C. R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

POLYNOMIALS WITH FROBENIUS GROUPS OF PRIME DEGREE AS GALOIS GROUPS

Alden A. Bruen, Christian U. Jensen and Noriko Yui**

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

1. Shafarevich [8] has shown that any finite solvable group G is realizable as a Galois group over the field Q of rational numbers. Thompson [7] has recently proved that any finite solvable group G whose every Sylow subgroup is abelian, or any finite group G which is nilpotent of class 2, can occur as a Galois group for a regular extension L over the function field $Q(x)$ (i.e. Q is algebraically closed in L). Their existence theorems, however, do not yield any explicit examples. Apparently, there seems to be a big difference between general existence theorems and actual constructions.

Recall that a Frobenius group G of degree $n \in \mathbb{N}$ is a transitive subgroup of the symmetric group S_n such that any element of G, different from the identity, has at most one fixed point, and that there exists a permutation in G apart from the identity which has a fixed point.

In this paper, we consider the case $G =$ a Frobenius group of prime degree p. We give a constructive and effective characterization of polynomials over Q having G as a Galois group over Q. In addition, actual constructions of parametric families with certain Frobenius groups as Galois groups are carried out. The details can be found in Bruen, Jensen and Yui [1].

2. Let $p(\geq 5)$ be a rational prime. A Frobenius group of degree p is a solvable group, and its structure is completely described by a theorem of Galois (see, e.g. Huppert [3, p.163]). Let $\mathbb{F}_p$ denote the finite field with p elements and let $\mathbb{F}_p^*$ be its multiplicative group. Denote by $Aff(\mathbb{F}_p) = \{x \to cx + d \mid c \in \mathbb{F}_p^*,\ d \in \mathbb{F}_p\} = \mathbb{F}_p \rtimes \mathbb{F}_p^*$ (the semi-direct product of $\mathbb{F}_p$ by $\mathbb{F}_p^*$). If G is a Frobenius group of degree p then G is a subgroup of $Aff(\mathbb{F}_p)$. Therefore G is identified with a semi-direct product $\mathbb{F}_p \rtimes K$ where K is the unique subgroup of $\mathbb{F}_p^*$ of order l with $l \mid p-1$. We denote by $F_{pl} = F_{lp}$ the Frobenius group of degree p and of order pl with $l \mid p-1$. (If $l = 2$, $F_{2p} = D_p$ (the dihedral group of order $2p$).)

3. A characterization of F_{pl} as a permutation group of degree p is essential for our discussion. Regarded as a permutation group acting on $\mathbb{F}_p$, a Frobenius group F_{pl} of degree p and of order pl with $l < p-1$ is transitive but not doubly transitive; the Frobenius group $F_{p(p-1)}$ of degree p and of the maximal possible order $p(p-1)$ is sharply doubly transitive. Conversely, these properties characterize completely Frobenius groups of degree p as permutation groups:

LEMMA A. *Let G be a transitive permutation group of degree p.*

(a) (Burnside, with proof by Wielandt (see, e.g. Passman [6, p.54]) *Assume that G is transitive, but not doubly transitive. Then G is a subgroup of $Aff(\mathbb{F}_p)$. Therefore, G is a Frobenius group F_{pl} with $l < p-1$.*

(b) (Zassenhaus [10]) *Assume that G is sharply doubly transitive. Then $G = F_{p(p-1)}$.*

* The first and third authors were partially supported by the Natural Sciences and Engineering Research Council of Canada.

4. Let $f(x)$ be a monic polynomial of degree p (prime ≥ 5) over $\mathbf{Q}$. Denote by D_f the discriminant of $f(x)$, by N the splitting field of $f(x)$ over $\mathbf{Q}$ and by $Gal(f)$ the Galois group $Gal(N/\mathbf{Q})$.

LEMMA B. *Let $f(x) \in \mathbf{Q}[x]$ a monic irreducible polynomial of degree p and let $\{\alpha_i \mid i = 1, \ldots, p\}$ be its roots in N. Then we have the following assertions.*

(a) (Jensen and Yui [4], Kurvatov [5]) *The roots $\{\alpha_i \mid i = 1, \ldots, p\}$ admit only a trivial $\mathbf{Q}$-linear relation, that is, $c_1\alpha_1 + c_2\alpha_2 + \cdots + c_p\alpha_p \in \mathbf{Q}$, $c_i \in \mathbf{Q}$ for all i, if and only if $c_1 = c_2 = \cdots = c_p$.*

Consequently, all sums of s $(1 \leq s < p)$ distinct algebraic numbers $\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_s}$ with $1 \leq i_1 < i_2 < \cdots < i_s \leq p$ are distinct.

(b) (Cf. Erbach, et al. [2].) *For each s $(1 \leq s \leq (p-1)/2)$, put*

$$p_{p_s}(x) := \prod_{1 \leq i_1 < i_2 \cdots < i_s \leq p} \{x - (\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_s})\}.$$

Then $p_{p_s}(x)$ is a polynomial defined over $\mathbf{Q}$ of degree $p_s := \binom{p}{s} = \frac{p!}{s!(p-s)!}$ having distinct roots. Furthermore, the splitting field of $p_{p_s}(x)$ over $\mathbf{Q}$ is N for every s. (If $p_{p_s}(x)$ is reducible over $\mathbf{Q}$, then the splitting field of each irreducible factor of $p_{p_s}(x)$ over $\mathbf{Q}$ is N.)

5. Now we can formulate our constructive characterizations of polynomials with Frobenius groups of degree p as Galois groups over $\mathbf{Q}$. We note that $F_{p(p-1)/2}$ is a subgroup of the alternating group A_p; however $F_{p(p-1)}$ is not a subgroup of A_p.

THEOREM C. *Let $f(x) \in \mathbf{Q}[x]$ be a monic polynomial of degree p and let $\{\alpha_i \mid i = 1, \ldots, p\}$ be its roots in N.*

(a) *Let $F_{pl} = \mathbf{F}_p \rtimes K$ be a Frobenius group of degree p where K is the unique subgroup of $\mathbf{F}_p^*$ of order l, $l < p-1$ such that $K \not\ni -1 \bmod p$ (resp. $K \ni -1 \bmod p$). Then the necessary conditions for $Gal(f) = F_{pl}$ are*

(i) *$f(x)$ is irreducible over $\mathbf{Q}$,* and

(ii) *$p_{p_2}(x) = \prod_{1 \leq i < j \leq p} \{x - (\alpha_i + \alpha_j)\}$ factors into the product of $(p-1)/2l$ (resp. $(p-1)/l$) distinct monic irreducible polynomials of degree pl (resp. $pl/2$) over $\mathbf{Q}$.*

(b) *Conversely we have the following assertions.*

(b1) *Suppose that*

(i) *$f(x)$ is irreducible over $\mathbf{Q}$,*

(ii) *D_f is a square, and that*

(iii) *$p_{p_2}(x)$ has a factor of degree t, $1 < t < p(p-1)/2$, over $\mathbf{Q}$.*

Then $t = pl$ with $l < (p-1)/2$, and all the factors of $p_{p_2}(x)$ have the same degree pl, so that $l \mid (p-1)/2$. Furthermore, $Gal(f) = F_{pl}$ or F_{2pl}. (If $l = 1$, F_p is interpreted as the cyclic group Z_p.) (For $l = 1$ or 2, see [4].)

(b2) *Suppose that $p > 5$ and that*

(i) *$f(x)$ is irreducible over $\mathbf{Q}$,*

(ii) D_f *is a square,*

(iii) $p_{p_3}(x)$ *remains irreducible over* $\mathbf{Q}$, *and that*

(iv) $p_{p_3}(x) = \prod_{1\le i<j<k\le p} \{x - (\alpha_i + \alpha_j + \alpha_k)\}$ *factors into a product of* $r(\ge 3)$ *distinct monic irreducible polynomials of degree* >1 *over* $\mathbf{Q}$.

Then $Gal(f) = F_{p(p-1)/2}$.

THEOREM D. *Let* $f(x) \in \mathbf{Q}[x]$ *be a monic polynomial of degree* $p > 5$ *and let* $\{\alpha_i \mid i = 1, \dots, p\}$ *be its roots in* N. *Then* $Gal(f) = F_{p(p-1)}$ *if and only if*

(i) $f(x)$ *is irreducible over* $\mathbf{Q}$,

(ii) D_f *is not a square,*

(iii) $p_{p_2}(x) = \prod_{1\le i<j\le p} \{x - (\alpha_i + \alpha_j)\}$ *is irreducible over* $\mathbf{Q}$,

(iv) $p_{p_3}(x) = \prod_{1\le i<j<k\le p} \{x - (\alpha_i + \alpha_j + \alpha_k)\}$ *factors into a product of* $r(\ge 2)$ *distinct monic irreducible polynomials of degree* >1 *over* $\mathbf{Q}$.

For $p = 5$ (i.e. F_{20}), we reformulate a result of Weber [9].

THEOREM E ([9]; cf.[1]). *Let* $f(x) \in \mathbf{Q}[x]$ *be a monic quintic polynomial. Then* $Gal(f) = F_{20}$ *if and only if*

(i) $f(x)$ *is irreducible over* $\mathbf{Q}$,

(ii) D_f *is not a square,*

(iii) *The Weber sextic resolvent of* $f(x)$ *has a rational root.*

(For the definition of the Weber sextic resolvent, see Weber [9, p.670].)

6. We now discuss actual constructions of parametric families with certain Frobenius groups as Galois groups.

THEOREM F ([9]; cf.[1]). *Let* $f(x) = x^5 + ax + b \in \mathbf{Q}[x]$. *Then* $Gal(f) = F_{20}$ *if and only if*

(i) $f(x)$ *is irreducible over* $\mathbf{Q}$,

(ii) $D_f = 4^4a^5 + 5^5b^4$ *is not a square,*

(iii) *the coefficients* a *and* b *are of the form*

$$a = \frac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2 - 6\lambda + 25)}; \quad b = \frac{5^5\lambda\mu^5}{(\lambda-1)^4(\lambda^2 - 6\lambda + 25)}$$

with $\lambda, \mu \in \mathbf{Q}$, $\lambda \ne 1$ *and* $\mu \ne 0$.

We now consider the case $G = F_{p(p-1)/2}$ with $p \equiv 3 \pmod 4$.

THEOREM G. *Let* p *be a rational prime such that* $p \equiv 3 \pmod 4$. *Let* $T_p(x)$ *denote the* p*-th Chebyshev polynomial of the first kind, and let*

$$f_p(x) := \sqrt{p+1}\, T_p\left(\frac{2x}{\sqrt{p+1}}\right) - 1.$$

Then

(a) *$f_p(x)$ has rational coefficients, and is irreducible over* $\mathbf{Q}$.

(b) *Gal$(f_p) = F_{p(p-1)/2}$.*

In particular, after a suitable transformation, F_{21} (resp. F_{55}) is realized as the Galois group of the polynomial

$$\tilde{f}_7(x) = x^7 + 14x^6 - 56x^4 + 56x^2 - 16 \in \mathbf{Q}[x]$$

(resp.

$$\tilde{f}_{11}(x) = x^{11} - 33x^9 + 396x^7 - 2079x^5 + 4455x^3 - 2673x - 243 \in \mathbf{Q}[x]).$$

The construction of Theorem G will work equally well if $\mathbf{Q}$ is replaced by a function field over $\mathbf{Q}$. Consequently, we can obtain a generic family of polynomials for $F_{p(p-1)/2}$.

