C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

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 présentés par les membres d'autres académies nationales. Notre programme de notes courtes écrits ou présentés par les membres reste inchangé.

RELATED FUNCTIONAL EQUATIONS APPLIED TO KOROVKIN APPROXIMATION AND TO THE CHARACTERIZATION OF RENYI ENTROPIES — LINKS TO THE UNIQUENESS THEORY

J. Aczél

F.R.S.C.

Abstract. The same trick concerning continuous convex functions can be applied to correct an error in a characterization of Rényi entropies and to the solution of the functional equation

$$\frac{f(x)+f(y)}{x+y} = \frac{x+y}{x^2+y^2}\, f\left(\frac{x^2+y^2}{x+y}\right),$$

originating in a closure problem of Korovkin approximations. Both these and related problems can be solved also by other methods, including uniqueness theorems for functional equations. We explore links to the uniqueness theory, its advantages and a disadvantage.

1. Introduction

In 1960, A. Rényi has introduced the Rényi entropies and immediately 'proved' a characterization theorem concerning them. There was, however, an error in the proof of this theorem (see Section 3). This has been pointed out to Rényi. The paper [Rényi 1960a] was 'fortunately' written 'only' in Hungarian and in the English version [Rényi 1960b], he replaced this theorem by a different (and correctly proved) characterization theorem for Rényi divergences (he called them information gains) rather than entropies.

Still the original 'theorem' — now conjecture — kept intriguing mathematicians, until it was proved [Daróczy 1963] in its original form. Soon after a somewhat shorter proof was found [Aczél 1964a, cf. Aczél-Daróczy 1975]. This latter proof was then reformulated as a special case of the first uniqueness theorem for functional equations [Aczél 1964b].

This became the start of a long chain of results on uniqueness of solutions of some general types of functional equations [e.g. Aczél-Hosszú 1965, Howroyd 1969, 1970, Miller 1970, Ng 1970, Paganoni Marzegalli 1971, Paganoni 1972, 1974, 1976, 1978, etc.]. These uniqueness theorems had many more applications [see e.g. Aczél 1964b] and they have shed considerable light on the structure and properties of functional equations.

In section 4 we want to show, however, that Rényi's original 'proof' can be 'saved' by an old-new idea and some technical tinkering, thus giving another proof of Rényi's theorem turned conjecture turned theorem.

But first we jump twenty years ahead. In the spring of 1984, H. Bauer (Erlangen) wrote me about the functional equation

$$\frac{f(x)+f(y)}{x+y} = \frac{x+y}{x^2+y^2} f\left(\frac{x^2+y^2}{x+y}\right) \quad (x > 0, y > 0) \tag{1}$$

originating in a closure problem of Korovkin approximations (the proof that the function space spanned by x and x^2 is its own Korovkin closure in $C^0]0,1]$, cf. Donner 1982 and Bauer-Donner 1984). I found that the same idea which I have recently applied to the Rényi problem can also serve to solve the above equation as will be shown in section 2. Bauer has found a solution too. A third solution will be given in section 5.

In further correspondence, H. Bauer enumerated several further equations related to (1). In section 5 we intend to show how the simplest uniqueness theorems apply to all these questions. But they don't give complete solution to a problem (hitherto unsolved) by H. Bauer, which we will solve in section 6.

2. The equation (1)

We may show that the Korovkin closure of the function space generated by x and x^2 is itself by proving, as H. Bauer noticed, the following.

Theorem 1. *The general real valued continuous solution of (1) is given by*

$$f(x) = ax^2 + bx \qquad (x > 0), \tag{2}$$

where a, b are arbitrary constants.

