indeterminate X over R . Set $S = R + rRX + X^2 R[X]$, viewed as a subring of $R[X]$. We shall show that S is not integrally closed in $S \otimes_R K$. To this end, view $S \otimes_R K$ as the ring of fractions $S_{R \setminus \{0\}}$ which, since $r \neq 0$, is evidently $R[X]_{R \setminus \{0\}} = K[X]$. Since $X^2 \in S$, it follows that X is in the integral closure of S in $S \otimes_R K$. However, $X \notin S$, since the choice of r assures that $1 \notin rR$. Therefore, (3) \Rightarrow (5).

Finally, to prove that (4) \Rightarrow (5), we suppose $R \neq K$ and seek an algebraic R -free R -algebra $S \supset R$ such that S is not integrally closed in $S \otimes_R K$. To this end, let $S = R[X]/(X^2)$, the ring of dual numbers over R . Then S is R -free on the basis $\{1, u\}$, where $u = X + (X^2)$ satisfies $u^2 = 0$. Since K is R -flat, $S \otimes_R K$ may be identified with $(R[X] \otimes_R K) / (X^2 R[X] \otimes_R K) \cong K[X]/(X^2)$, the ring of dual numbers over K . Write $S \otimes_R K$ as $K + Kv$, where $v^2 = 0$. The canonical map $S \rightarrow S \otimes_R K$ extends the inclusion map $R \rightarrow K$ and sends u to v . Choosing $d \in K \setminus R$, we see that $w = 1 + dv \in (S \otimes_R K) \setminus S$ satisfies $w^2 - 2w + 1 = 0$; thus, w is integral over S . A similar calculation reveals that S is algebraic over R , completing the proof.

Let R and K be as above. In view of Theorem 1, it seems natural to ask what happens if one restricts attention to changes of base $R \rightarrow S$ arising from algebraic (i.e., transcendence degree 0) integral domain extensions S of R . For the special case of overrings S of R (i.e., $R \subset S \subset K$), the answer is given by the following reformulation of a result of E.D. Davis [2, Theorem 1]: S is integrally closed (in $S \otimes_R K$) for each overring S of R if and only if R is a Prüfer domain. The next theorem answers the question raised above, as an application of the work in [1] on seminormal pairs.

THEOREM 2. For an integral domain R with quotient field K , the following are equivalent:

(1) If S is an integral domain which is algebraic over, and contains R , then S is integrally closed in $S \otimes_R K$;

(2) Either R is a Prüfer domain such that K is algebraically closed or R is a field.

Proof. (2) \Rightarrow (1): As above, the case $R = K$ is trivial. So we may suppose that R is a Prüfer domain and K is algebraically closed. Consider an algebraic extension $R \subset S$ of integral domains. The induced extension of quotient fields is algebraic, and hence trivial; i.e., S is an overring of R . By the result of Davis cited earlier, S is indeed integrally closed (in $S \otimes_R K \cong K$).

(1) \Rightarrow (2): Each overring of R is algebraic over R . Hence, by another appeal to Davis's result, (1) assures that R is a Prüfer domain. If the assertion fails, $K (\neq R)$ is not algebraically closed. Choose an algebraic proper field extension L of K , and let T denote the integral closure of R in L . As usual, clearing denominators leads to $T \otimes_R K \cong L$, and so $T \neq R$. Hence T is not an overring of R . Then, by [1, Lemma 2.2(c) (ii)], some ring contained between R and T is not seminormal. It follows easily (cf. [1, Lemma 2.1(f)]) that there exists $u \in L$ such that $u \notin S = R[u^2, u^3]$. Note that $S \otimes_R K$ may be identified with $R[u^2, u^3]_{R \setminus \{0\}} = K[u^2, u^3]$ which, since u^2 and u^3 are algebraic over K , is simply the field $K(u^2, u^3) = K(u)$. Thus $u \in (S \otimes_R K) \setminus S$, although u is evidently integral over S , contradicting (1). This completes the proof.

REMARK 3. (a) Let \mathbb{A} denote the ring of all algebraic integers, i.e., the integral closure of \mathbb{Z} in an algebraic closure $\bar{\mathbb{Q}}$ of \mathbb{Q} . Then \mathbb{A} satisfies condition (2) in the statement of Theorem 2. Indeed, \mathbb{A} is a Prüfer domain (cf. [5, Theorem 22.3]) and, in fact, a Bézout domain (cf. [6, Theorem 102]); and the quotient field of \mathbb{A} is $\bar{\mathbb{Q}}$, which is algebraically closed.

(b) "Prüfer" cannot be omitted from the statement of Theorem 2. To see this, begin with B , an integrally closed nonPrüfer integral domain, say with quotient field F . (Such B may be found by the $D + M$ construction: cf. [5, Exercise 13(2), page 286].) Let R be the integral closure of B in an algebraic closure \bar{F} of F . Since $B = R \cap F$ is not a Prüfer domain, neither is R , by [5, Theorem 22.4]. Thus, although R is integrally closed and has algebraically closed quotient field (viz., \bar{F}), R does not satisfy condition (2) of Theorem 2.

(c) Possibly outside the context of overrings, we can at least state the following, by applying a recent result of J.-P. Olivier [7, Theorem 5.1]. Let R be a Prüfer domain with quotient field K and let S be a commutative torsion-free R -algebra such that S is $S \otimes_R S$ -flat; then S is integrally closed in $S \otimes_R K$. This result applies if $R \rightarrow S$ is étale but, due to ramification, is of limited use for extensions of rings of algebraic integers.

(d) Despite the above comments, it is possible to characterize Prüfer domains via a universal property. Such results appear in [8, Theorem 4] and [4, Corollary 2.3 and Theorem 2.6].

REFERENCES

- [1] D.F. Anderson, D.E. Dobbs, and J.A. Huckaba, On seminormal overrings, *Comm. Algebra* 10(1982), 1421-1448.
- [2] E.D. Davis, Overrings of commutative rings, II. Integrally closed overrings, *Trans. Amer. Math. Soc.* 110(1964), 196-212.
- [3] M. Demazure and P. Gabriel, Introduction to algebraic geometry and algebraic groups, North Holland, Amsterdam, 1980.
- [4] D.E. Dobbs and M. Fontana, Universally going-down integral domains, *Arch. Math.* 42(1984), 426-429.
- [5] R. Gilmer, Multiplicative ideal theory, Dekker, New York, 1972.
- [6] I. Kaplansky, Commutative rings (rev. ed.), Univ. of Chicago Press, Chicago, 1974.
- [7] J.-P. Olivier, Going up along absolutely flat morphisms, *J. Pure Appl. Algebra* 30(1983), 47-59.
- [8] F. Richman, Generalized quotient rings, *Proc. Amer. Math. Soc.* 16(1965), 794-799.

Department of Mathematics
University of Tennessee
Knoxville, Tennessee 37996
U.S.A.

Received November 14, 1984

LE GROUPE DES AUTOMORPHISMES DU p-GROUPE DE SYLOW
DU GROUPE SYMETRIQUE DE DEGRE p^m : RESULTATS

PAUL LENTOUDIS

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

Outline: In our previous note [4], we have exposed the idea of the determination of the group of automorphisms $\text{Aut}(P_m)$ of the p-Sylow subgroup P_m of the symmetric group of the degree p^m . Here, we describe this group. We conserve the definitions and the notation of the note [4].

La méthode décrite dans notre note précédente [4] (dont on conserve les notations) permet de déterminer le groupe des automorphismes du p-groupe de Sylow P_m du groupe symétrique S_{p^m} de degré p^m . Dans cette note on présente la description de $\text{Aut}(P_m)$. Pour ce faire on donne tous les résultats intermédiaires, indispensables pour présenter les sous-groupes intervenant dans la description finale de $\text{Aut}(P_m)$ et en particulier du noyau de l'homomorphisme ϕ .

On note

$$G_0 = P_m \supset G_1 \supset \dots \supset G_{m-1} \supset G_m \quad (s)$$

la suite canonique de P_m . Afin de trouver le noyau $N(\phi)$, on a à déterminer d'abord toutes les images (s') de la suite canonique (s) de P_m par les automorphismes $\in N(\phi)$, en fait toutes les images G'_m du dernier groupe G_m de (s) (étant donné que les G_i , pour $i < m$, restent stables par les automorphismes $\in N(\phi)$). On pose $T = \overline{G'_m}$. Etant donné que les automorphismes $\in N(\phi)$ préservent les têtes de tout sous-groupe de P_m , $\overline{G'_m} = T$ et les groupes G'_m sont des extensions par T de leurs sous-groupes de fond. Les groupes, qui peuvent jouer le rôle de sous-groupes de fond des groupes cherchés G'_m (on les dira compatibles avec T), sont les sous-groupes H de Δ_{m-1} , qui vérifient les trois propriétés suivantes:

- a) H est d'indice p dans Δ_{m-1}
- b) H est anti-invariant dans P_m

c) H est stable par les conjugaisons $\omega_{\bar{A}}: X \rightarrow \bar{A}X\bar{A}^{-1}$ ($\bar{A} \in T, X \in \Delta_{m-1}$) induites par T sur Δ_{m-1} .

En plus, toute extension par T d'un sous-groupe H de Δ_{m-1} vérifiant a), b) et c) est un certain G_m^c .