THEOREM H. *Let p be a rational prime such that $p \equiv 3 \pmod 4$. Let $\mathbf{Q}(a,b)$ be a function field over $\mathbf{Q}$ with indeterminates a and b. With T_p as in Theorem G, let*

$$f_p(x;a,b) := (a^2 + pb^2)^{p/2} T_p\left(\frac{2x}{\sqrt{a^2+pb^2}}\right) - a(a^2+pb^2)^{(p-1)/2}.$$

Then

(a) *$f_p(x;a,b)$ is an irreducible polynomial of degree p over $\mathbf{Q}(a,b)$.*

(b) *The Galois group Gal$(f_p/\mathbf{Q}(a,b)) = F_{p(p-1)/2}$.*

Furthermore, for any pair $(a,b) \in \mathbf{Z}^2$ with $p \nmid ab$ and $a \equiv b \pmod 2$, $f_p(x;a,b)$ is irreducible in $\mathbf{Q}[x]$, and consequently has $F_{p(p-1)/2}$ as Galois group over $\mathbf{Q}$.

In particular, a parametric family with Galois group F_{21} (resp. F_{55}) is given by

$$f_7(x;a,b) = 64x^7 - 112(a^2+7b^2)x^5 + 56(a^2+7b^2)^2x^3 - 7(a^2+7b^2)^3x - a(a^2+7b^2)^3 \in \mathbf{Q}(a,b)[x]$$

(resp.

$$\begin{aligned} f_{11}(x;a,b) = {} & 2^{21}x^{11} - 2^{17}11(a^2+11b^2)x^9 + 2^{15}11(a^2+11b^2)^2x^7 \\ & - 2^57\cdot 11(a^2+11b^2)^3x^5 + 2^5\,5\cdot 11(a^2+11b^2)^4x^3 \\ & - 2\cdot 11(a^2+11b^2)^5x - a(a^2+11b^2)^5 \in \mathbf{Q}(a,b)[x]). \end{aligned}$$

Remarks. (a) That the polynomial $\tilde{f}_7$ (resp. $\tilde{f}_{11}$) obtained in Theorem G has indeed F_{21} (resp. F_{55}) as its Galois group over $\mathbf{Q}$ can be proved by Theorem C (b2). In fact, we have

(i) $\tilde{f}_7(x)$ is irreducible over $\mathbf{Q}$,

(ii) $D_f = 2^{24}7^{18}$ is a square,

(iii) $P_{21}(x)$ is irreducible over $\mathbf{Q}$, and

(iv) $P_{55}(x)$ factors as follows:

$$\begin{aligned} P_{55}(x) = {} & (x^7+42x^6+588x^5+2800x^4+392x^3-5600x^2-3920x-496) \\ & \times (x^7+42x^6+588x^5+2800x^4+392x^3-4816x^2+1568x+288) \end{aligned}$$

× (an irreducible polynomial of degree 21 over Q).

(Respectively, the similar proof can be applied for f_{11} and F_{55}.)

(b) For $F_{p(p-1)/2}$ with $p \equiv 1 \pmod 4$, a similar construction is possible, but becomes much more complicated.

REFERENCES

[1] A.A. Bruen, C.U. Jensen and N. Yui, *Polynomials with Frobenius groups of prime degree as Galois groups II*, J. Number Theory (to appear).

[2] D.W. Erbach, J. Fischer and J. McKay, *Polynomials with PSL(2,7) as Galois group*, J. Number Theory 11 (1979), 69-75.

[3] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, New York, 1967.

[4] C.U. Jensen and N. Yui, *Polynomials with D_p as Galois group*, J. Number Theory 15 (1982), 347-375.

[5] V.A. Kurvatov, *Galois extensions of prime degree and their primitive elements*, Soviet Math. (Iz. VUZ), 21 (1977), 45-53.

[6] D. Passman, *Permutation Groups*, Benjamin, New York, 1968.

[7] J.G. Thompson, *Regular Galois extensions of* Q[x], preprint (1984).

[8] I.R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk. USSR Ser. Mat. 18 (1954), 525-578.

[9] H. Weber, *Lehrbuch der Algebra Bd. I*, Braunschweig (1898).

[10] H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg 11 (1936), 187-220.

Alden A. Bruen
Department of Mathematics
University of Western Ontario
London, Ontario
CANADA M6A 5B7

Christian U. Jensen
Matematisk Institute
Københavns Universitet
Universitetsparken 5
DK-2100 København Ø
DENMARK

Noriko Yui
Department of Mathematics
University of Toronto
Toronto, Ontario
CANADA M5S 1A1

Received July 20, 1984

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

δ-ANNEAUX ET VECTEURS DE WITT

ANDRE JOYAL

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

Résumé

Nous donnons à la théorie des vecteurs de Witt une formulation nouvelle en utilisant les méthodes de l'algèbre universelle et de la théorie des catégories. On introduit une structure algébrique, celle de δ-anneau. Un δ-anneau est un anneau commutatif muni d'une opération unaire supplémentaire satisfaisant à des identités algébriques simples. Le résultat principal consiste à montrer que le foncteur oubliant de la catégorie des δ-anneaux vers celle des anneaux commutatifs possède un adjoint à droite W. Un calcul explicite permet l'identification de W(A) avec l'anneau des vecteurs de Witt sur A. On donne des démontrations plus conceptuelles de plusieurs résultats de la théorie des vecteurs de Witt [7,2].

1- δ-anneaux

Fixons une fois pour toute un nombre premier p et une puissance $q = p^r$ $(r \geq 0)$.

DEFINITION 1 Un δ-anneau A est un anneau commutatif muni d'une opération unaire $\delta: A \to A$ satisfaisant aux identités suivantes:

i) $$\delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{q-1} \frac{1}{p}\binom{q}{i} x^i y^{q-i}$$

ii) $$\delta(xy) = x^q\delta(y) + \delta(x)y^q + p\delta(x)\delta(y)\ ,\ \delta(1) = 0$$

Nous dirons aussi que A est un δ-anneau relativement au couple (p,q).

Ces conditions entraînent que l'opération unaire $f(x) = x^q + p\delta(x)$ est un endomorphisme de l'anneau A:

$$f(x+y) = f(x) + f(y)$$
$$f(xy) = f(x)f(y)$$
$$f(1) = 1$$

Nous dirons que f est l'endomorphisme de Frobenius. Inversement, soit f un endomorphisme d'un anneau commutatif A sans p-torsion. Supposons que pour tout $x \in A$

$$f(x) \equiv x^q \mod pA$$

On obtient une structure de δ-anneau sur A en définissant δ comme suit:

$$\delta(x) = \frac{1}{p}(f(x) - x^q)$$

Exemple 1. L'anneau $\mathbf{Z}$ admet une seule structure de δ-anneau puisque le seul endomorphisme de $\mathbf{Z}$ est l'identité.

Exemple 2 Soit L une extension galoisienne d'un corps K. Soit $B \subset L$ un anneau de valuation discrète et soit $A = B \cap K$. On suppose que $p = p \cdot 1$ est une uniformisante pour B et que $A/pA \simeq \mathbf{F}_q$. On sait montrer [1] l'existence d'une substitution de Frobenius $\sigma \in$ Galois (L/K) caractérisée par

i) $\sigma(B) = B$

ii) $\sigma(x) \equiv x^q \mod pB$

Un morphisme de δ-anneau est un homomorphisme d'anneaux qui préserve δ. Nous dirons aussi que c'est un δ-morphisme. On vérifie que l'endomorphisme de Frobenius est un δ-morphisme.

THEOREME 1 Soit $Z[x_0,x_1,\ldots]$ l'anneau des polynômes sur une suite infinie d'indéterminés. Il y a une seule structure de δ-anneau sur $Z[x_0,x_1,\ldots]$ pour laquelle $\delta(x_n) = x_{n+1}$ pour tout n. Muni de cette structure, $Z[x_0,x_1\ldots]$ est un δ-anneau libre sur x_0.

Désignons par $\underline{A}$ la catégorie des anneaux et par $\underline{\delta A}$ celle des δ-anneaux.

THEOREME 2 Le foncteur oubliant $U: \underline{\delta A} \to \underline{A}$ possède un adjoint à droite $W: \underline{A} \to \underline{\delta A}$.

La théorie des catégorie [6] met en évidence l'équivalence entre le théorème précédent et le suivant:

THEOREME 3 Soient $A \to B$ et $A \to C$ des morphismes de δ-anneaux. Considérons le carré

$$\begin{array}{ccc} A & \to & C \\ \downarrow & & \downarrow i_2 \\ B & \to & B \otimes_A C \\ & i_1 & \end{array}$$

Il y a sur $B \otimes_A C$ une seule structure de δ-anneaux pour laquelle i_1 et i_2 sont des δ-morphismes.

On peut donner une démonstration directe de ces théorèmes ou encore utiliser [8,9]. Comme conséquence, on a:

COROLLAIRE Le foncteur $W: \underline{A} \to \underline{\delta A}$ est représentable par l'anneau $Z[x_0,x_1,\ldots]$. Il y a une bijection naturelle:

$$\gamma_A: W(A) \xrightarrow{\sim} A^N$$

La bijection γ_A s'explicite comme suit:

$$\begin{aligned} W(A) &\simeq \mathrm{Hom}_{\delta}(\mathbb{Z}[x_0,x_1,\ldots], W(A)) \\ &\simeq \mathrm{Hom}\,(\mathbb{Z}[x_0,x_1,\ldots], A) \\ &\simeq A^{\mathbb{N}} \end{aligned}$$

2- Vecteurs de Witt

Pour voir que W(A) est isomorphe à l'anneau des vecteurs de Witt sur A, il suffira d'utiliser une description différente du δ-anneau libre sur un générateur. Cette description est basée sur le résultat suivant.

PROPOSITION 1 On peut définir dans la théorie des δ-anneaux une suite unique d'opérations unaires $\delta_0,\delta_1,\delta_2,\ldots$ vérifiant les identités

$$f^n(x) = \delta_0(x)^{q^n} + p\delta_1(x)^{q^{n-1}} + \ldots + p^n\delta_n(x) \qquad (n\geq 0)$$

Les deux premiers termes de la suite sont $\delta_0(x) = x$ et $\delta_1(x) = \delta(x)$.

PROPOSITION 2 Il y a sur $\mathbb{Z}[Y_0,Y_1,Y_2,\ldots]$ une seule structure de δ-anneau pour laquelle $\delta_n(Y_0) = Y_n$ pour tout $n\geq 0$. Muni de cette structure, $\mathbb{Z}[Y_0,Y_1,Y_2\ldots]$ est un δ-anneau libre sur Y_0.

THEOREME 4 Si $q=p$ l'anneau W(A) s'identifie à l'anneau des vecteurs de Witt sur A.

A chaque élément $x\in W(A)$ correspondant un vecteur de Witt $\pi_A(x)\in A^{\mathbb{N}}$. La description de π_A est semblable à celle de γ_A mais elle utilise plutôt le δ-anneau libre $\mathbb{Z}[Y_0,Y_1,\ldots]$.