My **proof** goes as follows: We write

$$g(x) := \frac{f(x)}{x} \qquad (x > 0), \tag{3}$$

so that (1) goes over into

$$\frac{xg(x) + yg(y)}{x+y} = g\left(\frac{x^2+y^2}{x+y}\right) \quad (x > 0, y > 0). \tag{4}$$

Let us write

$$p := \frac{x}{x+y}, \quad q := \frac{y}{x+y},$$

then we get

$$g(px+qy) = pg(x)+qg(y) \quad (p > 0, q > 0, p+q = 1). \tag{5}$$

If p and q were independent of x and y (in particular, if p and q were constants), then this would imply immediately that the continuous g – being both convex and concave – is linear. But p and q *do* depend upon x and y. However, even so, (5) states that *every chord on the graph of g contains a point of the graph other than the endpoints.* And *this, together with the continuity of g, guarantees that g is linear*, that is, *all* points of every chord on the graph are points of the graph itself [cf. Hardy-Littlewood-Pólya 1934]. Indeed, if there were a point G of the graph not on the chord, then there would be a last point P on the chord before Q and a first point R on the chord after Q (because the endpoints of the chord are on the graph and because g is continuous). But then the chord PR would contain no point of the graph other than P and R, contrary to supposition. So g is linear,

$$g(x) = ax+b \quad (x > 0) \tag{6}$$

is the general continuous solution of (4) and, by (3),

$$f(x) = ax^2 + bx \quad (x > 0)$$

is the general continuous solution of (1). (Straightforward substitution shows that these functions indeed satisfy (4) and (1), respectively.) □

3. Rényi's 'characterization' of the Rényi-Shannon entropies

The entropies of order α ($\neq 0$) or Rényi-Shannon entropies for possibly incomplete finite (discrete) probability distributions are defined by

$$\left.\begin{aligned} H_n^\alpha(p_1,p_2,\ldots,p_n) &= \frac{1}{1-\alpha}\log_2\Bigl(\sum_{k=1}^{n} p_k^\alpha \Big/ \sum_{k=1}^{n} p_k\Bigr) \quad (\text{for } \alpha \neq 1) \text{ and} \\ H_n^1(p_1,p_2,\ldots,p_n) &= -\sum_{k=1}^{n} p_k \log_2 p_k \Big/ \sum_{k=1}^{n} p_k \end{aligned}\right\} \tag{7}$$

(the latter is the Shannon entropy for possibly incomplete distributions), where

$$p_k > 0 \quad (k = 1,2,\ldots,n) \quad \text{and} \quad \sum_{k=1}^{n} p_k \leq 1; \quad n = 1,2,\ldots. \tag{8}$$

In [Rényi 1960a], these entropies were 'deduced' from the following assumptions:

(i) H_1 is nonnegative: $H_1(p) \geq 0$ $(0 < p \leq 1)$,

(ii) H_1 is normalized: $H_1(\frac{1}{2}) = 1$,

(iii) $\{H_n\}$ is quasilinear: $H_n(p_1,p_2,\ldots,p_n) = f^{-1}\bigl(\sum_{k=1}^{n} p_k f[H_1(p_k)] / \sum_{k=1}^{n} p_k\bigr)$, where $p_1,p_2,\ldots,p_n$, n are as in (8) and $f\colon H_1(]0,1]) \to \mathbf{R}$ is continuous and strictly monotonic, and

(iv) $\{H_n\}$ is additive: $H_n(p_1q,p_2q,\ldots,p_nq) = H_n(p_1,p_2,\ldots,p_n) + H_1(q)$, where $p_1,p_2,\ldots,p_n$, n are as in (8) and $q \in]0,1]$.

(We have slightly modified Rényi's conditions – in particular, (iv) is a special case of what Rényi and others [see e.g. Aczél-Daróczy 1975] called additivity – but the differences are not essential.)

The arguments in [Rényi 1960a] went essentially the following way. From (iv), $n = 1$,

$$H_1(pq) = H_1(p) + H_1(q) \quad (p,q \in \,]0,1]).$$

This, (i) and (ii) imply [see e.g. Aczél-Daróczy 1975]

$$H_1(p) = -\log_2 p \quad (p \in \,]0,1]). \tag{9}$$

If we put this into (iii), we get

$$H_n(p_1,p_2,\dots,p_n) = f^{-1}\Big(\sum_{k=1}^{n} p_k f\big(-\log_2 \sum_{k=1}^{n} p_k\big) \Big/ \sum_{k=1}^{n} p_k\Big) \tag{10}$$

or, with the new function $g\colon\,]0,1] \to \mathbf{R}$ defined by

$$g(p) := f(-\log_2 p) \quad (p \in \,]0,1]) \tag{11}$$

(also continuous and strictly monotonic),

$$H_n(p_1,p_2,\dots,p_n) = -\log_2 g^{-1}\Big(\sum_{k=1}^{n} p_k g(p_k) \Big/ \sum_{k=1}^{n} p_k\Big). \tag{12}$$