On prouve que les sous-groupes H de Δ_{m-1} , qui vérifient les conditions a) et b), sont ceux qui admettent un système générateur de la forme

$$S = \{A_i = [0, \dots, 0, a_m(x) = x^i - c_i]; c_i \in F_p, i \in J \setminus \{(0, \dots, 0)\}\}, \text{ où } J = \prod_{k=1}^{m-1} J_k, J_k = [0, p-1] \subset Z.$$

On démontre que H vérifie en plus la condition c) si et seulement si $c_i = 0$, pour tout i qui n'appartient à aucun des ensembles:

$$I_\xi = \{i = (i_{m-1}, \dots, i_1); i_j = p-1 \text{ si } j > \xi \text{ et } i_j = 0 \text{ si } j < \xi\}, \text{ où } 1 \leq \xi \leq m-1.$$

On pose $\tilde{G}_m = H_0$.

Les extensions de H par T peuvent être engendrées (mod H) par un système R de représentants des classes (mod H) (pour cela on les note (T, H; R)) de la forme suivante:

$$R = \{A(j, i, k) = [0, \dots, a_{j+1} = x_{j,i}^{(p-1)k}, 0, \dots, 0, d(j, i, k)]; d(j, i, k) \in F_p; (j, i, k) \in L\},$$

L étant l'ensemble des (j, i, k), tels que $2 \leq j \leq m-1, 1 \leq i \leq j, 1 \leq k \leq p-1$. Il existe d'ailleurs des extensions de H par T avec les $d(j, i, k)$ arbitraires.

Chacune des extensions (T, H; R) est donc complètement déterminée par le vecteur des constantes $(d(j, i, k); (j, i, k) \in L)$ et l'ensemble de ces vecteurs forme un groupe abélien. On a $G_m = (T, H_0; R_0)$, où R_0 est le système de représentants, qui correspond au vecteur des constantes zéro.

On montre qu'on peut choisir des automorphismes $f(R)$ resp. $f(H)$ de P_m , qui transforment (T, H; R) resp. (T, H₀; R) en (T, H; R) indépendamment de H resp. de R, et que les $f(R)$ resp. les $f(H)$ forment des groupes, qu'on va noter C_m resp. L_m , qui commutent élément par élément.

(†) On écrira resp. au lieu de respectivement

ment. Donc $f(R)f(H)=f(H)f(R)$ transforme $G_m=(T, H_0; R_0)$ en $G'_m=(T, H; R)$ et $C_m L_m = L_m C_m$ est un sous-groupe de $N(\phi)$ transformant la suite canonique (s) en son image (s') par les $f \in N(\phi)$ quelconques.

Les formules, qui définissent les éléments de C_m et qui sont trop longues pour être données ici, ont été trouvées par le calcul effectif de l'automorphisme donné par le théorème d'immersion dans la situation particulière correspondante. Le groupe C_m est isomorphe au groupe additif des vecteurs des constantes et il opère identiquement sur Δ_{m-1} .

Afin de décrire le groupe L_m , on désigne par

$$D_i = \frac{\partial}{\partial x_i}$$

l'opérateur usuel de dérivation partielle et on pose

$$D^{(j)} = D_{j+1} D_{j+2} \dots D_{m-1} \quad (1 \leq j \leq m-1).$$

Les automorphismes $\in L_m$ sont définis par la correspondance

$$[a_1, \dots, a_{m-1}, a_m] \rightarrow [a_1, a_2, \dots, a_{m-1}, a_m + \sum f_{j,k} (D^{(j)})^{p-1} D_j^k a_m],$$

où $f_{j,k} \in F_p$ et la sommation est faite sur tous les j, k tels que $1 \leq j \leq m-1; 1 \leq k \leq p-1$.

Les sous-groupes déjà exposés nous permettent de présenter le groupe $\text{Aut}(P_m)$.

(a) $\text{Aut}(P_m, s, N) = \text{Aut}(P_m, s) \cap N(\phi) = (N(\phi) \cap \Omega_m) (N(\phi) \cap \text{Int}_m(P_m))$ où $N(\phi) \cap \Omega_m$ est l'ensemble des automorphismes $w = (w_1, \dots, w_m)$ avec $w_i = 1 \in F_p$ pour chaque $1 \leq i \leq m-1$ et $N(\phi) \cap \text{Int}_m(P_m)$ est l'ensemble des intérieurs de P_m engendrés par les $A \in G_m$, qui vérifient $\bar{A} = [0, \dots, 0] \in P_{m-1}$

(b) $N(\phi) = L_m C_m \text{Aut}(P_m, s, N)$

(c) $\text{Im} \phi = \Omega_{m-1} \text{Int}(P_{m-1})$

(d) $\text{Im}^*(\phi) = \Omega_m \text{Int}(P_m)$

(e) $\text{Aut}(P_m) = \Omega_m \text{Int}(P_m) L_m C_m$

(f) $|L_m \cap \text{Int}(P_m)| = p$, $|\Omega_m| = (p-1)^m$, $|L_m| = p^{(m-1)(p-1)}$,

$$|C_m| = p^{\frac{(m-1)(m-2)}{2}(p-1)}$$

$$(g) \quad |\text{Aut}(P_m)| = (p-1)^m p^{n(m)} \quad \text{où } n(m) = p^{m-1} + p^{m-2} + \dots + p^2 + \frac{m^2 - m + 2}{2}(p-1).$$

BIBLIOGRAPHIE

- [1] Marshall Hall, Jr: The theory of groups, The Macmillan Company, New York, 1959
- [2] Leo Kaloujnine: Structures des p-groupes de Sylow des groupes symétriques finis, in Annales Scientifiques de l'Ecole Normale Supérieure, 1948, pp.239-271
- [3] M.Krasner-L.Kaloujnine: Produit complet des groupes de permutations et problème d'extension de groupes, in Acta Scientiarum Mathematicarum de Szeged: I:13(1950), pp.208-230, II:14(1951), pp.39-66 et III:14(1951), pp.69-82
- [4] Paul Lentoudis: Détermination du groupe des automorphismes du p-groupe de Sylow du groupe symétrique de degré p^m : l'idée de la méthode, in Comptes Rendus Mathématiques de l'Académie des Sciences, La Société Royale du Canada, VII(1), 67-72

Paul Lentoudis
 Université de Patras
 Département de Mathématiques
 Patras - GRECE

Received December 3, 1984

ON THE CLASSIFICATION OF NONCOMMUTATIVE TORI

Shaun Disney, George A. Elliott, F.R.S.C.,
Alexander Kumjian, and Iain Raeburn

Abstract. The classification of the C*-algebras associated with pairs (G, ρ) where G is a torsion-free discrete abelian group and ρ is an antisymmetric bicharacter on G with values restricted to be of finite order in \mathbb{T} (in other words, the higher dimensional analogues of the rational rotation algebras) is shown to be the same as the classification of the pairs (G, ρ) . This is done by identifying the pair (G, ρ) with an invariant of the associated C*-algebra. The invariant is formulated in terms of K-theory.

1. Let G be a torsion-free discrete abelian group and let $\rho: G \times G \rightarrow \mathbb{T}$ be an antisymmetric bicharacter on G . As in [6] and [3], denote by $A_\rho = A_{(G, \rho)}$ the enveloping C*-algebra of the *-algebra generated by a family of unitaries $(u_g)_{g \in G}$ with relations

$$u_h u_g = \rho(g, h) u_g u_h.$$

(As pointed out to the second author by Rieffel, this is the form the commutation relations must take for the formulas of [3] to be correct; in relation (1.1) of [3] $g \wedge h$ should be replaced by $h \wedge g$.)

In the present note we shall be concerned solely with the case that $\rho(g, h)$ is of finite order in \mathbb{T} for every g and h in G . We shall say in this case that ρ is locally of finite order. By Theorem 3.1 of [3] this is exactly the case that all projections in A_ρ have rational trace.

Consider the category of all pairs (G, ρ) where ρ is locally of finite order, with isomorphisms. By an isomorphism $(G, \rho) \rightarrow (G', \rho')$ we mean a group isomorphism $\alpha: G \rightarrow G'$ such that $\rho' = \rho(\alpha \wedge \alpha)$. Clearly the correspondence

$$(G, \rho) \mapsto A_{(G, \rho)}$$

is a functor from the category of pairs (G, ρ) to the category of C*-algebras $A_{(G, \rho)}$.

Theorem. The functor $(G, \rho) \mapsto A_{(G, \rho)}$ (restricted to ρ locally of finite order) has an inverse, with respect to isomorphisms.

2. In the case $G = \mathbb{Z}^2$, the classification of the algebras A_ρ is known, independently of whether ρ is of finite order or not, - the well known arguments in [5] and [4] do not distinguish between these alternatives for ρ . Our result gives additional information in this case, provided that ρ is of finite order: namely, the determinant of the automorphism of $K_1(A_\rho) = \mathbb{Z}^2$ induced by an automorphism of A_ρ must be equal to $+1$, unless $\rho^2 = 1$.

The arguments in [5] and [4], which consist in computing the ordered group $K_0(A_\rho)$ from which (the isomorphism class of) ρ may easily be recovered, when $G = \mathbb{Z}^2$, also work for any torsion-free group of rank two. If G is allowed to have rank three or more, however, then the ordered group $K_0(A_\rho)$ (together with the class of $1 \in A_\rho$) is no longer sufficient to determine ρ . It seems that our functorial approach to the problem, while for technical reasons successful so far only for extremely special bicharacters ρ , may be what is needed in the general case.

3. Recall that by the computation in [3] of the Chern character of Connes (defined in [1]) for $A_{(G,\rho)}$, an injection $K_*(A_{(G,\rho)}) \rightarrow \Lambda_{\mathbb{R}} G$, $K_*(A_{(G,\rho)})$ has a \mathbb{Z}^+ -filtered structure with relative quotients isomorphic to $\Lambda^n G$, $n = 1, 2, \dots$.