L'endofoncteur composé $\underline{A} \xrightarrow{W} \underline{\delta A} \xrightarrow{U} \underline{A}$ est une co-monade [6,3,2] sur $\underline{A}$. Pour simplifier, nous noterons encore ce foncteur par W. On a des transformations naturelles

$$W(A) \xrightarrow{\epsilon_A} A \qquad W(A) \xrightarrow{E_A} W(W(A))$$

satisfaisant à des conditions d'associativité et d'unité. L'homomorphisme E_A est étroitement relié à l'exponentielle de Artin-Hasse [3]. Une structure de δ-anneau sur A équivaut à une structure de co-algèbre [6] $\underline{\delta}: A \to W(A)$. Celle-ci se décrit comme suit: pour tout $x \epsilon A$ on a $\pi_A \underline{\delta}(x) = (\delta_0(x), \delta_1(x), \ldots)$.

Remarques

1) Soit A un anneau sans p-torsion muni d'un endomorphisme f tel que pour tout $x \epsilon A$, $f(x) \equiv x^q \bmod pA$. Le lemme de Dieudonné-Cartier [4, page 508] affirme l'existence d'un homomorphisme $s_f: A \to W(A)$. Ce résultat s'interprète comme suit dans le contexte présent: les hypothèses entraînent l'existence d'une structure de δ-anneau sur A et on vérifie que $s_f = \underline{\delta}$.

2) Sous les hypothèses de la remarque précédente, on donne une description particulièrement simple de W(A) [5]. Posons

$$B = \{(a_n) \epsilon A^N \mid a_{n+1} \equiv f(a_n) \bmod p^{n+1} \ \forall n\}$$

On vérifie que B est un sous-anneau de l'anneau produit A^N. L'opérateur de translation $t((a_n)) = (a_{n+1})$ est un endomorphisme de B et pour tout $x \epsilon B$,

$$t(x) \equiv x^q \bmod pB$$

Comme B est sans p-torsion, on a une structure de δ-anneau sur B pour laquelle t est l'endomorphisme de Frobenius. On vérifie ensuite directement

qu'avec la projection $B \to A$, B devient le δ-anneau co-libre sur l'anneau A, donc que $B=W(A)$.

Bibliographie

[1] Bourbaki. Algèbre, Chap. V, 11.

[2] Bourbaki. Algèbre, Chap. 8 et 9.

[3] M. Hazewinkel. Formal Groups and Applications. Academic Press Monographs 78, 1978.

[4] L. Illusie. Complexe de De Rham-Witt et cohomologie cristalline. Annales Scientifiques de l'Ecole Normale Supérieure. 4^0 série, t12, 1979, p. 501 à 661.

[5] M. Lazard. Commutative Formal Groups. Lect. Notes in Math. 443, Springer-Verlag.

[6] S. MacLane. Category theory for the working Mathematician. Graduate text in Math. 5, Springer Verlag.

[7] P. Ribenboim. L'Arithmétique des corps. Hermann, Paris 1972.

[8] D.O. Tall, G.C. Wraith. Representable Functors and Operations on Rings. Proceedings of the London Mathematical Society (3) 20 (1970) p. 619-643.

[9] G.C. Wraith. Algebras over theories. Colloquium Mathematicum. vol. XXIII (1971) fasc 2.

Département de Mathématiques
et d'informatique
Université du Québec à Montréal

Received March 28, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

ON FIELDS FOR WHICH THE NUMBER OF ORDERINGS IS DIVISIBLE BY A HIGH POWER OF 2

Ján Mináč

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

Abstract: We generalize the well known Bröcker-Brown's theorem about existence of a certain valuation on a superordered field with finitely many orderings to the fields which have the number of orderings divisible by a high power of 2.

1. Introduction; In this paper we keep to the notation used in [1], [2], [6]. Henceforth it is understood that we are treating only fields with finitely many orderings; and we adapt the standard theorems to our special case.

We define F to be a formally real field, T to be the set of elements in F that are the sum of non-zero squares of elements of F, $\dot{F}$ is the multiplicative group of the field F, $[\dot{F} : T]$ is the group index, v - a valuation on F, F_v - the residue field of v, U_v - the group of units of A_v, M_v - the maximal ideal of A_v.

v is strongly compatible with T iff $1 + M_v \subset T$.

The field F is of type $(k, 2^n)$ if $[\dot{F} : T] = 2^n$ and the number of orderings of the field F is k.

For each integer $n \geq 1$, we define the set $O(n)$ of natural numbers by the following recursive formula:

$$O(1) = \{1\}, \quad O(2) = \{2\}, \quad O(3) = \{3,4\} \ldots.$$

$$O(n) = 2\,O(n-1) \cup \{1 + O(n-1)\}$$

We note that if F is of the type $(h, 2^n)$ then $h \in O(n)$ (see [1])

An element ℓ of $O(n)$ is called decomposable if ℓ can be written as $a+b=\ell$, $a \in O(s)$, $b \in O(t)$, $s+t=n$. (we use the same abuse of notation as in [6]. (see p. 188)). Otherwise $\ell \in O(n)$ is called indecomposable. If $\ell \in O(n)$ is decomposable then $\ell-1 \in O(n-1)$ ([6], Proposition 2.6). If $k \in O(n)$, $k \geq n+1$ then $k \in O(n+1)$ ([6], Proposition 2.8). If $2k \in O(n)$, $k \geq n-1$ then $k \in O(n-1)$ [6], Proposition 2.11).

A set of different orderings $\{P_1,P_2,P_3,P_4\}$ of the field F is called a 4-element fan if $P_1 \cap P_2 \cap P_3 \subset P_4$. Two orderings $P,Q, P \neq Q$ of the field F are called equivalent if there exist orderings R, S of the field F such that the set $\{P,Q,R,S\}$ forms a 4-element fan of the field F.

2. A superordered field with finitely many orderings is of type $(2^{n-1},2^n)$, with $n \geq 1$. It is known that such a field F has a valuation v, strongly compatible with T, such that $[\dot{F}_v : T_v] \leq 4$ ([2]). The following theorem generalizes this:

Theorem 1: Let F be a field of a type $(2^{n-j}\, m, 2^n)$, where $n > 2j$, $m \geq 1$. Then there exists a non-trivial valuation v on F, strongly compatible with T, such that

$$[\dot{F}_v : T_v] = 2^s \leq 2^{2j}$$

Proof: Firstly we shall show that there exists a valuation u on F, strongly compatible with T, such that $\dot{F} \neq U_u \dot{F}^2$.

We know that if F is of the type $(k,2^n)$ where $k \in O(n)$, $k \geq 4$ with $k \in O(n)$ is indecomposable, then any two orderings of F are equivalent ([4], Theorem 3.3). But if F has only a finite number

of orderings, (at least four) of which any two are equivalent, then there exists a real valuation u on F such that $U_u \dot{F}^2 \neq \dot{F}$ ([5], Theorem (2.8)). Thus it is enough to prove that if $k = 2^{n-j} \cdot m \in 0(n)$, and $n > 2j$ then k is an indecomposable element of $0(n)$.

We shall prove this by induction on j.

1) Suppose $j = 1$. We observe that $m = 1$ as 2^{n-1} is the largest element of $0(n)$. If $2^{n-1} \in 0(n)$ is decomposable, then $2^{n-1} - 1 \in 0(n-1)$. But then $2^{n-1} - 1 \leq 2^{n-2}$ which gives $n \leq 2$. But by assumption $n > 2$ and so we established a contradiction.

2) We assume that our assertion holds for $j - 1$, but not for j. We assume $j \geq 2$. Thus there exists $n > 2j$, $m \in \mathbb{N}$ such that $k = 2^{n-j} m \in 0(n)$ is decomposable and so $k - 1 \in 0(n-1)$. Since $k - 1$ is odd we see that $k - 2 = 2(2^{n-j-1} m - 1) \in 0(n-2)$. But $2^{n-j-1} m - 1 - (n-3) \geq 2^{j-1} - 2j + 2 \geq 0$. Thus $2^{n-j-1} m - 1 \in 0(n-3)$. Hence $2^{(n-2)-(j-1)} m \in 0(n-2)$ is decomposable. But as $n - 2 > 2(j-1)$ this contradicts our assumption that the assertion is true for $j - 1$.

Hence $k \in 0(n)$ is indecomposable so that there exists a non-trivial valuation u on a field F, strongly compatible with T, such that $\dot{F} \neq U_u \dot{F}^2$.

We shall now conclude the proof using induction on n. Suppose that $n = 2j + 1$. We know that there exists a non-trivial valuation v on the field F, strongly compatible with T, such that $\dot{F} \neq U_v \dot{F}^2$. Hence $[\dot{F}_v : T_v] \leq 2^{2j}$. Thus the theorem is true for $n = 2j + 1$.

Now suppose that our assertion is true for n', where $2j < n' < n$. Let $2j < n$, $m \geq 1$ and let F be a field of type $(2^{n-j} \cdot m, 2^n)$ and u a valuation on F, strongly compatible with

T , such that $U_u\dot{F}^2 \neq \dot{F}$. We shall show that $U_u\dot{F}^2 = U_uT$. Indeed if $a_1,\dots,a_n \in \dot{F}$, let $a = a_i$ where $u(a_i) \leq u(a_k)$ for $k = 1,2,\dots,n$. Then

$$a_1^2 + \dots + a_n^2 = a^2\left(\left(\frac{a_1}{a}\right)^2 + \dots + \left(\frac{a_n}{a}\right)^2\right)$$

$$= a^2 b$$

where $b \in U_u$. (Here we use the fact that F_u is a formally real field). Hence

$$[\dot{F} : U_uT] = [\dot{F} : U_u\dot{F}^2] = 2^t \ , \ t \geq 1$$

Suppose now that F_u is of type $(g,2^h)$. Then we have

$$g = 2^{n-t-j} \cdot m \ , \ 2^h = 2^{n-t}$$

If $h \leq 2j$ we can take $v = u$.

If $h > 2j$, then since $h < n$ we can use our induction hypothesis on the field F_u , so that there exists a valuation w on F_u strongly compatible with T_u such that $[\dot{F}_w : T_w] = 2^s \leq 2^{2j}$. We take $v = u \circ w$ the standard composition of the valuations u , w . Then F_v is isomorphic to F_w so that $[F_v : T_v] = 2^s \leq 2^{2j}$. To show that v is strongly compatible with T let $c \in M_v$. Since the valuation w is strongly compatible with T_u , there must exist elements $a_1,\dots,a_n \in \dot{F}$ such that

$$a_1^2 + \dots + a_n^2 = (1+c)(1+d) \ ,$$

where d is some element from M_u .

Since u is strongly compatible with T , there exist elements $b_1,\dots,b_\ell \in \dot{F}$ such that $1+d = b_1^2 + \dots + b_\ell^2$. Hence $1+c$ is a sum of squares of the elements of F , which concludes the proof.

Remarks. As elements $2^j \in 0(2j)$, $j \geq 1$ are decomposable from theorem 4.1 [6] we get that theorem 1 does not hold if $n = 2j$.