Putting this and (9) into (iv) yields

$$g^{-1}\Big(\sum_{k=1}^{n} p_k g(p_k q) \Big/ \sum_{k=1}^{n} p_k\Big) = g^{-1}\Big(\sum_{k=1}^{n} p_k g(p_k) \Big/ \sum_{k=1}^{n} p_k\Big) q \tag{13}$$

($p_1,p_2,\dots,p_n$, n as in (8), $q \in \,]0,1]$).

At this point in [Rényi 1960a], it was argued that the continuous and strictly monotonic solutions of (13) are 'known' [Knopp 1929, Jessen 1930, cf. Hardy-Littlewood-Pólya 1934] to be exactly

$$g(p) = A \log_2 p + B \quad \text{and} \quad g(p) = Ap^{a} + B \quad (p \in \,]0,1]), \tag{14}$$

($A \neq 0$, $a \neq 0$, otherwise a,A,B arbitrary constants). So we get, in view of (12), either

$$H_n(p_1,p_2,\dots,p_n) = -\sum_{k=1}^{n} p_k \log_2 p_k \Big/ \sum_{k=1}^{n} p_k = H_n^1(p_1,p_2,\dots,p_n),$$

the Shannon entropy, or

$$H_n(p_1,p_2,\dots,p_n) = -\frac{1}{a}\log_2\Big(\sum_{k=1}^{n} p_k^{a+1} / \sum_{k=1}^{n}\Big) = H_n^{a+1}(p_1,p_n,\dots,p_n)$$

which, with $\alpha = a+1$, goes over into the Rényi entropies of order $\alpha \neq 1$, cf. (7). (Actually, in the first version, Rényi restricted the argument to $\sum_{k=1}^{n} p_k = 1$, which would lead to even greater complications [see Daróczy 1964].)

It was pointed out to Rényi, however, that the 'known' theorem does not apply to (13) but to

$$g^{-1}\Big(\sum_{k=1}^{n} w_k g(p_k q) / \sum_{k=1}^{n} w_k\Big) = g^{-1}\Big(\sum_{k=1}^{n} w_k g(p_k) / \sum_{k=1}^{n} w_k\Big) q, \tag{15}$$

where the positive w_k are independent of the p_k (usually the w_k were constants, the p_k – and q – the variables). Also in (13), cf. (8), the restriction

$$\sum_{k=1}^{n} p_k \leq 1$$

was imposed, while in (15) the p_k (and q) can move arbitrarily on the positive half line or on one of its subintervals. But we will show in the next section that, rather than quoting the Jessen-Knopp theorem, one should analyze an appropriate proof and so one can eliminate the first difficulty. The second makes a more careful analysis necessary.

4. A method for salvaging the Rényi characterisation without explicit use of uniqueness theorems

It will be enough to suppose (iv) for ($n = 1$ and) $n = 2$. So we will take $n = 2$ also in (13) and (15). The Jessen-Knopp proof for (15) can be reformulated as follows. Keeping q in (15) temporarily constant and writing

$$\bar{g}(p) := g(pq) \quad (p \in\,]0,1]), \tag{16}$$

we get

$$\bar{g}^{-1}\left(\frac{w_1\bar{g}(p_1)+w_2\bar{g}(p_2)}{w_1+w_2}\right) = g^{-1}\left(\frac{w_1g(p_1)+w_2g(p_2)}{w_1+w_2}\right)$$

for $p_k \in \,]0,1]$ (say), $k = 1,2$,. For the new function $G\colon g(]0,1]) \to \mathbf{R}$, defined by

$$G(x) := \bar{g}[g^{-1}(x)] \quad (x \in g(]0,1]), \tag{17}$$

this gives, with

$$x_k := g(p_k) \quad (k = 1,2), \tag{18}$$

the equation

$$G\left(\frac{w_1x_1+w_2x_2}{w_1+w_2}\right) = \frac{w_1G(x_1)+w_2G(x_2)}{w_1+w_2}. \tag{19}$$

From this Jensen-type equation ($w_1 > 0$, $w_2 > 0$), and from the continuity of G, it follows that G is linear

$$G(x) = ax+b$$

because (19) states that *every chord of the graph of G contains a point of the graph other than the endpoints* (cf. section 2).