Theorem. For pairs (G,ρ) with ρ locally of finite order, the \mathbb{Z}^+ -filtered structure of $K_*(A_{(G,\rho)})$ and the identification of the relative quotients with $\Lambda^n G$, derived from the Chern character $K_*(A_{(G,\rho)}) \rightarrow \Lambda_{\mathbb{R}} G$, are natural with respect to isomorphisms.

Proof. We must show that if $\alpha: (A_{(G,\rho)} \rightarrow A_{(G',\rho')})$ is an isomorphism of C^* -algebras then the induced isomorphism $[\alpha]: K_*(A_{(G,\rho)}) \rightarrow K_*(A_{(G',\rho')})$ preserves the \mathbb{Z}^+ -filtered structure and in the relative quotients becomes an isomorphism of exterior algebras $\Lambda G \rightarrow \Lambda G'$.

Noting that α takes the centre of $A_{(G,\rho)}$ onto the centre of $A_{(G',\rho')}$, we shall reduce the problem to the commutative case.

Denote by H (resp. H') the largest subgroup of G such that $\rho(H \wedge G) = 1$ (resp. $\rho'(H' \wedge G') = 1$). As established in the proof of Lemma 2.3 of [3], the centre

of $A_{(G,\rho)}$ is generated by $(u_h)_{h \in H}$ and is in this way isomorphic to $A_{(H,1)}$. Similarly the centre of $A_{(G',\rho')}$ is isomorphic to $A_{(H',1)}$.

It is clear from the description of the Chern character in 4.3 of [3] that the following diagram is commutative:

$$\begin{array}{ccc} K_* (A_{(G,\rho)}) & \rightarrow & \Lambda_{\mathbb{R}} G \\ \uparrow & & \uparrow \\ K_* (A_{(H,1)}) & \rightarrow & \Lambda_{\mathbb{R}} H \end{array} .$$

Here the horizontal maps are the Chern character and the vertical ones are canonical.

Since ρ is locally of finite order, $\mathbb{Q} \otimes H = \mathbb{Q} \otimes G$. By the computation in 4.2 and 4.3 of [3], the Chern character is injective. Furthermore, in the case that ρ is locally of finite order, the image of the Chern character is contained in $\Lambda_{\mathbb{Q}} G = \mathbb{Q} \otimes \Lambda G$, and its tensor product with \mathbb{Q} maps $\mathbb{Q} \otimes K_* (A_{(G,\rho)})$ onto $\Lambda_{\mathbb{Q}} G$. Since this is also true for the pair $(H,1)$, and since $\Lambda_{\mathbb{Q}} H = \Lambda_{\mathbb{Q}} G$, we see that the canonical map

$$\mathbb{Q} \otimes K_* (A_{(H,1)}) \rightarrow \mathbb{Q} \otimes K_* (A_{(G,\rho)})$$

is an isomorphism. By commutativity of the diagram this isomorphism preserves the \mathbb{Z}^+ -filtered structure and the identification of the relative quotients with $\Lambda_{\mathbb{Q}}^n H = \Lambda_{\mathbb{Q}}^n G$.

This reduces the theorem to the commutative case (i.e., the case $\rho = 1$). In this case the Chern character is an isomorphism $K_* (A_{(G,1)}) \rightarrow \Lambda G$, and also an isomorphism of graded algebras. (See 2.1 of [3].) The conclusion of the theorem (as restated in the first paragraph above) is therefore clear in this case. (Hence it follows in general.)

4. Proof of Theorem 1. By 3.1 and 3.2 of [3], $\rho = (\exp 2\pi i \tau) |G \wedge G$; this expression makes sense since $\tau(1) = 1$. (More precisely, since $\tau(1) = 1$ the restriction of $\exp 2\pi i \tau$ to the second order filtered subgroup within $K_0(A_{(G,\rho)})$ is equal to 1 on the zeroth order filtered subgroup $\Lambda^0 G = \mathbb{Z}[1]$, and the quotient of these is equal to $G \wedge G$.)

By Theorem 3 this description of ρ is natural with respect to C^* -algebra isomorphisms (under the assumption that ρ is locally of finite order).

5. Let us remark finally that our result leads to the classification result of [2] in the case $G = \mathbb{Z}^3$. (The interpretation of our result in case $G = \mathbb{Z}^2$ is obvious: $\mathbb{Z}^2 \wedge \mathbb{Z}^2 = \mathbb{Z}$ and $[\alpha] \wedge [\alpha] = \det[\alpha]$, so there exists an isomorphism $\alpha: A_\rho \rightarrow A_{\rho'}$, (here ρ and ρ' are of finite order) if, and only if, $\rho' = \rho^{\det[\alpha]}$, and this of course happens if, and only if, $\rho' = \rho^{\pm 1}$.)

The exterior product $\mathbb{Z}^3 \wedge \mathbb{Z}^3$ is identified contravariantly with \mathbb{Z}^3 , in such a way that the canonical action of $GL(3, \mathbb{Z})$ on $\mathbb{Z}^3 \wedge \mathbb{Z}^3$ corresponds to the (contravariant) action $t \mapsto (\det t)t^{-1}$ on \mathbb{Z}^3 . This of course maps $GL(3, \mathbb{Z})$ onto $SL(3, \mathbb{Z})$. Denote $\rho: \mathbb{Z}^3 \wedge \mathbb{Z}^3 \rightarrow \mathbb{T}$ by (ρ_1, ρ_2, ρ_3) where $\rho_i = \rho_{jk}$ with i, j , and k in cyclic order. It follows that there exists an isomorphism $\alpha: A_\rho \rightarrow A_{\rho'}$, (here ρ and ρ' are of finite order) if, and only if, $\rho' = \rho^{(\det[\alpha])[\alpha]^{-1}}$, and this happens if, and only if, $\rho' = \rho^s$ for some $s \in SL(3, \mathbb{Z})$. By ρ^s for $s \in SL(3, \mathbb{Z})$ we mean the image of ρ under the quotient action of s on $\mathbb{R}^3/\mathbb{Z}^3 = \mathbb{T}^3$.

But it is easy to see that the orbit of an element ρ of the group $\mathbb{Q}^3/\mathbb{Z}^3$ under the action of $SL(3, \mathbb{Z})$ is determined by the order of ρ . (This is in fact true for any $n \geq 2$ in place of 3, and the general case of this follows from the case $n = 2$.)

Acknowledgements: This work was partially supported by the Mathematical Sciences Research Centre of the Australian National University, the 1984 Australian Harmonic Analysis Conference (University of New South Wales), the Danish Natural Science Research Council, and the Natural Sciences and Engineering Research Council of Canada.

References

1. A. Connes, C^* -algèbres et géométrie différentielle, C.R. Acad. Sci. Paris 290 (1980), 599-604.
2. S. Disney and I. Raeburn, Homogeneous C^* -algebras whose spectra are tori, J. Austral. Math. Soc., to appear.

3. G.A. Elliott, On the K-theory of the C*-algebra generated by a projective representation of a torsion-free discrete abelian group, *Operator Algebras and Group Representations, Volume 1*, Pitman, London, 1984, 157-184.
4. M. 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.
5. M.A. Rieffel, C*-algebras associated with irrational rotations, *Pacific J. Math.* 93 (1981), 415-429.
6. J. Slawny, On Factor representations and the C*-algebra of canonical commutation relations, *Comm. Math. Phys.* 24 (1972), 151-170.

S.D., A.K., and I.R.: School of Mathematics,
University of New South Wales,
P.O. Box 1, Kensington, New South Wales 2033

G.A.E.: Mathematics Institute,
Universitetsparken 5,
DK-2100 Copenhagen Ø

Received January 2, 1985

PETITS DEGRÉS DE TRANSCENDANCE PAR LA
METHODE DE SCHNEIDER EN UNE VARIABLE

Michel WALDSCHMIDT

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

Résumé. Dans [6], nous avons montré que la méthode de transcendance de Schneider permet de minorer le degré de transcendance de certains corps engendrés par des valeurs de fonctions d'une ou plusieurs variables. Nous donnons ici un énoncé plus fin, dans le cas d'une variable, quand on veut montrer seulement que le degré de transcendance est au moins 2.

1. Sous-groupes à un paramètre de groupes algébriques.

Soit K un sous-corps de \mathbb{C} de degré de transcendance t sur \mathbb{Q} . Soient d_0, d_1, d_2 des entiers positifs ou nuls, avec $d = d_0 + d_1 + d_2 > 0$. On pose $G_0 = \mathbb{C}_a^d$, $G_1 = \mathbb{C}_m^d$. Soit G_2 un groupe algébrique commutatif connexe de dimension d_2 , défini sur K , et soit $G = G_0 \times G_1 \times G_2$.

On considère un homomorphisme analytique non constant φ de \mathbb{C} dans $G(\mathbb{C})$, dont l'image dans $G(\mathbb{C})$ est dense pour la topologie de Zariski, et un sous-groupe $Y = \mathbb{Z}y_1 + \dots + \mathbb{Z}y_\ell$ de \mathbb{C} , de rang ℓ sur \mathbb{Z} , tel que $\varphi(Y) \subset G(K)$. Enfin on note κ le rang sur \mathbb{Z} de $\text{Ker } \varphi$.

Les résultats du chapitre 4 de [3] peuvent être regroupés dans l'énoncé suivant :

Théorème 1. Si $\ell d > \ell - \kappa + d_1 + 2d_2$, alors $t \geq 1$.

Le résultat principal de cette note est le suivant :

Théorème 2. On suppose

$$\ell d \geq 2(\ell + d_1 + 2d_2)$$

ou

$$\kappa = 1 \text{ et } 2\ell d > 3(\ell - 1 + d_1 + 2d_2).$$

Alors $t \geq 2$.