Hence assumption $n > 2j$ is necessary. However, if we fix odd number $m \geq 3$ and investigate fields of a type $(2^{n-j}m, 2^n)$ we can get better results. To formulate it let us define (see [6], Def. 2.A.1, Proposition 2.A.4)

$$\mu(m) = t + \sum_{i=0}^{t} \epsilon_i \quad , \text{ where}$$

$$m = \sum_{i=0}^{t} \epsilon_i 2^i \quad , \ \epsilon_i \in \{0,1\} \quad , \ \epsilon_t = 1 \quad .$$

Theorem 2: Let F be a field of a type $(2^{n-j} \cdot m \ , \ 2^n)$ where m is an odd number ≥ 3 and $n > 2j-\mu(m)$. Then there exists a non-trivial valuation v on F , strongly compatible with T , such that

$$[\dot{F}_v : T_v] = 2^s \leq 2^{2j-\mu(m)}$$

Furthermore, one can observe that numbers $2^k m \in 0(\mu(m) + 2k)$, $k \geq 0$ are decomposable and hence condition $n > 2j-\mu(m)$ is necessary.

Moreover the following is true: Proposition: Suppose j,m are natural numbers, m is odd ≥ 3 . Then there exists natural number n such that $2^{n-j} \cdot m \in 0(n)$ iff $j \geq \mu(m)$.

Using our Theorems and results established in various papers (see e.g. [2], [3], [4], [5], [6], [7]) we are able to deduce the following.

Let F be a field of type $(2^{n-j}.m, 2^n)$. From Theorems 1,2 we know that there is a valuation v on F , strongly compatible with T , such that $[\dot{F}_v : T_v] = 2^s \leq 2^{2j}$ if $m = 1$ and $[\dot{F}_v : T_v] = 2^s \leq 2^{2j-\mu(m)}$ if m is an odd ≥ 3 . Moreover:

Corollary 1. Let $W_{red}(F)$ denote the reduced Witt ring of the field F . Then $W_{red}(F) \cong W_{red}(F_v)[H]$, where $W_{red}(F_v)[H]$ is a group ring and H is a 2-elementary abelian group of rank $n-s = \ell$.

Furthermore we assume that F is a Pythagorean field retaining

the above properties. Then

Corollary 2. F is quadratically equivalent to the field $F_v((t_1))\ldots((t_\ell))$, where $\ell = n-s$, with $t_1,\ldots,t_\ell$ indeterminates.

Corollary 3. The square class invariant (introduced by A. Solow (see [3]) classifies quadratic forms over F if and only if there exists a 2-henselian valuation u on F such that F_u is a SAP field and $[F_u : T_u] = 2^r \leq 2^{2j}$. Hence if $j = 1$ or 2 then the square class invariant classifies quadratic forms over F .

Corollary 4. There exists an exact split sequence of pro-2 groups

$$1 \to \mathbb{Z}_2^{\ell} \to G_2(F) \to \$ \to 1$$

where $\ell = n-s, G_2(F) = \mathrm{Gal}\,(F(2)/F)$. Here F(2) denotes the maximal 2-extension of F and $\mathbb{Z}_2$ is the additive group of 2-adic integers

1. L. Bröcker, Über die Anzahl der Anordnungen eines komutativen Körpers, Arch. Math. 29, (1977) 458-464.
2. T. Y. Lam, Orderings, Valuations and Quadratic Forms, CBMS VOL. 52, (1983).
3. T. Y. Lam and D. B. Shapiro, The Square Class Invariant for Pythagorean fields, Contemporary Math. Vol. 8, (1982), p. 327-340.
4. M. Marshall, Classification of finite spaces of orderings, Can. Math., Vol. XXXI, No. 2, (1979), pp. 320-330.
5. M. Marshall, Spaces of Orderings IV, Canad. J. Math. 32, (1980), 603-627.
6. J. Merzel, Quadratic forms over fields with finitely many orderings, Contemporary Math., Vol. 8, (1982), p. 185-229.
7. R. Ware, Quadratic forms and Pro-2-groups III. (Rigid elements and semidirect products.) Preprint No. 84017, Dept. of Math., Pennsylvania State University.

Acknowledgement: This paper has been written whilst pursuing a doctoral degree at Queen's University in Kingston. I am indebted to Professors Paulo Ribenboim and T. M. Viswanathan for their encouragement and suggestions. I would also like to thank Andrew Granville for making many helpful suggestions, some of them concerning this paper.

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

Received December 17, 1984

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

ON THE CLASSIFICATION OF NONCOMMUTATIVE TORI, II

Joachim Cuntz, George A. Elliott, F.R.S.C., Frederick M. Goodman,
Palle E. T. Jorgensen

Abstract. The classification of the canonical smooth subalgebras of the C*-algebras associated with pairs (G,ρ), where G is a finitely generated free abelian group and ρ is a nondegenerate antisymmetric bicharacter on G with generic Diophantine properties, 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 algebra. The invariant is expressed in terms of K-theory, with the help of Connes' cyclic cohomology.

1. Let G be a torsion-free abelian group and denote by $S(G)$ the space of complex-valued functions on G of rapid decay, i.e. the space of functions a on G such that the function $b^p a$ is summable for each linear function b on G (i.e. each $b \in \mathrm{Hom}(G,\mathbb{C})$) and each $p = 0,1,2,\ldots$.

Let $\rho: G\times G \to \mathbf{T}$ be a nondegenerate antisymmetric bicharacter on G, and denote by $A_{(G,\rho)}$ the C*-algebra introduced by Slawny in [8], - the unique prime C*-algebra generated by unitaries $(u_g)_{g\in G}$ such that for each $g,h \in G$,

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

$A_{(G,\rho)}$ is simple and has a unique tracial state τ. For brevity we will often write $A_{(G,\rho)} = A_\rho$.

Denote by A_ρ^∞ the subspace of A_ρ consisting of all elements a such that the function $(\tau(a\, u_g^{-1}))_{g\in G}$ belongs to $S(G)$. A_ρ^∞ is a subalgebra of A_ρ, and is a complete locally convex topological algebra with respect to the seminorms

$$\|a\|_{b,p} = \sum_{g\in G} |b(g)^p \tau(a\, u_g^{-1})|$$

where $b \in \mathrm{Hom}(G,\mathbb{C})$ and $p = 0,1,2,\ldots$.

Consider the category of all such pairs (G,ρ) (i.e. with G a torsion-free abelian group and $\rho: G\wedge G \to \mathbb{T}$ a nondegenerate antisymmetric bicharacter), with isomorphisms as maps. By an isomorphism of pairs (G,ρ) and (G',ρ') is meant a group isomorphism $\alpha: G \to G'$ such that $\rho'(\alpha\wedge\alpha) = \rho$. The correspondence

$$(G,\rho) \mapsto A^{\infty}_{(G,\rho)}$$

is clearly a functor to the category of algebras $A^{\infty}_{(G,\rho)}$ with algebra isomorphisms. We wish to construct an inverse to this functor, but we can do this only for the subcategory of pairs (G,ρ) such that G is finitely generated and ρ has generic Diophantine properties: for each $g \in G$ there exists $b \in \mathrm{Hom}(G,\mathbb{C})$ and $p = 0,1,2,\ldots$ such that

$$|\rho(g\wedge h)-1|^{-1} \leq |b(h)|^{p} \quad \text{whenever} \quad \rho(g\wedge h) \neq 1 .$$

Theorem. The functor $(G,\rho) \mapsto A^{\infty}_{(G,\rho)}$ restricted to pairs (G,ρ) such that G is finitely generated and ρ has generic Diophantine properties has an inverse (with respect to isomorphisms).

2. It would be desirable to formulate the invariant in the category of the C*-algebras $A_{(G,\rho)}$, rather than that of the algebras $A^{\infty}_{(G,\rho)}$, as was done in [4] in the opposite extreme case in which ρ has only values of finite order (the case of maximal degeneracy).

In fact, we do define the invariant in terms of the K-group $K_*(A^{\infty}_{\rho})$, which is the same as $K_*(A_{\rho})$, but we need the $\mathbb{Z}^+$-filtered structure of this group described in [5]. This filtered structure is not known to be invariant under C*-algebra isomorphisms. To prove that it is invariant under smooth isomorphisms, i.e. at the level of the subalgebra A^{∞}_{ρ} (at least for generic ρ), we use the cyclic cohomology of this algebra, defined by Connes in [3].

3. In the case $G = \mathbb{Z}^2$, our result goes beyond the classification result of Rieffel, [7], and Pimsner and Voiculescu, [6]. It implies that the determinant of

the automorphism of the K_1-group $\mathbb{Z}^2$ induced by an automorphism of the algebra $A^{\infty}_{(\mathbb{Z}^2,\rho)}$ is equal to $+1$. Here ρ is nondegenerate, i.e., of infinite order. In the case $G = \mathbb{Z}^2$ we do not need to assume that ρ has generic Diophantine properties. However, we cannot yet deal with arbitrary automorphisms of the C*-algebra $A_{(\mathbb{Z}^2,\rho)}$. The assertion to the contrary made in [5] (page 178, lines 17 to 20) must be withdrawn.

4. Lemma. Any isomorphism $A^{\infty}_{(G,\rho)} \to A^{\infty}_{(G',\rho')}$ where G and G' are countable is continuous and preserves the trace τ.

Proof. The proof of Theorem 3.1 of [1] shows that every derivation of A^{∞}_{ρ} is continuous. A similar argument shows that every isomorphism from A^{∞}_{ρ} to $A^{\infty}_{\rho'}$ is continuous.

Let us show that τ is the unique continuous linear functional on A^{∞}_{ρ} such that $\tau(1) = 1$ and $\tau(ab) = \tau(ba)$. It is enough to show that if $\omega(ab) = \omega(ba)$ then $\omega(u_g) = 0$ for all $g \neq 0$. If $g \neq 0$, then $\rho(g\wedge h) \neq 1$ for some $h \in G$, and

$$\omega(u_g) = \omega(u_h u_g u_h^{-1}) = \omega(\rho(g\wedge h)u_g) = \rho(g\wedge h)\omega(u_g) \quad .$$

5. Lemma. Let δ be an approximately inner derivation of $A^{\infty}_{(G,\rho)}$, with respect to the C*-algebra norm. If G is finitely generated and ρ has generic Diophantine properties then δ is inner.

Proof. The case $G = \mathbb{Z}^2$ is dealt with in Remark 4.3 of [1]. The case $G = \mathbb{Z}^k$ is similar: δ is determined by $d \in A^{\infty}_{(G,\rho)}$ where

$$d(g) = (\rho(g\wedge h)-1)^{-1}\, c^h(g) \quad , \quad \text{for any } h \text{ with } \rho(g\wedge h) \neq 1 \, .$$

Here, as in Theorem 2.1 of [1], $\delta(u_g) = \Sigma_{h\neq 0}\, c^g(h) u_g u_h$.

6. Note that if $\delta_1,\ldots,\delta_n$ are mutually commuting derivations of an algebra annihilating the trace τ, then

$$\tau_\delta(a_0,a_1,\ldots,a_n) = \Sigma_{\sigma\in S_n}\, \varepsilon(\sigma)\tau(a_0\delta_{\sigma(1)}(a_1)\ldots\delta_{\sigma(n)}(a_n))$$

is a cyclic cocycle in the sense of [3].