Going back to (17) and (16), we get

$$g(pq) = a(q)g(p) + b(p) \quad \text{for all} \quad p,q \in \,]0,1], \tag{20}$$

the solutions of which are indeed well known [e.g. Aczél 1966, Aczél-Daróczy 1975].

Let us see how this argument works for (13). The substitutions

$$\bar{g}(p) := g(pq) \quad (p \in \,]0,1]), \tag{16}$$

$$G(x) := \bar{g}[g^{-1}(x)] \quad (x \in g(]0,1]), \tag{17}$$

$$x_k := g(p_k) \quad (k = 1,2) \tag{18}$$

give for the continuous function G again

$$G\left(\frac{p_1x_1+p_2x_2}{p_1+p_2}\right) = \frac{p_1G(x_1)+p_2G(x_2)}{p_1+p_2}. \tag{21}$$

Even though the x_k are now linked to the p_k by (18), the above observation, that for the linearity of the continuous function G, it is sufficient that *some* point of every chord (other than the endpoints) of the graph of G should lie on the graph, assures already that G is linear on $g(]0,1])$, so we could proceed as before.

However, from (8) and (18), we have restrictions in (21), $p_1+p_2 \leq 1$, $p_k > 0$, $(k = 1,2)$, which does not really restrict the 'weights' $p_1/(p_1+p_2)$ and $p_2/(p_1+p_2)$ in $]0,1[$ but it imposes upon the 'variables' the restriction

$$g^{-1}(x_1)+g^{-1}(x_2) \leq 1 \quad (g^{-1}(x_k) > 0,\ k = 1,2), \tag{22}$$

(as g is continuous and strictly monotonic, g^{-1} exists on $g(]0,1])$). Since (13) is invariant under linear transformation of g (replacement of g by $\alpha g+\beta$, $\alpha \neq 0$), we may suppose without loss of generality that

$$g(1) = 1 \quad \text{and} \quad g(\tfrac{1}{2}) = \tfrac{1}{2}.$$

This g is continuous and strictly *increasing* and therefore so is g^{-1}. Also,

$$g^{-1}(x_1)+g^{-1}(x_2) \leq 1 \quad \text{if} \quad g^{-1}(x_k) \leq \frac{1}{2} \quad (k = 1,2)$$

so, by the above argument, since (21) holds for $x_k \in g(]0,1/2])$, $(k = 1,2)$

$$G(x) = ax+b \quad \text{for all} \quad x \in g(]0,1/2]). \tag{23}$$

We define M by

$$M = \sup \{\mu \mid G(x) = ax+b \text{ if } x \in g(]0,\mu])\}.$$

Since G,g are continuous, this supremum is a maximum. By (23), $M \geq \frac{1}{2}$. If $M < 1$, there would exist a decreasing sequence $\{M_n\}$ in $]M,1[$, converging to M and such that

$$G[g(M_n)] \neq ag(M_n)+b \quad (n = 1,2,\ldots). \tag{24}$$

Fix $p \in]0,1-M_1[\subset]0,1/2[$ and choose $M_m \in \{M_n\}$ (so $p+M_m < 1$) close enough to

M so that

$$\frac{pg(p)+M_m g(M_m)}{p+M_m} < g(M)$$

(such an m exists, since $p < M$, so

$$\frac{pg(p)+Mg(M)}{p+M} < g(M),$$

while

$$\frac{pg(p)+M_n g(M_n)}{p+M_n} \geq g(M)$$

for all n would imply

$$\frac{pg(p)+Mg(M)}{p+M} \geq g(M),$$

since g is continuous and $M = \lim M_n$). So G is linear at $g(p)$ and at $(pg(p)+M_m g(M_m))/(p+M_m)$ and (21) gives