Cet énoncé améliore, pour les sous-groupes à un paramètre, le théorème 5.1 de [4]. Il contient des résultats classiques d'indépendance algébrique pour les valeurs de la fonction exponentielle, ainsi que certaines généralisations aux fonctions elliptiques, dues à Brownawell, Kubota, Shmelev, Masser et Wüstholz (voir [5] I §3). Comme dans [6] II, on déduit du théorème 2 des énoncés d'indépendance algébrique portant sur les valeurs de fonctions exponentielle, elliptiques, sigma et zêta de Weierstrass, ainsi que de fonctions abéliennes ou quasi abéliennes.

2. La méthode de Schneider.

Remarquons d'abord que d_0 et κ valent chacun 0 ou 1. De plus, si $\kappa = 1$, alors $d_0 = 0$ et $d_1 = 0$ ou 1.

Sous les hypothèses du théorème 2, supposons $t = 1$.

a) La fonction auxiliaire.

On montre l'existence d'un plongement de G dans $A_{d_0 + d_1} \times P_N$, défini sur K , d'une constante $C > 0$, et d'une suite $(P_S)_{S \in S_0}$ de polynômes de l'anneau

$$K[U_1, \dots, U_{d_0}, V_1, \dots, V_{d_1}, W_0, \dots, W_N]$$

ayant les propriétés suivantes :

(i) le polynôme P_S est de degré $\leq D_0$ en U_1, \dots, U_{d_0} , de degré $\leq D_1$

en V_1, \dots, V_{d_1} , et il est homogène de degré $\leq D_2$ en W_0, \dots, W_N ,
où D_0, D_1, D_2 sont des fonctions de S définies par

$$D_0 \log S = D_1 S = D_2 S^2 = \Delta$$

avec

$$\Delta^{d-2} = c S^{d_1+2d_2} (\log S)^{d_0-1} \quad \text{si } \kappa=0$$

et

$$\Delta^{d-\frac{3}{2}} = c S^{d_1+2d_2-1} \quad \text{si } \kappa=1.$$

(ii) P_S ne s'annule pas partout sur $G(K)$.

(iii) Pour une infinité de S , P_S s'annule en chaque point de l'image par φ de l'ensemble

$$Y(S) = \{h_1 y_1 + \dots + h_\ell y_\ell ; (h_1, \dots, h_\ell) \in \mathbb{Z}^\ell ; 0 \leq h_j \leq S, 1 \leq j \leq \ell\}.$$

Pour démontrer cela, on utilise les arguments de [4] §2.

On plonge d'abord G_2 dans P_N , grâce à la compactification lisse de Serre. La proposition 2.1 de [4] permet ensuite de construire P_S vérifiant (i) et (ii) de telle sorte que la fonction entière F_S obtenue en substituant aux variables U_i, V_j, W_k les coordonnées de φ vérifie

$$\sup_{|z|=r} |F_S(z)| \leq e^{-c_1 \Delta^2}$$

avec

$$r = \begin{cases} c_2 S & \text{si } \kappa=0 \\ c_2 \Delta D_2^{-1/2} & \text{si } \kappa=1, \end{cases}$$

et c_1, c_2 sont des constantes positives ne dépendant pas de S .

Pour démontrer (iii), on utilise le critère de Gel'fond (voir par exemple [5] théorème 7), grâce à l'hypothèse $t=1$.

b) Le lemme de zéros.

Nous appellerons "lemme de zéros" soit le théorème 2 de [2], soit le théorème B de [1] qui est plus faible, mais qui suffit ici. Pour l'utiliser, nous avons besoin d'un lemme préliminaire.

Lemme. Soient G un groupe algébrique commutatif sur \mathbb{C} de dimension d , $\varphi: \mathbb{C} \rightarrow G(\mathbb{C})$ un homomorphisme analytique d'image Zariski dense dans $G(\mathbb{C})$, Y un sous-groupe de \mathbb{C} de rang ℓ sur \mathbb{Z} , $\Gamma = \varphi(Y)$, et H un sous-groupe algébrique de G de codimension $r \geq 1$. Soit κ le rang sur \mathbb{Z} du noyau de φ . Alors le rang sur \mathbb{Z} de $\Gamma / \Gamma \cap H$ est

$$\begin{cases} \ell \text{ ou } \ell - \kappa & \text{si } r = d \text{ et } d \geq 2 \\ \ell \text{ ou } \ell - 1 & \text{si } 1 < r < d \\ \ell, \ell - 1 \text{ ou } \ell - 2 & \text{si } r = 1. \end{cases}$$

De plus, si G est linéaire, ce rang est

$$\begin{cases} \ell & \text{si } r > 1 \\ \ell \text{ ou } \ell - 1 & \text{si } r = 1. \end{cases}$$

Démonstration du lemme. Notons $\pi: G \rightarrow G/H$ la projection, et ψ la restriction de $\pi \circ \varphi$ à Y . Alors

$$\text{rg}_{\mathbb{Z}} \Gamma / \Gamma \cap H = \text{rg}_{\mathbb{Z}} Y - \text{rg}_{\mathbb{Z}} \ker \psi.$$

Mais $\pi \circ \varphi$ est un sous-groupe à un paramètre de G/H , d'image Zariski dense, donc

$$\text{rg}_{\mathbb{Z}} \ker \psi \leq \text{rg}_{\mathbb{Z}} \ker \pi \circ \varphi \leq \begin{cases} \kappa & \text{si } r = d \\ 1 & \text{si } 1 < r < d \\ 2 & \text{si } r = 1. \end{cases}$$

Enfin, si G est linéaire,

$$\text{rg}_{\mathbb{Z}} \ker \pi \circ \varphi \leq \begin{cases} 0 & \text{si } r > 1 \\ 1 & \text{si } r = 1. \end{cases}$$

D'où le lemme.

Soit ν un entier positif assez grand. On choisit S suffisamment grand par rapport à ν .

Si $\kappa = 1$, on a par hypothèse $2\ell d > 3(\ell - 1 + d_1 + 2d_2)$, d'où

$$S^{\ell-1} \geq \nu D_0^d D_1^{d_1} D_2^{d_2},$$

et

$$S^{\ell-2} \geq \nu D_1.$$

On obtient alors facilement une contradiction avec le lemme de zéros.

Nous supposons désormais $\kappa=0$. Si G est un groupe linéaire, l'hypothèse $\ell d \geq 2(\ell + d_1)$ implique

$$S^{\ell} \in \nu D_0^{d_0} D_1^{d_1}$$

et

$$S^{\ell-1} \in \nu D_0.$$

Le lemme de zéros donne la contradiction voulue.

On peut maintenant supposer $d_2 \geq 1$, et $\ell \geq 5$; de plus, si $d_0=1$, alors $d_1 \leq 2$. On vérifie alors

$$S^{\ell} \in \nu D_0^{d_0} D_1^{d_1} D_2^{d_2},$$

$$S^{\ell-1} \in \nu D_0^{d_0} D_1^{d_1} D_2^{d_2-2},$$

et

$$S^{\ell-2} \in \begin{cases} \nu D_0 & \text{si } d_0=1 \\ \nu D_1 & \text{si } d_0=0. \end{cases}$$

On utilise encore le lemme de zéros : il existe un sous-groupe algébrique H de G , de dimension 1, tel que $\text{rg}_2 \Gamma / \Gamma \cap H = \ell - 1$, et

$$S^{\ell-1} \in \nu D_0^{d_0} D_1^{d_1} D_2^{d_2-1}.$$

Alors $d > 3$, et

$$\ell \geq \frac{2(d_1 + 2d_2)}{d - 2} > \frac{3(d_1 + 2d_2 - 1)}{2d - 5}.$$

Le cas $\kappa=1$ du théorème 2, appliqué à G/H , donne finalement la contradiction voulue.

3. Compléments.

On peut généraliser le théorème 2 en introduisant un type de transcendance. On peut aussi obtenir des grands degrés de transcendance, en adaptant la méthode de [6], mais il faut alors ajouter une hypothèse technique.

Signalons enfin que R. TUBBS (Exposé à Bowdoin, Juillet 1984) a obtenu des raffinements du théorème 2, sous l'hypothèse que $\varphi'(0)$ est définie sur K (méthode de Gel'fond).

Références.

- [1] D.W. MASSER and G. WÜSTHOLZ.- Zero estimates on group varieties I ; Invent. Math., 64 (1981), 489-516.
- [2] J-C. MOREAU.- Démonstrations géométriques de lemmes de zéros II ; in : Approximations diophantiennes et nombres transcendants, Luminy 1982, Progress in Math., 31 (1983), 191-197, Birkhäuser Verlag.
- [3] M. WALDSCHMIDT.- Nombres transcendants et groupes algébriques ; Soc. Math. France, Astérisque 69-70, 1979.
- [4] M. WALDSCHMIDT.- Sous-groupes analytiques de groupes algébriques ; Annals of Math., 117 (1983), 627-657.
- [5] M. WALDSCHMIDT.- Algebraic independence of transcendental numbers. Gel'fond's method and its developments ; in : Perspective in Mathematics, Anniversary of Oberwolfach 1984, 551-571, Birkhäuser Verlag.
- [6] M. WALDSCHMIDT.- Groupes algébriques et grands degrés de transcendance ; à paraître.