Recall that in $A^\infty_{(G,\rho)}$ (with ρ nondegenerate) every derivation annihilates the unique tracial state τ (see Corollary 2.2 of [1]).

Corollary. Let $\delta_1,\ldots,\delta_n$ be mutually commuting derivations of $A^\infty_{(G,\rho)}$, and let $\delta_1',\ldots,\delta_n'$ be mutually commuting derivations of $A^\infty_{(G,\rho)}$ such that $\delta_i' = \delta_i + \bar{\delta}_i$ where $\bar{\delta}_i$ is approximately inner in the C*-algebra norm. If G is finitely generated and ρ has generic Diophantine properties then the cyclic cocycles τ_δ and $\tau_{\delta'}$ define the same cyclic cohomology class.

Proof. By Lemma 5 there exist $b_1,\ldots,b_n \in A^\infty_{(G,\rho)}$ such that $\bar{\delta}_i = \text{ad } b_i$.

Using only the derivation law for $\delta_1,\ldots,\delta_{n-1}$ one sees that the Hochschild n-cochain

$$\tau(a_0\delta_1(a_1)\ldots\delta_{n-1}(a_{n-1})[b_n,a_n])$$

is the coboundary of the (n-1)-cochain

$$\tau(a_0\delta_1(a_1)\ldots\delta_{n-1}(a_{n-1})b_n) \quad .$$

Repeating this with obvious substitutions and summing yields a Hochschild (n-1)-cochain φ with coboundary equal to $\tau_{\delta'} - \tau_\delta$.

Integrating by parts and using the commutation relations

$$[\delta_i,\delta_j] = 0 = [\delta_i',\delta_j']$$

one verifies that the cochain φ constructed in this way is cyclic. The only step which need be noted is that, as the centre of $A^\infty_{(G,\rho)}$ is the scalars and all derivations annihilate τ (see above), the relation $[\delta_i,\delta_j] = [\delta_i',\delta_j']$ may be expressed as

$$\delta_i(b_j) - \delta_j(b_i) + [b_i,b_j] = 0 \quad .$$

7. For each $X \in \text{Hom}(G,\mathbb{C})$ there is a derivation δ_X of $A^\infty_{(G,\rho)}$ specified by $\delta_X(u_g) = X(g)u_g$, $g \in G$. Since these derivations form a commutative Lie algebra,

one may identify the exterior algebra $\Lambda\,\mathrm{Hom}(G,\mathbb{C})$ with the space of cyclic cocycles τ_δ as above with $\delta = (\delta_{X_1},\ldots,\delta_{X_n})$.

Theorem. For pairs (G,ρ) such that G is finitely generated and ρ has generic Diophantine properties, the map from $\Lambda\,\mathrm{Hom}(G,\mathbb{C})$ into the cyclic cohomology of $A^\infty_{(G,\rho)}$ is natural (with respect to isomorphisms).

Proof. We must show that for each algebra isomorphism $\alpha\colon A^\infty_{(G,\rho)} \to A^\infty_{(G',\rho')}$ the induced isomorphism of cyclic cohomology determines an isomorphism of exterior algebras $\Lambda\,\mathrm{Hom}(G',\mathbb{C}) \to \Lambda\,\mathrm{Hom}(G,\mathbb{C})$.

First we define a map $\beta\colon \mathrm{Hom}(G',\mathbb{C}) \to \mathrm{Hom}(G,\mathbb{C})$ as follows. If $X \in \mathrm{Hom}(G',\mathbb{C})$, by Theorem 2.1 of [1] there exists a unique $\beta(X) \in \mathrm{Hom}(G,\mathbb{C})$ such that the derivation $\alpha^{-1}\delta_X\alpha - \delta_{\beta(X)}$ of $A^\infty_{(G,\rho)}$ is approximately inner, i.e., by Lemma 5, inner. Since α preserves innerness, it is clear that β is an isomorphism.

By Lemma 4, $\tau = \tau\alpha^{-1}$. Hence if $\delta = (\delta_{X_1},\ldots,\delta_{X_n})$ with $X_i \in \mathrm{Hom}(G',\mathbb{C})$, the transform of the cyclic cocycle τ_δ on $A^\infty_{(G',\rho')}$ by α is $\tau_{\alpha^{-1}\delta\alpha}$ where $\alpha^{-1}\delta\alpha = (\alpha^{-1}\delta_{X_1}\alpha,\ldots,\alpha^{-1}\delta_{X_n}\alpha)$. By Corollary 6, $\tau_{\alpha^{-1}\delta\alpha}$ defines the same cyclic cohomology class as $\tau_{\beta(\delta)}$, where $\beta(\delta) = (\delta_{\beta(X_1)},\ldots,\delta_{\beta(X_n)})$. This shows that the extension of β to an isomorphism $\Lambda\,\mathrm{Hom}(G',\mathbb{C}) \to \Lambda\,\mathrm{Hom}(G,\mathbb{C})$ is compatible with the action of α on cyclic cohomology, as desired.

8. Proof of Theorem 1. By Proposition 14 of [3], $\Lambda\,\mathrm{Hom}(G,\mathbb{C})$ is in duality with the group $K_*(A^\infty_{(G,\rho)})$. By Theorem 7 this duality is natural with respect to algebra isomorphisms. It is straightforward to check that this duality factorizes through the Chern character $K_*(A^\infty_{(G,\rho)}) \to \Lambda_{\mathbf{R}}G$ defined in [2], and computed in [5]. Hence the $\mathbb{Z}^+$-filtered structure of $K_*(A^\infty_{(G,\rho)})$ derived from $\Lambda_{\mathbf{R}}G$ is invariant under algebra isomorphisms, and the identification of the relative quotients as Λ^nG, $n = 0,1,2,\ldots$, is natural. By Theorem 3.1 of [5], the restriction of $\exp 2\pi i\tau$ to Λ^2G, which makes sense since $\tau(1) = 1$, is equal to ρ. This identifies $\rho\colon G\wedge G \to \mathbf{T}$ as an invariant of $A^\infty_{(G,\rho)}$.

Acknowledgements. This research was partially supported by the Centre National de la Recherche Scientifique (France), the Danish Natural Science Research Council, the Natural Sciences and Engineering Research Council of Canada, and the National Science Foundation (U.S.A.).

References

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

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

3. A. Connes, Non commutative differential geometry, Chapter II: de Rham homology and non commutative algebra, preprint, IHES, 1983.

4. S. Disney, G. A. Elliott, A. Kumjian, and I. Raeburn, On the classification of noncommutative tori, C. R. Math. Rep. Acad. Sci. Canada 72(1985),137-142.

5. 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.

6. 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.

7. M. A. Rieffel, C*-algebras associated with irrational rotations, Pacific J. Math. 93 (1981), 415-429.

8. J. Slawny, On factor representations and the C*-algebra of canonical commutation relations, Comm. Math. Phys. 24 (1972), 151-170.

J. C.: Département de Mathématiques, Faculté des Sciences de Luminy, Case 901, F-13288 Marseille Cédex 9

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

F. M. G. and P. E. T. J.: Department of Mathematics, University of Iowa, Iowa City, Iowa 52242

Received January 7, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

SUR LA CONNEXION ENTRE UNE ÉQUATION FONCTIONNELLE ET L'ÉQUATION DIFFÉRENTIELLE DES FONTIONS ELLIPTIQUES JACOBIENNES

I. FENYÖ - L. PAGANONI

Présentée par J. Aczél, F.R.S.C.

RÉSUMÉ. Si (f,g) est une paire de fonctions analytiques définies dans un entourage de l'origine et satisfaisantes à l'équation fonctionnelle (1) sous les conditions initiales (2) et f' n'est pas une constante, alors f satisfait aussi à une équation différentielle de la forme (3). Aussi l'inverse de cette proposition est vrai, ce qui dérive d'un théorème démontrè en [1] .

1. Dans un travail précedent [1] nous avons déterminé toutes les paires (f,g) de fonctions analytiques définies dans un entourage de l'origine satisfaisantes à l'équation fontionnelle :

$$(1) \quad g(z_1+z_2) - g(z_1) - g(z_2) = f(z_1)f(z_2)f(z_1+z_2) \qquad (z_1,z_2 \in \mathbb{C}).$$

Plus précisement nous avons démontré le

Théorème ([1]) . *Soit (f,g) une paire de fonctions analytiques, definies dans un entourage de l'origine, satisfaisante à l'equation fonctionnelle (1). Alors :*

a) si $f(0) \neq 0$, *ils existent des constantes (complexes)* α *et* γ *telles que* $f(z) = \alpha$, $g(z) = -\alpha^3 + \gamma z$ $(z \in \mathbb{C})$

b) si $f(0) = 0$ *et* $f'(z) = \alpha$ *(constante) pour chaque* $z \in \mathbb{C}$, *alors il existe un nombre* $\gamma \in \mathbb{C}$ *tel que*

$$f(z) = \alpha z \quad , \quad g(z) = (\alpha^3/3)z^3 + \gamma z$$

c) si $f(0) = 0$ *et* f' *diffère d'une constante alors ils existent des nombres complexes* $\alpha \neq 0$, $\beta \neq 0$, γ *et* k *tels que*

$$f(z) = \alpha\, sn(\beta z,k) \quad , \quad g(z) = \alpha^3 \int_0^{\beta z} sn^2(t,k)\, dt + \gamma z \, .$$

Ici $sn(u,k)$ désigne la fonction elliptique de Jacobi et la courbe d'integration dans l'expression de $g(z)$ ne traverse aucun pôle de $sn(u,k)$.

Nous désignerons maintenant par A la classe des fonctions analytiques definies dans un entourage de l'origine pour lesquelles il existe une fonction analytique g(z) de sorte que la paire (f,g) soit une solution de (1). Si $f \in A$ et f' n'est pas une constante,alors, grâce au théorème cité en haut, f a les propriétés suivantes : $f(0) = 0$ et $f'(0) \neq 0$; c'est pour cela qu'on peut considérer, sans réstriction de la généralité, la sous-classe A_o de A de toutes les fonctions $f \in A$ satisfaisantes aux conditions

$$f(0) = 0 \quad , \quad f'(0) = 1 \tag{2}$$

et pour lesquelles f' n'est pas une constante.

Notre théorème cité en haut signifie que A_o ne contient que les fonctions de la forme

$$f(z) = \alpha\, sn(z/\alpha,k) \qquad (\alpha,k \text{ arbitraires}, \alpha \neq 0).$$

Il est bien connu, d'autre part, que la classe de ces fonctions-ci représente exactement les solutions de la famille des équations différentielles

$$(f')^2 = \left(1 - \frac{f^2}{\alpha^2}\right)\left(1 - \frac{k^2}{\alpha^2} f^2\right) \qquad (\alpha,k \in \mathbb{C},\ \alpha \neq 0) \tag{3}$$

qui possèdent les propriétés (2).

Donc il est naturel de se poser la question s'il est possible dériver (3) *directement* de (1),sans recours à la solution générale de (1). En [1] nous avons déjà dérivé de (1) une equation différentielle de deuxième ordre ((4) ci-dessous), mais il est différente de (3). Ici nous montrons comment (3) suit de (4).

2. Soit donc $f \in A_o$. Comme nous avons montré dans [1] , si on dérive (1) une fois selon la variable z_1 , deux fois selon la variable z_2 et on pose $z_1=z=-z_2$, alors on arrive à l'équation différentielle du deuxième ordre pour la fonction f considerée :

$$ff'' - 2(f')^2 + f'''(0)f^2 + 2 = 0 \quad . \tag{4}$$

$f'''(0)$ est une constante, un paramètre; ici il sera avantageux d'écrire cette constante dans la forme

$$f'''(0) = -(1+k^2)/\alpha^2 \tag{5}$$

où α ($\alpha \neq 0$) et k sont des nombres (complexes) arbitraires.

Nous allons maintenant introduire une fonction auxiliaire ϕ :

$$\phi = (f')^2 - \left(1 - \frac{1}{\alpha^2} f^2\right)\left(1 - \frac{k^2}{\alpha^2} f^2\right) = \tag{6}$$

$$= (f')^2 - 1 + \frac{1 + k^2}{\alpha^2} f^2 - \frac{k^2}{\alpha^4} f^4 \quad .$$

En dérivant ϕ et en multipliant ϕ' par f, on obtien:

$$f\phi' = 2f'\left[ff'' + \frac{1+k^2}{\alpha^2}f^2 - 2\frac{k^2}{\alpha^4} f^4\right] . \tag{7}$$

On peut écrire la relation (4) dans la forme :

$$ff'' + \frac{1+k^2}{\alpha^2} f^2 - 2\frac{k^2}{\alpha^4} f^4 = \tag{8}$$

$$= 2(f')^2 - 2 + 2\frac{1+k^2}{\alpha^2} f^2 - 2\frac{k^2}{\alpha^4} f^4 \quad ,$$

d'ou, en tenant compte de (6) et de (7), on obtien

$$f\phi' = 4f'\phi \quad . \tag{9}$$

De (9) on déduit

$$\phi = c\, f^4 \qquad (c \in \mathbb{C} \text{ arbitraire}) \; . \tag{10}$$

En substituant cette expression au première membre de (6), on reconnait immédiatement que f satisfait à la suivante èquation différentielle :

$$(11) \qquad (f')^2 = 1 - \frac{1+k^2}{\alpha^2} f^2 + \left(\frac{k^2}{\alpha^4} + c\right) f^4 \quad .$$

On doit remarquer que l'hypothèse selon laquelle f' n'est pas une constante implique que les coefficients

$$\beta = \frac{1+k^2}{\alpha^2} \qquad \text{et} \qquad \gamma = \frac{k^2}{\alpha^4} + c$$

ne s'annulent pas simultanément et c'est pour ça qu'il est toujours possible de determiner deux paramètres $\tilde{\alpha}$ ($\neq 0$) et $\tilde{k}$ tels que

$$(12) \qquad \frac{1+k^2}{\alpha^2} = \frac{1+\tilde{k}^2}{\tilde{\alpha}^2} \qquad \text{et} \qquad \frac{k^2}{\alpha^4} + c = \frac{\tilde{k}^2}{\tilde{\alpha}^4} \quad .$$

En effet, de (12) suit l'équation

$$\gamma\tilde{\alpha}^4 - \beta\tilde{\alpha}^2 + 1 = 0$$

pour $\tilde{\alpha}$, qui a toujours des solutions (complexes) puisque $|\beta| + |\gamma| \neq 0$; après on peut déterminer aussi $\tilde{k}$.

En remplaçant ces expressions dans (11) on obtient l'équation différentielle

$$(13) \qquad (f')^2 = 1 - \frac{1+\tilde{k}^2}{\tilde{\alpha}^2} f^2 + \frac{\tilde{k}^2}{\tilde{\alpha}^4} f^4 = \left(1 - \frac{1}{\tilde{\alpha}^2} f^2\right)\left(1 - \frac{\tilde{k}^2}{\tilde{\alpha}^2} f^2\right) \quad .$$

Cette équation a la même forme que l'équation (3), mais avec de différents coefficients.

On en conclut donc que, si $f \in A_o$, alors de (4) dérive (3). D'autre part (4) est une conséquence de (1). Cela signifie que pour chaque fonction f de la classe A_o on peut faire correspondre une équation différentielle du type (3).

Aussi l'inverse de cette affirmation est vrai, parce que, grâce au Théorème([1]), chaque intégrale d'une équation différentielle du type (3) avec la condition initiale (2) est un membre de la classe A_o.

On a donc le

Théorème. *L'inclusion* $f \in A_o$ *est valable si et seulement si* f *est un intégrale d'une équation différentielle de la forme (3) avec la condition initiale (2).*

Bibliographie

[1] Fenyö, I. - Paganoni, L. : Su una equazione funzionale proveniente dalla teoria delle funzioni ellittiche jacobiane. Rend. Mat. (sous presse).

Stromfel Aurél u. 27
H-1124 Budapest
Hungary

Dipartimento di Matematica
Università degli Studi di Milano
Via C. Saldini 50
I-20133 Milano, Italy

Received February 7, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

CHARACTERIZATION OF AN AFFINE CONFORMAL VECTOR FIELD

R. Sharma and K.L. Duggal*

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

Abstract: Yano [4] has shown that an affine conformal vector field on a compact orientable Riemannian manifold without boundary is a conformal vector field. The purpose of this paper is to characterize an affine conformal vector field over an arbitrary semi-Riemannian manifold and describe it geometrically. We also give an example of an affine conformal vector field other than a conformal vector field.

1. Characterization. Let (M,g) denote an n-dimensional smooth semi-Riemannian manifold endowed with a metric tensor g of arbitrary signature and corresponding Levi-Civita connection ∇. All the geometric objects on M are assumed smooth. A vector field ξ on M is said to be conformal, if $\pounds_\xi g = 2\rho g$, where ρ is a scalar function and $\pounds_\xi$ denotes Lie-derivative operator via ξ. We shall denote arbitrary vector fields on M by X,Y and Z.

Definition: A vector field ξ on M is said to be affine conformal if

$$(\pounds_\xi \nabla)(X,Y) = (X\rho)Y + (Y\rho)X - g(X,Y)\ \text{grad}\ \rho \qquad (1.1)$$

It is well-known [4] that a conformal vector field is also affine conformal, but the converse holds when M is a compact

* Research supported by NSERC of Canada

orientable Riemannian manifold without boundary. We prove the following:

Theorem 1.1. A vector field ξ on a semi-Riemannian manifold (M,g) is affine conformal iff the strain tensor $\mathcal{L}_\xi g$ is equal to $2\rho g$ plus a symmetric parallel tensor h of type $(0,2)$.

Proof: We follow the setting $\nabla_X Y = \nabla(X,Y)$. The commutation of the operators $\mathcal{L}_\xi$ and ∇_X is given by

$$\mathcal{L}_\xi \nabla_X Y - \nabla_X \mathcal{L}_\xi Y = (\mathcal{L}_\xi \nabla)(X,Y) + \nabla_{[\xi,X]} Y \tag{1.2}$$

As shown in [3], $(\nabla_X \mathcal{L}_\xi g)(Y,Z) = g(Y, \mathcal{L}_\xi \nabla_X Z - \nabla_X \mathcal{L}_\xi Z)$
$+ g(Z, \mathcal{L}_\xi \nabla_X Y - \nabla_X \mathcal{L}_\xi Y) - [\xi,X] g(Y,Z)$

Using (1.2) in the above equation, we get

$$(\nabla_X \mathcal{L}_\xi g)(Y,Z) = g(Y, (\mathcal{L}_\xi \nabla)(X,Z)) + g(Z, (\mathcal{L}_\xi \nabla)(X,Y)) \tag{1.3}$$

Now let ξ be affine conformal. Then use of (1.1) in (1.2) implies $(\nabla_X \mathcal{L}_\xi g)(Y,Z) = 2(X\rho) g(Y,Z)$. Thus $\nabla_X (\mathcal{L}_\xi g - 2\rho g) = 0$. Hence $\mathcal{L}_\xi g = 2\rho g + h$, where h is a symmetric parallel tensor field of type $(0,2)$. Conversely, if $\mathcal{L}_\xi g = 2\rho g + h$; where h is parallel, then (1.3) implies $(g(Y, (\mathcal{L}_\xi \nabla)(X,Z)) + g(Z, (\mathcal{L}_\xi \nabla)(X,Y)) = 2(X\rho) g(Y,Z)$ whence one readily obtains $g(Z, (\mathcal{L}_\xi \nabla)(X,Y)) = (X\rho) g(Y,Z) + (Y\rho) g(X,Z) - g(X,Y) Z\rho$. Hence (1.1) follows which completes the proof.

2. Geometrical Description. Let $\{\phi_\varepsilon : \varepsilon =$ an infinitesimal real parameter$\}$ be the 1-parameter group of local transformations generated by the affine conformal vector field ξ. Then the

equation $\pounds_\xi g = 2\rho g + h$ and its equivalent equation (1.1) can be expressed as:

$$g' = (1 + 2\varepsilon\rho)g + \varepsilon h \tag{2.1}$$

$$\nabla'_X Y = \nabla_X Y + \varepsilon\{(X\rho)Y + (Y\rho)X - g(X,Y)\text{grad } \rho\} \tag{2.2}$$

where $g'(X,Y) = g(d\phi_\varepsilon X, d\phi_\varepsilon Y)$ and $\nabla'_X Y = \nabla_{d\phi_\varepsilon X} d\phi_\varepsilon Y$; $d\phi_\varepsilon$ denoting the Jacobian differential of ϕ_ε. It follows from (2.1) that (i) A null vector field U will be transformed by ϕ_ε into a null vector field iff $h(U,U) = 0$, (ii) A non-null vector field retains its causal character (space-like or time-like) [2] under ϕ_ε. In general; ϕ_ε is not angle preserving. In particular, two orthogonal vector fields U and V will be transformed into orthogonal vector fields $d\phi_\varepsilon U$ and $d\phi_\varepsilon V$ iff $h(U,V) = 0$.

Now it is well-known [1] that, under an infinitesimal conformal transformation a geodesic does not, in general, remain a geodesic unless it is null and in this case the transformed geodesic is again null. Let us consider the analogous situation in the case of infinitesimal affine conformal transformation ϕ_ε. Suppose U denotes the tangent vector field to a geodesic in (M,g), which is transformed into a geodesic in (M,g'). Therefore $\nabla_U U = \nabla'_U U = 0$. Hence (2.2) implies $2(U\rho)U = g(U,U)\text{grad } \rho$ which gives rise to two possibilities; either (i) ρ = constant, or (ii) $g(U,U) = 0$ and $U\rho = 0$. Case (i) reduces ξ to an affine Killing vector field which is trivial. Case (ii) asserts that a geodesic does not, in general, remain a geodesic unless it is null (like infinitesimal conformal transformation) and tangent to the level hypersurface,

ρ = constant, of M. But the transformed geodesic will not be null, unless $h(U,U) = 0$ (unlike infinitesimal conformal transformation).