Michel WALDSCHMIDT
 Institut Henri Poincaré
 11, rue Pierre et Marie Curie
 75231 PARIS CEDEX 05

Received January 2, 1985

ELLIPTIC OPERATORS AND RELATIVE K-HOMOLOGY GROUPSON MANIFOLDS WITH BOUNDARY

Krzysztof Wojciechowski

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

The purpose of the paper is to give a simple analytic realisation of the group $K_0(X, Y)$ where X is a smooth manifold with boundary Y . Such a definition was discussed in [5]. Details were rather complicated and Baum and Douglas raised in [2] the problem of a clear interpretation of relative cycles in terms of operators living on X . In the case of a closed manifold all cycles are determined by elliptic operators. We prove that $K_0(X, Y)$ is a subgroup of $K_0(\tilde{X})$ where \tilde{X} is a double of X generated by the classes of operators of special form. Namely we consider the elliptic operator A on \tilde{X} and let A_1 be its restriction to the one exemplar of X . We can paste A_1 on one exemplar of X with A_1^* given on the other copy and get a new operator on \tilde{X} denoted by $A_1 U A_1^*$. The classes of such operators give $K_0(X, Y)$. The main analytical tool used in the note is cutting and pasting of elliptic operators on closed manifolds along the submanifold of codimension 1. It was used before in [3] and [7] to some other problems of index theory. This construction is described in section 1. The analytic definition of $K_0(X, Y)$ is given in section 2. There one can also find the proof that the object we defined is really a suitable K-group. In section 3 using our definition we describe the exact sequence

$$K_0(Y) \rightarrow K_0(X) \rightarrow K_0(X, Y) \rightarrow K_1(Y) \quad .$$

In this note we consider only K-groups and assume that X is even-dimensional and oriented. Generalizations and all details of the proofs will be published in a subsequent paper.

1. *Cutting and pasting of elliptic operators.* Let M be a closed manifold, X a submanifold of M such that X and $M \setminus X$ are submanifolds with common boundary Y . We consider triples (A_1, A_2, g) such that $A_i : C^\infty(M, E_i) \rightarrow C^\infty(M, F_i)$ are elliptic operators of first order acting on sections of vector bundles E_i, F_i over M . We can fix Hermitian structures on E_i, F_i and Riemannian structure on M . We assume that A_1 has the following form on the collar neighbourhood $N \cong I \times Y$ of Y :

$$(1.1) \quad G_1(Y) \left(\frac{\partial}{\partial t} + B_1 \right)$$

Here $G_1 : E_1|_Y \rightarrow F_1|_Y$ is a unitary vector bundle isomorphism, t is the normal coordinate, $B_1 : C^\infty(Y, E_1|_Y) \rightarrow C^\infty(Y, E_1|_Y)$ is an elliptic self-adjoint operator. On an even-dimensional oriented closed manifold any elliptic operator can be deformed to the elliptic differential operator (see [6]). In this case B_1 is uniquely defined up to its class in $K_1(Y)$ (see [5]). Now $g : E_1|_Y \rightarrow E_2|_Y$ is a bundle isomorphism such that for each $y \in Y$ and $\zeta \in S_{Y,Y}$ (S_Y is the cotangent sphere bundle of Y)

$$(1.2) \quad g(y)b_1(y, \zeta) = b_2(y, \zeta)g(y)$$

where b_i denotes the principal symbol of B_i . In this situation we define vector bundles E^g, F^g over M

$$(1.3) \quad E^g = E_1|_X \cup_g E_2|_{M \setminus X}, \quad F^g = F_1|_X \cup_{G_2 g G_1^{-1}} F_2|_{M \setminus X}$$

where we identify $E_{1,Y} \ni e$ with $g(y)e \in E_{2,Y}$ and $F_{1,Y} \ni f$ with $G_2 g G_1^{-1}(y)f \in F_{2,Y}$. We introduce also the new elliptic symbol $a^g : \pi^*(E^g) \rightarrow \pi^*(F^g)$, where $\pi : SM \rightarrow M$ is the natural projection

$$(1.4) \quad a^g = a_1 \text{ on } X, \quad a^g = a_2 \text{ on } M \setminus X$$

where a_i denotes the principal symbol of A_i . a^g is well defined because of our identification. Let $(x, \xi) = (0, y; \nu, \zeta) \in S_x^M$ where ν is conormal to Y and $\zeta \in T^*Y$; then for $e \in E_{1,Y}$ we have

$$(1.5) \quad \begin{aligned} a_1(0, y; \nu, \zeta)e &\sim G_2 g G_1^{-1}(y)a_1(0, y; \nu, \zeta)e = \\ &G_2 g G_1^{-1}(y)G_1(y)(i\nu + b_1(y, \zeta))e = \\ &G_2(y)(i\nu + g(y)b_1(y, \zeta)g^{-1}(y))g(y)e = a_2(0, y; \nu, \zeta)g(y)e. \end{aligned}$$

We denote an elliptic operator with symbol a^g by $A_1 \cup_g A_2$. Let me make some comments in the case when we paste two "pieces" of operators given on X . In this case we define \tilde{X} "double" of X $\tilde{X} = X_1 \cup X_2$ (X_i are copies of X with reversed orientation) and $S\tilde{X} = SX_1 \cup SX_2$ where we identify $\sigma(0, y: \nu, \zeta) = (0, y: -\nu, \zeta)$. Let now $A : C^\infty(\tilde{X}, E) \rightarrow C^\infty(\tilde{X}, F)$ be an elliptic operator on \tilde{X} and $A_1 = A|_{X_1}$, $A = A_1 \cup A_2$. In general we can't paste A_1 with A_1 to get a "double" of A_1 on \tilde{X} , but we can paste A_1 with A_1^* using G (see 1.1):

$$(1.6) \quad \begin{aligned} E^G &= E|_{X_1} \cup_{G^F}|_{X_1}, & F^G &= F|_{X_1} \cup_{G^{-1}F}|_{X_1} \\ a^G &= a_1 \text{ on } X_1, & a^G &= a_1^* \text{ on } X_2, \end{aligned}$$

where a_1 is the principal symbol of A_1 . The definition is correct because we have

$$(1.7) \quad \begin{aligned} a_1(0, y: \nu, \zeta) e \sim G^{-1}(y) a_1(0, y: \nu, \zeta) e &= (i\nu + b(y, \zeta)) e = \\ G^{-1}(y) (i\nu + G(y)b(y, \zeta)) G^{-1}(y) G(y) e &= a_1(0, y: -\nu, \zeta) G(y) e. \end{aligned}$$

Another case of interest to us is the elliptic operator algebraically degenerated on the boundary. It is a 0-th order elliptic pseudodifferential operator which is equal to the bundle automorphism in some collar neighbourhood of the boundary. Now the situation is even better than in the first order case. The principal symbol of A in the collar neighbourhood of the boundary is equal to the bundle automorphism r on the manifold and we can assume that r is unitary and doesn't depend on the normal coordinate. $A \cup A^* : C^\infty(X; E \cup_r E) \rightarrow C^\infty(\tilde{X}; E \cup_{-1} E)$ with symbol equal to the principal symbol of A on X_1 and the principal symbol of A^* on X_2 . Similarly we define $A \cup A$, $A \cup \text{Id}$. These operators are equivalent to the operators $(AP) \cup (AP)^*$, $(AP) \cup (AP)$ and $(AP) \cup P$ where P is an elliptic formally self-adjoint differential operator of first order on \tilde{X} .

2. The group $K_0(X, Y)$. Now let X be an oriented even-dimensional manifold with boundary Y . Let M denote the set of all A such that A is an elliptic operator on some closed manifold M containing X as a submanifold in the way we describe in section 1. We introduce an equivalence relation on M

$$(2.1) \quad S \sim T \quad \text{if and only if} \quad [(S|_X) \cup (S|_X)^*] = [(T|_X) \cup (T|_X)^*] \\ \text{in } K_0(\tilde{X}).$$

Let me remind you that $K_0(\tilde{X})$ can be interpreted as the set of all elliptic operators on \tilde{X} modulo suitable equivalence relation (see

[5]) while $K_0(X) = K_0(DX) = K^0(DX, \partial(DX)) = K^0(DX, SX \cup DX|_Y)$ is the set of all elliptic operators algebraically degenerated on the boundary modulo the same relation (see [5] §2).

Theorem 1. $M / \sim = K_0(X, Y)$.

We prove the theorem using exact sequence

$$(2.2) \quad \begin{array}{ccc} K_*(X) & \xrightarrow{i_*} & K_*(\tilde{X}) \\ \partial_* = 0 \swarrow & & \nwarrow p_* \\ & & K_*(X, Y) \end{array}$$

From (2.2) one can see that it is enough to decompose any element of $K_0(\tilde{X})$ into two parts where the first is an element of M/\sim and the second an element of $i_0(K_0(X))$. Let $A = A_1 \cup A_2$ be a first order elliptic operator on \tilde{X}

$$(2.3) \quad [A] = [A_1 \cup A_2] = [A_1 \cup_{id} A_2] + [A_1^* \cup_{G_1} A_1] - [A_1^* \cup_{G_1} A_1] = [(A_1 \otimes A_1^*) \cup_{id \otimes G} (A_2 \otimes A_1)] - [A_1^* \cup_{G_1} A_1] .$$

The operator $A_1 \otimes A_1^*$ is formally self-adjoint so we can deform its symbol to the identity (out of some collar neighbourhood of Y) and $[(A_1 \otimes A_1^*) \cup_{id \otimes G} (A_2 \otimes A_1)] = [Id \cup D]$ in $K_0(\tilde{X})$ where D is algebraically degenerated on the boundary . As a result we get

$$(2.4) \quad [A] = [A_1 \cup A_2] = [Id \cup D] + [A_1 \cup_{G_1} A_1^*] .$$

Now the theorem is an easy consequence of the fact that the maps in (2.2) can be realised as follows:

$$(2.5) \quad i_0[A] = [Id \cup A] , \quad p_0[D] = p_0[D_1 \cup D_2] = [D_1 \cup D_1^*] .$$