3. A Non-trivial Example. Consider a non-degenerate submanifold (M,g) of a semi-Riemannian manifold $(\bar{M},g)$, defined by an isometric imbedding. Then the metric on M is the restriction of the metric g on $\bar{M}$, to M. Consider a conformal vector field V on $\bar{M}$. V can be decomposed uniquely into its tangential part ξ and normal part ν. As V is a conformal vector field on $\bar{M}$ we have $(\pounds_{\xi+\nu}g)(X,Y) = 2\rho g(X,Y)$. Hence $(\pounds_{\xi}g)(X,Y) = 2\rho g(X,Y) - g(\bar{\nabla}_X\nu,Y) - g(X,\bar{\nabla}_Y\nu)$, where $\bar{\nabla}$ is the Levi-Civita connection of $\bar{M}$. Application of Weingarten's formula to the foregoing equation provides $(\pounds_{\xi}g)(X,Y) = 2\rho g(X,Y) + 2g(II_\nu X,Y)$, where II_ν stands for the second fundamental form of M corresponding to the normal vector field ν. Suppose II_ν is parallel. Then define a $(0,2)$-symmetric tensor h on M such that $2g(II_\nu X,Y) = h(X,Y)$. Consequently we obtain $\pounds_\xi g = 2\rho g + h$, where h is parallel. Hence ξ is an affine conformal vector field on M.

Remark 1. In the above example, for a totally umbilical submanifold (M,g) the vector field ξ would reduce to a conformal vector field.

Remark 2. In the above example, if (M,g) were taken as a compact orientable Riemannian submanifold of the semi-Riemannian manifold $(\bar{M},g)$ then (M,g) would reduce to a totally geodesic submanifold, such that the tangential part of V would reduce to a conformal vector field on (M,g).

Acknowledgement. We are thankful to the referee whose valuable suggestions improved the paper.

REFERENCES

[1] S.W. Hawking and G.F.R. Ellis, The large scale structure of space-time, Cambridge University Press, London, 1973.

[2] B. O'Neill, Semi-Riemannian geometry, Academic Press, New York, 1983.

[3] R. Sharma, A relation between an affine Killing vector and the strain tensor of a pseudo-Riemannian manifold, C.R. Math. Acad. Sci. Canada 4(1982), 305-307.

[4] K. Yano, Integral formulas in Riemannian geometry, Marcel Dekker, New York, 1970.

Department of Mathematics,
University of Windsor,
Windsor, Ontario,
N9B 3P4, Canada.

Received February 20, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

ASSOCIATIVE OPERATIONS CLOSE TO A GIVEN ONE

C.Alsina (Barcelona) and R.Ger (Katowice)

Presented by J. Aczél, F.R.S.C.

Given two bijections f and g from $[0,\infty)$ onto $[0,\infty)$ we can generate the following associative operations:

$$F(x,y) = f^{-1}(f(x) + f(y)) \quad \text{and} \quad G(x,y) = g^{-1}(g(x) + g(y)).$$

In this case we call f and g additive generators of F and G, respectivily, and it is not hard to check that they are unique up to a multiplicative positive constant; in particular, if $\alpha,\beta > 0$ then F and G are also generated by αf and βg, respectively. Then a natural question arises: if F and G are uniformly close can we deduce that at least two of their corresponding generators will be also uniformly close?,i.e., given $\varepsilon > 0$ and the condition:

$$|F(x,y) - G(x,y)| < \varepsilon \quad \text{for all } x,y \text{ in } [0,\infty),$$

are there positive constants α and β such that

$$|\alpha f(x) - \beta g(x)| < \varepsilon \quad \text{for all } x \text{ in } [0,\infty)?.$$

The aim of this paper is to give, under some additional assumptions, an affirmative answer to this problem. In the case $g(x)=x$ and $G(x,y)= x + y$ this leads to a special case of the celebrated Hyers' inequality ([2]).

LEMMA 1. *Given $\varepsilon>0$ then, if a function ϕ from $[0,\infty)$ into itself satisfies the inequality*

$$(1) \qquad |\phi(x + y) - \phi(x) - \phi(y)| \leq \varepsilon \quad \text{for all } x,y \text{ in } [0,\infty),$$

then there exists an additive function a from $\mathbb{R}$ into $\mathbb{R}$ such that

(2) $|\phi(x) - a(x)| \leq \varepsilon$ for all x in $[0,\infty)$.

The proof of this lemma is a straightforward modification of the classical result of Hyers ([2]), so will be omited here.

LEMMA 2. Given $\varepsilon>0$, let g be a bijective function from $[0,\infty)$ into $[0,\infty)$ such that, for some positive constant M, the inequality

$$|g(x) - g(y)| \leq M\,|x-y|$$

holds for all x,y in $[0,\infty)$. If a bijective function f from $[0,\infty)$ into $[0,\infty)$ satisfies

(3) $|f^{-1}(f(x)+f(y)) - g^{-1}(g(x)+g(y))| \leq \varepsilon$ for all x,y in $[0,\infty)$,

then the function $\phi = g \circ f^{-1}$ satisfies the inequality

(4) $$|\phi(x+y) - \phi(x) - \phi(y)| \leq M\,\varepsilon\,.$$

Proof. For all x and y in $[0,\infty)$ we have the following:

$$\begin{aligned}
|\phi(x+y)-\phi(x)-\phi(y)| &= |g(f^{-1}(x+y))-g(f^{-1}(x))-g(f^{-1}(y))| \\
&= |g(f^{-1}(x+y))-g[g^{-1}(g(f^{-1}(x))+g(f^{-1}(y)))]| \\
&\leq M|f^{-1}(x+y)-g^{-1}(g(f^{-1}(x))+g(f^{-1}(y)))| \\
&= M.|f^{-1}(f(f^{-1}(x))+f(f^{-1}(y)))- \\
&\quad -g^{-1}(g(f^{-1}(x))+g(f^{-1}(y)))| \\
&\leq M\,.\varepsilon\,.
\end{aligned}$$

Now we will prove the main result:

THEOREM 1. Given $\varepsilon>0$, let g be a bijective lipschitzian function from $[0,\infty)$ into $[0,\infty)$. Suppose that a one-to-one function f from $[0,\infty)$ onto itself is such that

(5) $|f^{-1}(f(x)+f(y))-g^{-1}(g(x)+g(y))| \leq \varepsilon$ for all x,y in $[0,\infty)$

and f satisfies one of the following conditions:

(i) f is strictly monotonic;

(ii) f^{-1} is mesurable;

(iii) f^{-1} is bounded on a set of positive measure.

Then there exist two non-negative constants α and β such that

$$|\alpha f(x) - \beta g(x)| \leq \varepsilon \quad \text{for all } x \text{ in } [0,\infty) \tag{6}$$

Proof. Let $M > 0$ be such that $|g(x)-g(y)| \leq M|x-y|$ for all x,y in $[0,\infty)$.

Applying Lemma 2, the function $\phi = g \circ f^{-1}$ satisfies

$$|\phi(x+y) - \phi(x) - \phi(y)| \leq M\varepsilon \quad \text{for all } x,y \geq 0.$$

Thus, by Lemma 1, there exists an additive function a from $\mathbb{R}$ into $\mathbb{R}$ such that

$$|\phi(x) - a(x)| \leq M\varepsilon \quad \text{for all } x \geq 0.$$

Hence, for all $x \geq 0$, we have

$$-M\varepsilon \leq a(x) - g(f^{-1}(x)) \leq M\varepsilon,$$

or, equivalently,

$$-M\varepsilon \leq g(f^{-1}(x)) - M\varepsilon \leq a(x) \leq g(f^{-1}(x)) + M\varepsilon.$$

From this and the hypothesis on f it follows immediately that a is continuous and, since it is also additive, there must be a nonnegative constant λ such that $a(x) = \lambda x$. Consequently

$$|g(f^{-1}(x)) - \lambda x| < M\varepsilon \quad \text{for all } x > 0,$$

and, taking $\alpha = \lambda/M$ and $\beta = 1/M$, we obtain the desired result:

$$|\alpha f(x) - \beta g(x)| < \varepsilon \quad \text{for all } x > 0.$$

An immediate consequence of this result is the following:

THEOREM 2. Let F and G two continuous strictly monotonic binary operations on $[0,\infty)$ which are associative and have 0 as a unit. If there exists a positive number ε such that

$$|F(x,y) - G(x,y)| < \varepsilon \quad \text{for all } x,y \text{ in } [0,a),$$

then there are two additive generators f and g of F and G, respectively, such that

$$|f(x) - g(x)| < \varepsilon.$$

THEOREM 3. Let g be a one-to-one strictly increasing function from $[0,\infty)$ into itself such that g^{-1} is subadditive and let $\varepsilon > 0$ be a given positive real number. Consider ϕ to be any bijective solution of Hyers' inequality:

$$|\phi(x+y) - \phi(x) - \phi(y)| \leq g(\varepsilon) \quad \text{for all } x,y \text{ in } [0,\infty). \tag{7}$$

Then the function $f = \phi^{-1} \circ g$ satisfies

$$|f^{-1}(f(x)+f(y)) - g^{-1}(g(x)+g(y))| \leq \varepsilon \quad \text{for all } x,y \text{ in } [0,\infty).$$

Proof. Since g^{-1} is subadditive and increasing, we have

$$\begin{aligned} |g^{-1}(x) - g^{-1}(y)| &= g^{-1}(\mathrm{Max}(x,y)) - g^{-1}(\mathrm{Min}(x,y)) \\ &= g^{-1}(\mathrm{Min}(x,y) + |x-y|) - g^{-1}(\mathrm{Min}(x,y)) \\ &\leq g^{-1}(\mathrm{Min}(x,y)) + g^{-1}(|x-y|) - g^{-1}(\mathrm{Min}(x,y)) \\ &= g^{-1}(|x-y|). \end{aligned}$$

Using this property and (7) we obtain at once:

$$\begin{aligned} |f^{-1}(f(x)+f(y)) - g^{-1}(g(x)+g(y))| &= |g^{-1}(\phi[\phi^{-1}(g(x))+\phi^{-1}(g(y))]) - g^{-1}(g(x)+g(y))| \\ &\leq g^{-1}(|\phi[\phi^{-1}(g(x))+\phi^{-1}(g(y))] - g(x) - g(y)|) \\ &= g^{-1}(|\phi[\phi^{-1}(g(x))+\phi^{-1}(g(y))] - \\ &\quad - \phi[\phi^{-1}(g(x))] - \phi[\phi^{-1}(g(y))]|) \leq g^{-1}(g(\varepsilon)) = \varepsilon. \end{aligned}$$

References

1. J.Aczél, Lectures on Functional Equations and their Applications. Academic Press, New York and London (1966).

2. D.H.Hyers, On the Stability of the Linear Functional Equation. Proc.Nat.Acad.Sci.USA, Vol.27(1941), 222-224.

Dept. Matemàtiques i Estadística
E.T.S.A.B.
Universitat Politècnica de Catalunya
Avda.Diagonal 649. 80828 Barcelona,Spain.

Institute of Mathematics
Silesian University
Bankowa, 14
40-007 Katowice. Poland.

Received March 14, 1985

C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

NORMAL SUBGROUPS AND INVARIANTS IN THE CATEGORY OF TRANSFORMATION GROUPS

A. E. Fekete

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

Abstract: Invariants are defined in the category of transformation groups, and a necessary and sufficient condition for normal subgroup relation in terms of the invariants is given.