3. *Analytic realisation of the exact sequence* . Now we describe analytic realisation of the exact sequence

$$(3.1) \quad K_0(Y) \xrightarrow{i_0} K_0(X) \xrightarrow{q_0} K_0(X, Y) \xrightarrow{\beta_0} K_1(Y)$$

We start with definition of i_0 . Let $D : C^\infty(Y, V) \rightarrow C^\infty(Y, W)$ be a 0-th order elliptic operator . We use results of Gilkey and Smith (see [4]) . They consider the class of operators with symbols given by Clifford multiplication . Such operators always

exist and from Lemma 2.2.2 we know that if X is orientable and even-dimensional then such an operator P admits a local elliptic boundary condition. Moreover we can assume that P is formally self-adjoint and take as a boundary condition the orthogonal projection $B : E|_Y \rightarrow V_1$ of $E|_Y$ onto some subbundle. Here E is a bundle on which P acts. In that situation (P, B) is elliptic and self-adjoint so $[P_B] = 0$ in $K_0(X)$ where P_B denotes the elliptic operator algebraically degenerated on the boundary constructed from (P, B) by the Atiyah-Bott construction (see [1]). Adding (or tensoring by) trivial pieces to the bundles and operators we can assume that $V = V_1$ and define $(P, DB) : C^\infty(X, E) \rightarrow C^\infty(X, E) \oplus C^\infty(Y, W)$. Now we put

$$(3.2) \quad i_0[D] = [(P, DB)] = [P_{DB}] = [P_{DB}] - [P_B]$$

$$q_0[A] = [AUA^*] .$$

The equality $q_0 i_0 = 0$ is obvious. The operator P_{DB} is not trivial only on the collar neighbourhood of Y but this piece of it in the operator $P_{DB} \cup P_{DB}^*$ is eaten by a suitable piece from the operator P_{DB}^* . Now let A be algebraically degenerated on the boundary and assume that $q_0[A] = [AUA^*] = 0$ in $K_0(X, Y)$, but $[AUA^*] = [A \cup \text{Id}] + [\text{Id}UA^*]$ and as a consequence $[A \cup \text{Id}] = [\text{Id}UA]$. This last equality means that A is equal to the identity operator out of some collar neighbourhood of Y and such operators always come from boundary problem which depends only on the boundary data. So $q_0[A] = 0$ implies that $[A] = i_0[D]$ for some D elliptic on Y . Now we have to define

$\partial_0 : K_0(X, Y) \rightarrow K_1(Y)$. Any class in $K_0(X, Y)$ is represented as $[(A|_X) \cup (A|_X)^*]$ where A is an elliptic operator of first order on closed M so A has the form (1.1) on the collar neighbourhood of Y where $[B]$ the class of B in $K_1(Y)$ is uniquely defined. We put

$$(3.3) \quad \partial_0[AUA^*] = [B] .$$

If A is algebraically degenerated on the boundary then $[AUA^*] = [(AUA^*)P]$ where P is elliptic differential self-adjoint operator of first order and for such operators the operator B from the decomposition (1.1) gives trivial class in $K_1(Y)$ so we have $\partial_0 q_0 = 0$. Now if $\partial_0[AUA^*] = 0$ then A admits a local elliptic boundary condition (see [1], [4]). We take any elliptic condition D and construct a suitable operator A_D algebraically degenerated on the boundary. We have equality

$$(3.4) \quad [AUA^*] = [A_DUA_D^*] = q_0[A_D] .$$

References

1. M.F. Atiyah and R. Bott: The index problem for manifolds with boundary. *Differential Analysis (Bombay Colloquium)*, Oxford 1968.
2. P. Baum and R.G. Douglas: Index theory, Cobordism, and K-homology. *Contemporary Mathematics vol. 10*, Amer. Math. Soc. 1982.
3. B. Booss and K. Wojciechowski: Desuspension of splitting elliptic symbols. Preprint, Roskilde Universitetscenter.
4. P.B. Gilkey and L. Smith: The twisted index problem for manifolds with boundary. *Journal of Differential Geometry* 18 (1983), 393-444.
5. G.G. Kasparov: Topological invariants of elliptic operators. I.: K-homology. *Izv. Akad. Nauk SSSR, Ser. Mat.* 39 (1975), 796-838.
6. R. Palais: Seminar on Atiyah-Singer theorem. Princeton 1965.
7. K. Wojciechowski: Spectral flow and General Linear Conjugation Problem. *Simon Stevin Journal* (to appear).

Instytut Matematyki
Uniwersytet Warszawski
00-901 PKiN Warszawa

Received January 2, 1985

ON PELL NUMBERS WHICH ARE SUMS OF NOT FEWER THAN FOUR SQUARES

by Neville Robbins

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

ABSTRACT The Pell sequence is defined by : $P_0 = 0$, $P_1 = 1$,
 $P_n = 2P_{n-1} + P_{n-2}$ for $n \geq 2$. We determine all n such that
 $P_n \neq a^2 + b^2 + c^2$.

Introduction Let $a = 1+2^{\frac{1}{2}}$, $b = 1-2^{\frac{1}{2}}$. The Pell sequence is defined for non-negative integers by

$$(*) \quad P_n = (a^n - b^n) / (a - b)$$

The secondary Pell sequence is defined by

$$(**) \quad R_n = a^n + b^n$$

(The names of these sequences are due to Lucas [2, p. 187] .)

A well-known theorem of Lagrange states that every natural number is the sum of at most four positive squares [1, p. 302]. In this article , we determine all n such that P_n is a sum of not fewer than four positive squares . By (1) and (2) below , each R_n is a sum of at most three positive squares . For the sake of convenience , we occasionally write $P(n)$ instead of P_n , $R(n)$ instead of R_n .

Preliminaries

- (1) $m \neq a^2 + b^2 + c^2$ iff $m = 4^j k$, where $j \geq 0$ and $k \equiv 7 \pmod{8}$
- (2) $P_{2n} = P_n R_n$

- (3) $R_{2n} = R_n^2 - 2(-1)^n$
 (4) $P_{m+n} = P_m P_{n-1} + P_{m+1} P_n$
 (5) $P_n \not\equiv 7 \pmod{8}$
 (6) $P_n \equiv 1 \pmod{8}$ iff $n \equiv \pm 1 \pmod{8}$
 (7) If m is odd and $j \geq 1$, then $R(4^j m) \equiv 2 \pmod{32}$
 (8) $R_n \equiv 2 \pmod{4}$ for all n
 (9) $P(2^j m) = P(m) \prod_{i=1}^j R(2^{i-1} m)$

Remarks: (1) is stated on p. 311 of [1]. (2), (3), and (4) follow from (*) and (**), noting that $ab = -1$. (5) and (6) are established by observing the periodic residues of the Pell sequence (mod 8), namely: 0, 1, 2, 5, 4, 5, 6, 1, 0, 1, etc. (7) and (8) are established by observing the periodic residues of the secondary Pell sequence (mod 32), namely: 2, 2, 6, 14, 2, 18, 6, 30, 2, 2, etc. (9) follows from (2).

The Main Results

Lemma 1 $2^j \parallel P_n$ iff $2^j \parallel n$

Proof: By observing the periodic residues of the Pell sequence (mod 2), namely: 0, 1, 0, 1, etc., we see that $2 \mid P_n$ if and only if $2 \mid n$. Let $j \geq 1$. Suppose $2^j \parallel n$, i.e. $n = 2^j m$ with m odd. Then (9) and (8) imply $2^j \parallel P_n$. Conversely, suppose $2^j \parallel P_n$. Therefore $2 \mid n$, so $n = 2^k m$ with m odd. But (9) and (8) imply $2^k \parallel P_n$, so $k = j$, i.e. $2^j \parallel n$.

Lemma 2 If m is odd and $j \geq 1$, then

$$P(4^{j+1}m)/4^{j+1} \equiv P(4^j m)/4^j \pmod{8}.$$

Proof: (2) implies $\frac{P(4^{j+1}m)}{4^{j+1}} = \frac{P(4^j m)}{4^j} * \frac{R(4^j m)R(2*4^j m)}{4}$,

so it suffices to show that $\frac{1}{4}R(4^j m)R(2*4^j m) \equiv 1 \pmod{8}$, or equivalently (i) $R(4^j m)R(2*4^j m) \equiv 4 \pmod{32}$. But hypothesis and (7) imply $R(4^j m) \equiv 2 \pmod{32}$. Now (3) implies $R(2*4^j m) \equiv 2 \pmod{32}$, so that (i) is established.

Lemma 3 If $m = 1, 3, 5, \text{ or } 7$, and if $j \geq 1$, then

$$P(4^j m)/4^j \equiv m+2(-1)^{\frac{1}{2}(m-1)} \pmod{8}.$$

Proof: follows from Lemma 2 by induction on j , since

$$\frac{1}{4}P_4 = 3 \equiv 3 \pmod{8}; \quad \frac{1}{4}P_{12} = 3465 \equiv 1 \pmod{8};$$

$$\frac{1}{4}P_{20} = 3998607 \equiv 7 \pmod{8}; \quad \frac{1}{4}P_{28} = 4614389013 \equiv 5 \pmod{8}.$$

Lemma 4 If $m = 1, 3, 5, \text{ or } 7$, and if $j \geq 1$, then

$$P(4^j(m+8k))/4^j \equiv m+2(-1)^{\frac{1}{2}(m-1)} \pmod{8}.$$

Proof: (induction on k) The case $k = 0$ follows from Lemma 3.

$$P(4^j(m+8(k+1))) = P(4^j(m+8k+8)) =$$

$$P(4^j(m+8k))P(4^j 8^{-1}) + P(4^j(m+8k)+1)P(4^j 8), \text{ by (4).}$$

Now (6) implies $P(4^j 8^{-1}) \equiv 1 \pmod{8}$; Lemma 1 implies

$$P(4^j 8) \equiv 0 \pmod{2^{2j+3}}, \text{ so } P(4^j 8) \equiv 0 \pmod{8}. \text{ Therefore}$$

$$P(4^j(m+8(k+1)))/4^j \equiv (1)P(4^j(m+8k))/4^j + (0)P(4^j(m+8k)+1)/4^j$$

$\equiv P(4^j(m+8k))/4^j \pmod{8}$. The conclusion now follows from the induction hypothesis.

Theorem 1 $P_n \neq a^2+b^2+c^2$ iff $n = 4^j t$, $j \geq 1$, $t \equiv 5 \pmod{8}$.

Proof: Suppose $P_n \neq a^2+b^2+c^2$. Then (1) implies $P_n = 4^j(8k+7)$. (5) implies $j \geq 1$. Now Lemma 1 implies $n = 4^j t$, with t odd. Lemma 4 implies $t \equiv 5 \pmod{8}$. Conversely, if $n = 4^j t$, with $j \geq 1$ and $t \equiv 5 \pmod{8}$, then Lemma 4 implies $P_n/4^j \equiv 7 \pmod{8}$, so that (1) implies $P_n \neq a^2+b^2+c^2$.

References

1. G. H. Hardy & E. M. Wright " The Theory of Numbers " , Oxford University Press , Fourth Edition , 1960
2. E. Lucas " Theorie des fonctions numeriques simplement periodiques " Am. J. Math. v. 1 (1877) p. 184-240;289-321

Mathematics Department
San Francisco State University
San Francisco , CA 94132
USA

Received January 8, 1985

AN EASY PROOF FOR SCHUR'S INEQUALITY

Jason J. Levy

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

Let a, b, c be positive and not all equal, let μ be any real number, and consider the expression

$$\Gamma = a^\mu(a-b)(a-c) + b^\mu(b-c)(b-a) + c^\mu(c-a)(c-b).$$

I think I have a proof that $\Gamma > 0$.

We can assume that no two of a, b, c are equal, since if $b = c$, $\Gamma = a^\mu(a-b)^2$. Also by permuting a, b, c , we can assume that $a > b > c$. We consider two cases: $\mu \geq 0$ and $\mu < 0$.

$$\begin{aligned} \text{If } \mu \geq 0, \Gamma &= (a-b)\{a^\mu(a-c) - b^\mu(b-c)\} + c^\mu(a-c)(b-c) \\ &> (a-b)(a^\mu - b^\mu)(b-c) + c^\mu(a-c)(b-c) \\ &> 0. \end{aligned}$$

$$\begin{aligned} \text{If } \mu < 0, \Gamma &= a^\mu(a-b)(a-c) + (b-c)\{-b^\mu(a-b) + c^\mu(a-c)\} \\ &> a^\mu(a-b)(a-c) + (b-c)(-b^\mu + c^\mu)(a-c) \\ &> 0. \end{aligned}$$

Editorial Note

The case $\mu \geq 0$ was communicated by I. Schur to Hardy, Littlewood and Pólya [2, p. 64]. For the case $\mu < 0$, see Watson [3, p. 246; 4, p. 207], who considered separately $\mu \leq -1$ and $-1 < \mu < 0$. Watson noticed that the cases $\mu \geq 0$ and $\mu \leq -1$ had already been published by Barnard and Child [1, p. 217].

REFERENCES

- [1] S. Barnard and J. M. Child: Higher Algebra. Macmillan, London, 1936.
- [2] G. H. Hardy, J. E. Littlewood and G. Pólya: Inequalities. Cambridge University Press, Cambridge, 1934.
- [3] G. N. Watson: Two inequalities. Math. Gazette 37(1953), 244-246.
- [4] G. N. Watson: Schur's inequality. Math. Gazette 39 (1955), 207-208.

York University
4700 Keele Street
Downsview, Ontario
Canada M3J 1P3

Received January 31, 1985

L'ENTROPIE TOPOLOGIQUE D'UN GROUPE D'ITERATION

Jürgen Weitkämper

*Presented by J. Aczél, F.R.S.C.*Sommaire

La loi $h(f^t) = |t| \cdot h(f^1)$ où h désigne l'entropie topologique, est prouvée pour les groupes d'itération $\{f^t: X \rightarrow X; t \in \mathbb{R}\}$, où l'élément neutre f^0 n'est pas nécessairement la fonction identique de l'ensemble X .

Introduction

L'entropie topologique d'une fonction d'un espace compact dans lui-même a été introduite par Adler, Konheim et McAndrew [1] en 1965. En général, on considère cette entropie comme mesure de la complexité de la relation entre la structure topologique et la structure itérative déterminée par la fonction. Adler, Konheim et McAndrew ont conjecturé que la relation $h(f^t) = |t| \cdot h(f^1)$ est vraie pour les fonctions f^t d'un groupe d'itération d'un espace compact. Le but de cette note est de prouver cette conjecture pour les groupes d'itération $\{f^t(x)\}$ d'espaces métriques compacts continus globalement en les deux variables x et t . Nous ne supposons pas que l'élément neutre f^0 est l'application identique de l'espace.

Définitions

On appelle groupe d'itération un groupe $\{f^t: X \rightarrow X; t \in \mathbb{R}\}$ d'applications f^t d'un ensemble X dans lui-même vérifiant $f^{s+t} = f^s \circ f^t$ pour chaque $s, t \in \mathbb{R}$. Sklar [2] a remarqué que l'élément neutre d'un tel groupe n'est pas nécessairement la fonction identique de l'ensemble X . C'est-à-dire que les fonctions f^t ne sont pas nécessairement bijectives. On observe, que l'ensemble $\{f_0^t: X_0 \rightarrow X_0; t \in \mathbb{R}\}$ avec $X_0 = f^0(X)$ et $f_0^t = f^t|_{X_0}: X_0 \rightarrow X_0$ forme un groupe d'itération de l'ensemble X_0 . L'élément neutre de ce groupe est l'application identique de l'ensemble X_0 et les fonctions f_0^t sont bijectives. Alors nous avons seulement les orbites (dans le sens de Kuratowski et G.T. Whyburn) des fonctions f^t dont l'image est

une chaîne (ordonnée comme \mathbb{Z}) ou un cycle. Les applications avec cette structure orbitale sont appelées ultrastabiles par Sklar (voir [2]). Nous appelons un groupe d'itération globalement continu si X est un espace topologique et si la fonction $F: X \times \mathbb{R} \rightarrow X$ définie par $F(x,t) = f^t(x)$ est continue.

Soit f une application continue d'un espace compact dans lui-même. Pour chaque recouvrement ouvert A de X , $N(A)$ désigne le nombre d'ensembles dans un sous-recouvrement ayant la puissance minimale. Pour deux recouvrements A et B nous définissons le recouvrement $A \vee B$ par $A \vee B = \{a \cap b; a \in A \text{ et } b \in B\}$. La limite $h(f,A) = \lim_{n \rightarrow \infty} 1/n \cdot N(\bigvee_{k=0}^{n-1} f^{-k}A)$ existe et l'entropie topologique de f est définie par $h(f) = \sup h(f,A)$, A parcourant les recouvrements ouverts de X . Pour une définition plus précise et pour les propriétés de cette entropie nous renvoyons à Adler, Konheim et McAndrew [1].

Théorème

Soient X un espace métrique compact et $\{f^t: X \rightarrow X; t \in \mathbb{R}\}$ un groupe d'itération globalement continu. Alors on a

$$(1) \quad h(f^t) = |t| \cdot h(f^1) \quad \text{pour chaque } t \in \mathbb{R}.$$

Nous allons prouver ce théorème en deux étapes. D'abord nous observons que $h(f^t) = h_0(f_0^t)$ où X_0 et f_0^t sont définis comme dans l'introduction et h_0 désigne l'entropie topologique relative à l'espace X_0 (cf. le lemme ci-dessous). Le problème se réduit alors à la preuve de la formule (1) pour le groupe $\{f_0^t\}$. Nous allons démontrer que ce groupe remplit les conditions d'un théorème de S. Ito [3] qui prouve la formule (1) pour un groupe d'homéomorphismes.

Lemme

Soient X un espace compact et $g, e: X \rightarrow X$ des fonctions continues avec

$g = g \circ e = e \circ g$ et $e \circ e = e$. Alors $h(g) = h_0(g_0)$, dont $h(g)$ désigne l'entropie de la fonction g relative à l'espace X et $h_0(g_0)$ désigne celle relative à $X_0 = e(X)$ de l'application $g_0 = g|_{X_0} : X_0 \rightarrow X_0$.

Preuve du lemme. Etant l'image d'un espace compact par une application continue, l'ensemble X_0 est compact. La fonction g_0 , étant une restriction de g , est continue. Comme $g = g \circ e$, on a $g(X) \subset e(X)$ et alors g_0 est une fonction dans l'ensemble X_0 . Ainsi, l'entropie topologique $h_0(g_0)$ est définie. Puisque $e \circ e = e$ nous avons $e(x) = x$ pour chaque $x \in X_0$.