H. S. M. Coxeter suggested in 1967 that Felix Klein's Erlangen Program, classifying geometries according to subgroups of a group of transformations, has been superseded by classification of geometries according to pairs of subgroups K, H the smaller of which is a normal subgroup, in symbols: $K \trianglelefteq H$. Coxeter stated: "When a geometry is characterized, two groups arise: a group H under which all propositions remain valid, and a normal subgroup K under which the concepts and their properties are maintained" [1].

The rationale for declaring the Erlangen Program obsolete is clear. There are far too many subgroups of the group of collineations and it is unrealistic to expect a new invariant and a new geometry to arise for every one of them. Much scarcer are the pairs of subgroups the smaller of which is a normal subgroup of the larger, and the problem of finding a complete classification of geometric invariants in the new sense appears to be more accessible. Yet the import of Coxeter's suggestion has been lost on a generation of geometers. This note is designed to revive the problem, and also to put it in the slightly more general context of the category of transformation groups (wherein the groups act on sets bereft of any structure).

Let the transformation group G act on a (nonempty) set X. An invariant α, by definition, is an equivalence relation, denoted $\overset{\alpha}{\equiv}$, on the set X, giving rise to the quotient set X/α (whose elements are the equivalence classes modulo α). We shall say that $g \in G$ respects the invariant α if

$$x \overset{\alpha}{\equiv} x' \implies g(x) \overset{\alpha}{\equiv} g(x')$$

where $x, x' \in X$. The set H of $g \in G$ respecting α is clearly a subgroup of G. We shall say that $g \in G$ preserves the invariant α if

$$g(x) \overset{\alpha}{\equiv} x$$

for all $x \in X$. The set K of $g \in G$ preserving α is clearly a subgroup of G. Moreover, K is also a subgroup of H:

$$g \in K \implies g(x) \overset{\alpha}{\equiv} x,\ g(x') \overset{\alpha}{\equiv} x'$$
$$\implies [x \overset{\alpha}{\equiv} x' \implies g(x) \overset{\alpha}{\equiv} g(x')] \implies g \in H$$

In fact, K is a normal subgroup of H:

$$h \in H,\ k \in K \implies k(h^{-1}(x)) \overset{\alpha}{\equiv} h^{-1}(x) \quad \text{for all } x \in X$$
$$\implies h(k(h^{-1}(x)) \overset{\alpha}{\equiv} h(h^{-1}(x)) = x$$
$$\implies h \circ k \circ h^{-1}(x) \overset{\alpha}{\equiv} x \implies h \circ k \circ h^{-1} \in K$$

We say that the group K acts on X transitively modulo α if $x \overset{\alpha}{\equiv} x' \implies x' = k(x)$ for some $k \in K$.

THEOREM

Suppose that the group $K \leqq G$ acts on X transitively modulo α and it preserves the invariant α. Then the group $H \leqq G$ respects the invariant α if, and only if, $H \geq K$.

Proof: In view of the foregoing it will suffice to prove that $h \in H$ respects α, provided that $H \geq K$. We have

$$x \overset{\alpha}{\equiv} x' \implies x' = k(x), \quad k \in K$$

$$\implies h(x') = h(k(x)) = h \circ k \circ h^{-1}(h(x)) = k'(h(x))$$

where $k' = h \circ k \circ h^{-1} \in K \implies h(x) \overset{\alpha}{\equiv} h(x')$

It is also clear from the proof that if K is the group of all transformations preserving α, then the normalizer of K in G is the group H of all transformations $g \in G$ respecting α. The significance of the quotient group H/K is this: H/K is a transformation group acting on the quotient set X/α effectively, i.e., no nonidentity transformation in H/K fixes all the equivalence classes modulo α.

Examples

1. Let $A^{\pm}$ be the affine group of the plane, $D^{\pm}$ the subgroup of dilatations, X the set of straight lines, and α the parallelism of straight lines. $A^{\pm}$ respects (but does not preserve) α. $D^{\pm}$ preserves α and $A^{\pm} \geq D^{\pm}$. The quotient group $A^{\pm}/D^{\pm}$ acts on the quotient set X/α (= the line at infinity) effectively. In fact, $A^{\pm}/D^{\pm} = PG(\mathbb{R})$, the group of projectivities of the real projective line.

2. Let $A^{\pm}$ be the affine group of the plane, E the subgroup of equiaffinities, X the set of triangles, and let the invariant α be the area, i.e.,

$$x \overset{\alpha}{\equiv} x' \iff \text{area}(x) = \text{area}(x')$$

It is clear that $A^{\pm}$ respects (but does not preserve) area, and that E preserves area. Indeed, $A^{\pm} \geq E$.

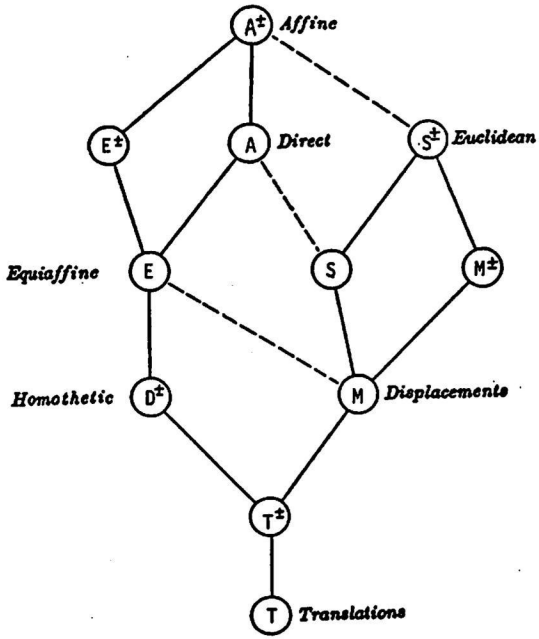
The quotient group is the multiplicative group of real numbers: $A^{\pm}/E = \mathbb{R}^{\times}$ and it acts on the quotient set X/α (the elements of which are the equivalence classes of equiareal triangles) effectively.

Oswald Veblen was the first to study geometries in the context of normal subgroups. In volume II of Projective Geometry [2], first published in 1918, he lists eleven subgroups of $A^{\pm}$ (p 118) :

$A^{\pm}$	the affine group
A	the group of direct affinities
$E^{\pm}$	the group of equiaffinities and skew reflections
E	the equiaffine group
$S^{\pm}$	the Euclidean group (i.e., the group of similarities)
S	the group of direct similarities
$M^{\pm}$	the group of displacements and reflections
M	the group of displacements
$D^{\pm}$	the homothetic group (i.e., the group of dilatations)
$T^{\pm}$	the group of translations and reflections
T	the group of translations

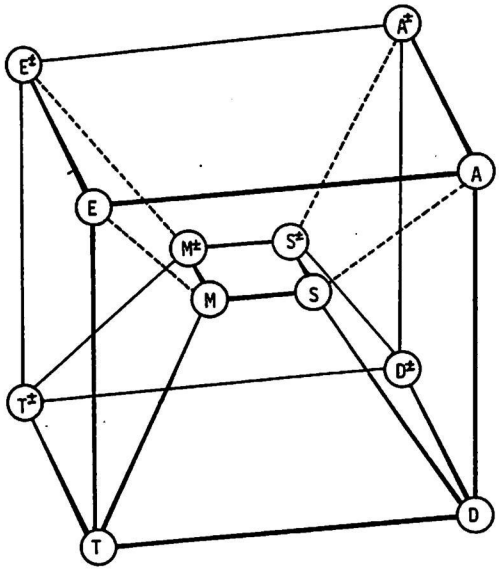
and observes the following relationships between them:

where the dotted line indicates that the lower of the two groups joined is a subgroup of the upper, and a solid line that it is a normal subgroup (however, not all normal subgroups relationships are shown).



Veblen's diagram contains two celebrated errors. The first one is an error of commission: As pointed out by Coxeter in 1967 ([1], p 15) $D^{\pm}$ is not a normal subgroup of E. The second one is an error of omission: As pointed out by Paul B. Yale in 1968 ([3], p 73) there is an important normal subgroup D of $S^{\pm}$, the group of dilatations with positive ratio. In fact D, no less than T, is a normal subgroup of every subgroup of $A^{\pm}$ that contains it.

As a result of these two errors, Veblen's diagram fails to bring out the significance of these normal subgroup relations. With both errors corrected, however, the diagram springs to life:



and it incorporates two additional features:

1. A pair of parallel solid lines gives rise to a pair of isomorphic quotient groups (the solid lines $T^{\pm}M^{\pm}$, $D^{\pm}S^{\pm}$, TM, DS are also considered parallel)
2. For a group $B^{\pm}$, B is a subgroup of index 2, and $B^{\pm}/B = \{1, -1\}$, the multiplicative group of order 2.

References

1. H.S.M. Coxeter, Transformation Groups from the Geometric Viewpoint, CUPM Report, No. 18, Washington, D.C.: Mathematical Association of America, October 1967, pp. 1-71.
2. O. Veblen and J.W. Young, Projective Geometry, volume II by O. Veblen, New York: Ginn 1946, p 118.
3. Paul B. Yale, Geometry and Symmetry, San Francisco: Holden Day, 1968, p 73.

Department of Mathematics
Memorial University
St. John's, Newfoundland
A1C 5S7

Received April 22, 1985

Mailing Addresses

1. C. Alsina — Dept. Matemàtiques i Estadistica, E.T.S.A.B., Universitat Politècnica de Catalunya, Avda. Diagonal 649, 80828 Barcelona, Spain

2. A.A. Bruen — Department of Mathematics, University of Western Ontario, London, Ontario, Canada M6A 5B7

3. J. Cuntz — Département de Mathématiques, Faculté des Sciences de Luminy, Case 901, F-13288 Marseille, Cédex 9, France

4. K.L. Duggal — Department of Mathematics, University of Windsor, Windsor, Ontario, Canada N9B 3P4

5. G.A. Elliott — Mathematics Institute, Universitetsparken 5, DK-2100 Copenhagen Ø, Denmark

6. I. Fenjö — Stromfel Aurél u. 27, H-1124 Budapest, Hungary

7. A.E. Fekete — Department of Mathematics, Memorial University, St. John's, Newfoundland, Canada A1C 5S7

8. R. Ger — Institute of Mathematics, Silesian University, Bankowa 14, 40-007 Katowice, Poland

9. F.M. Goodman — Department of Mathematics, University of Iowa, Iowa City, IA 52240, U.S.A.

10. C.U. Jensen — Matematisk Institute, Kobenhavns Universitet, Universitetsparken 5, DK-2100 Københaven Ø, Denmark

11. P.E.T. Jorgensen — Department of Mathematics, Universi y of Iowa, Iowa City, IA 52240, U.S.A.

12. A. Joyal — Département de Mathematiqus et d'informatique
Université du Québec à Montréal
Québec, Canada H3C 3P8

13. J. Mináč — Department of Mathematics and Statistics
Queens University
Kingston, Ontario, Canada K7L 3N6

14. L. Paganoni — Dipartimento di Matematica
Università degli Studi di Milano
via c. Saldini 50, I-20133
Milano, Italy

15. R. Sharma — Department of Mathematics
University of Windsor
Windsor, Ontario, Canada N9B 3P4

16. N. Yui — Department of Mathematics
University of Toronto
Toronto, Ontario, Canada M5S 1A1