Nous prouverons que pour chaque recouvrement A de X il y a un recouvrement A_0 de X_0 avec $h(g, A) = h_0(g_0, A_0)$ et vice-versa. Alors les ensembles $\{h(g, A); A \text{ recouvrement ouvert de } X\}$ et $\{h_0(g_0, A_0); A_0 \text{ recouvrement ouvert de } X_0\}$ sont identiques et par conséquent leurs bornes supérieures, c'est-à-dire les entropies sont égales.

Dans le texte qui suit l'indice-inférieur 0 signifie que les quantités A_0 , N_0 , h_0 se réfèrent à l'espace X_0 .

Sans preuve, nous indiquons les quatre propriétés suivantes:

- (i) Soit B_0 un recouvrement ouvert de X_0 . Alors $B = e^{-1}(B_0)$ est un recouvrement ouvert de X avec $N(B) = N_0(B_0)$.
- (ii) Soit A un recouvrement ouvert de X . Alors $A_0 = \{a \cap X_0; a \in A\}$ est un recouvrement ouvert de X_0 et $g^{-k}(A) = e^{-1}(g_0^{-k}(A_0))$ pour chaque $k \in \mathbb{N}$.
- (iii) Soient A_0 et B_0 des recouvrements ouverts de X_0 . Alors $e^{-1}(A_0) \vee e^{-1}(B_0) = e^{-1}(A_0 \vee B_0)$.
- (iv) Soit B_0 un recouvrement ouvert de X_0 , alors $e^{-1}(g_0^{-k}(B_0)) = g^{-k}(e^{-1}(B_0))$ pour chaque $k \in \mathbb{N}$.
- (v) Soient A un recouvrement ouvert de X et $A_0 = \{a \cap X_0; a \in A\}$. Pour chaque $n \in \mathbb{N}$ on obtient:

$$N\left(\bigvee_{k=0}^{n-1} g_0^{-k}(A)\right) = N\left(\bigvee_{k=0}^{n-1} e^{-1}(g_0^{-k}(A_0))\right) \quad (\text{d'après (ii)})$$

$$= N\left(e^{-1}\left(\bigvee_{k=0}^{n-1} g_0^{-k}(A_0)\right)\right) \quad (\text{d'après (iii)})$$

$$= N_0\left(\bigvee_{k=0}^{n-1} g_0^{-k}(A_0)\right) \quad (\text{d'après (i)}).$$

Alors nous avons $h(g, A) = h_0(g_0, A_0)$.

(vi) Soient B_0 un recouvrement ouvert de X_0 et $B = e^{-1}(B_0)$. Pour chaque $n \in \mathbb{N}$ on obtient:

$$N_0\left(\bigvee_{k=0}^{n-1} g_0^{-k}(B_0)\right) = N\left(e^{-1}\left(\bigvee_{k=0}^{n-1} g_0^{-k}(B_0)\right)\right) \quad (\text{d'après (i)})$$

$$= N\left(\bigvee_{k=0}^{n-1} e^{-1}(g_0^{-k}(B_0))\right) \quad (\text{d'après (iii)})$$

$$= N\left(\bigvee_{k=0}^{n-1} g^{-k}(e^{-1}(B_0))\right) \quad (\text{d'après (iv)}).$$

Alors nous avons $h(g, B) = h_0(g_0, B_0)$.

(vii) Pour chaque recouvrement ouvert A de X il y a un recouvrement ouvert A_0 de X_0 avec $h(g, A) = h_0(g_0, A_0)$ d'après (v). Alors:

$$\begin{aligned} h(g) &= \sup \{h(g, A); A \text{ est un recouvrement ouvert de } X\} \\ &\leq \sup \{h_0(g_0, A_0); A_0 \text{ est un recouvrement ouvert de } X_0\} \\ &= h_0(g_0). \end{aligned}$$

On prouve de même que $h(g) \geq h_0(g_0)$ en appliquant (vi).

Cela nous permet de prouver le théorème.

Preuve du théorème. Nous définissons le groupe d'itération $\{f_0^t\}$ comme dans l'introduction. Les fonctions f_0^t sont bijectives et f_0^{-t} est l'inverse de l'application f_0^t . Ce groupe est globalement continu, parce que la fonction $F_0: X_0 \times \mathbb{R} \rightarrow X_0$ avec $F_0(x, t) = f_0^t(x)$ est une restriction de l'application

correspondante F pour le groupe $\{f^t\}$. Alors les fonctions f_0^t sont des homéomorphismes. L'espace X_0 est compact car il est l'image d'un espace compact par une fonction continue. Alors le groupe $\{f_0^t\}$ remplit les hypothèses du théorème d'Ito [3] qui prouve $h_0(f_0^t) = |t| \cdot h_0(f_0^1)$. En utilisant le lemme deux fois (avec f^0 pour la fonction e) on obtient pour chaque $t \in \mathbb{R}$:

$$\begin{aligned} h(f^t) &= h_0(f_0^t) && \text{(d'après le lemme)} \\ &= |t| \cdot h_0(f_0^1) && \text{(d'après le théorème d'Ito)} \\ &= |t| \cdot h(f^1) && \text{(d'après le lemme).} \end{aligned}$$

Ainsi le théorème est prouvé.

Remarque

Si $\{f^t\}$ est un groupe d'itération d'un intervalle compact les fonctions f_0^t sont strictement croissantes (voir Zdun [4]). Alors $h(f^t) = 0$ pour chaque $t \in \mathbb{R}$,

p. ex.:

$$f^t: [0,2] \rightarrow [0,2], \quad t \in \mathbb{R}, \quad f^t(x) = \begin{cases} x(3^{-t}) & , x \in [0,1], \\ (2-x)(3^{1-t}) & , x \in [1,2]. \end{cases}$$

Exemple

Soit $Y = \{0,1\}^{\mathbb{Z}}$ l'espace des suites ayant pour éléments 0 ou 1, muni de la topologie produit. La fonction $T: Y \rightarrow Y$ ('shift') est définie par $(Ty)_i = (y)_{i+1}$. L'application T est continue avec $h(T) = \log 2$ (v. [1], Exemple 2).

Dans les espaces $X'_0 = Y \times [0,1] \subset X' = Y \times [0,1.5]$, nous définissons la relation d'équivalence \sim par $(y,1) \sim (Ty,0)$ pour chaque $y \in Y$. Les espaces quotients $X = X'/\sim$ et $X_0 = X'_0/\sim$ sont compacts.

Dans X_0 un groupe d'itération $\{f_0^t; t \in \mathbb{R}\}$ est défini par $f_0^t((x,u)) = (T^n x, u+s)$ où $s = t-n$, $n \in \mathbb{Z}$, avec $-u \leq s \leq 1-u$. Le groupe est globalement continu et nous avons $f_0^1((x,u)) = (Tx,u)$ et $h_{X_0}(f_0^1) = h(T) = \log 2$.

Soit $e: X \rightarrow X$ la fonction définie par

$$e((x,u)) = \begin{cases} (x,u) & , u \in [0,1], \\ (x,2-u) & . u \in [1,1.5], \end{cases}$$

alors e est continue et les fonctions $f^t: X \rightarrow X$ définies par $f^t = f_0^t \circ e$ forment un groupe d'itération. On a $h_X(f^1) = h_{X_0}(f_0^1) = \log 2$ d'après le lemme et $h_X(f^t) = |t| \cdot \log 2$.

Références

- [1] Adler, R.L., A.G. Konheim et M.H. McAndrew, Topological Entropy, Trans. Amer. Math. Soc. 114 (1965), 309-319.
- [2] Sklar, A., The embedding of functions in flows, Aequationes Math. 17 (1978), 367.
- [3] Ito, Sh., On the topological entropy of a dynamical system, Proc. Japan. Acad. 45 (1969), 838-840.
- [4] Zdun, M.C., Continuous and differentiable iteration semigroups, Univ. Śląski w Katowicach Prace Nauk. Nr. 308 (1979).

FB Mathematik Univ. Marburg
Lahnberge
D-3550 Marburg
West Germany

Received February 13, 1985

Mailing Addresses

1. H.S.M. Coxeter
Department of Mathematics
University of Toronto
Toronto, Ontario, Canada, M5S 1A1
2. S. Disney
School of Mathematics
University of New South Wales,
P.O. Box 1, Kensington (NSW 2033),
Australia
3. D.E. Dobbs
University of Tennessee
Knoxville, TN 37996, U.S.A.
3. G.A. Elliott
Mathematics Institute
Copenhagen University, Copenhagen,
Denmark
4. A. Kumjian
School of Mathematics
University of New South Wales
P.O. Box 1, Kensington (NSW 2033),
Australia
5. P. Lentoudis
Département de Mathématiques
Université de Patras
Patras, Greece
6. J.L. Levy
York University
4700 Keele Street
Downsview, Ontario, Canada M3J 1P3
7. T. Mazumdar
Department of Mathematics and
Statistics
Wright State University
Dayton, OH 45435, U.S.A.
8. I.F. Putnam
Department of Mathematics,
University of Cal Berkeley
Berkeley, CA 94720, U.S.A.
9. I. Raeburn
School of Mathematics
University of New South Wales
P.O. Box 1, Kensington (NSW 2033),
Australia
10. N. Robbins
Mathematics Department
San Francisco State University
San Francisco, CA 94132, U.S.A.
11. M. Waldschmidt
Institut Henri Poincaré,
11 rue Pierre et Marie Curie
75231 Paris (Cedex 05), France

12. J. Weitkämper

F.B. Mathematik Univ. Marburg
Lahnberge, D-3550 Marburg
West Germany

13. K. Wojciechowski

Instytut Matematyki
Uniwersytet Warszawski
00-901 PKiN Warszawa, Poland