$$a\,\frac{pg(p)+M_m g(M_m)}{p+M_m} + b = G\left(\frac{pg(p)+M_m g(M_m)}{p+M_m}\right) = \frac{pG[g(p)]+M_m G[g(M_m)]}{p+M_m}$$

$$= \frac{apg(p)+bp+M_m G[g(M_m)]}{p+M_m}$$

and thus

$$G[g(M_m)] = ag(M_m)+b,$$

contrary to (24). So $M = 1$ and

$$G(x) = ax+b \quad \text{for all} \quad x \in g(]0,1]).$$

Again going back to (17) and (16), we get (20) and thus (cf. (14))

$$g(p) = A\log_2 p+B \quad \text{or} \quad g(p) = Ap^{\alpha-1}+B \quad (p \in]0,1]),$$

$(A \neq 0, \alpha \neq 1)$. So, in view of (12), the Shannon and Rényi entropies (7) are again obtained and the gap in Rényi's original proof is filled (for arguments similar to parts of the above proof, see also [Aczél 1964a] and [Van der Pyl 1976]) and the theorem in [Daróczy 1963, Aczél 1964a,b] is proved again.

Theorem 2. *The Rényi-Shannon entropies (7) and only these satisfy the conditions (i)-(iv), where it is sufficient to suppose (iv) for* $n = 1$ *and* $n = 2$.

5. Related equations and relations to the uniqueness theory

In [Aczél 1964b], Theorem 2 was derived from the following theorem.

Theorem A. *Let* $I = \langle\alpha,\beta\rangle \subseteq \mathbf{R}$ *be an interval (open, half-open, closed, finite or infinite),* $\alpha',\beta' \in I$, *let* $S \subset \mathbf{R}^2$ *be such that* $\langle\alpha,\beta']^2 \subseteq S$ *and for every* $x \in\,]\beta',\beta\rangle$ *there exists a* $y \in \langle\alpha,\beta']$ *such that* $(x',y) \in S$ *for all* $x' \in\,]\beta',x]$. *Suppose that* $f_k\colon I \to I' \subseteq \mathbf{R}$, $(k = 1,2)$ *and* $F\colon S \to \mathbf{R}$ *are continuous,* F *internal, i.e.*

$$x < F(x,y) < y \quad \text{if} \quad x < y \quad \text{and} \quad x > F(x,y) > y \quad \text{if} \quad x > y \qquad ((x,y) \in S),$$

$u \mapsto H(x,y,u,v)$ *strictly monotonic (for all* $x,y \in I$, $v \in I'$*) and that*

$$f_k[F(x,y)] = H[x,y,f_k(x),f_k(y)] \quad (k = 1,2) \quad \text{on} \quad S.$$

Then

$$f_1(\alpha') = f_2(\alpha') \quad \text{and} \quad f_1(\beta') = f_2(\beta')$$

imply

$$f_1(x) = f_2(x) \quad \text{for all} \quad x \in I.$$

While the conditions are not particularly appetizing, the proof is only about twice as long as the above proof of Theorem 2. For Theorem 1, the following special case of Theorem A is more than enough.

Theorem B. *Let* $I \subseteq \mathbf{R}$ *be an interval,* $\alpha', \beta' \in I$, $f_k: I \to I' \subseteq \mathbf{R}$ *and* $F: I^2 \to \mathbf{R}^2$ *continuous,* F *internal on* I^2, *and* $u' \mapsto H(x,y,u,v)$ *strictly monotonic*

$$f_k[F(x,y)] = H[x,y,f_k(x),f_k(y)] \quad (k = 1,2) \text{ on } I^2.$$

Then

$$f_1(\alpha') = f_2(\alpha') \quad \text{and} \quad g_1(\beta') = g_2(\beta')$$

imply

$$f_1(x) = f_2(x) \text{ for all } x \in I.$$

Theorem 1 follows from Theorem B with $I =]0,\infty[$,

$$F(x,y) = \frac{x^2+y^2}{x+y}$$

which is indeed internal,

$$H(x,y,u,v) = \frac{x^2+y^2}{(x+y)^2}(u+v),$$

$\left(u \mapsto \frac{x^2+y^2}{(x+y)^2}(u+v)\right.$ indeed strictly monotonic) and with

$$f_1(x) = f(x), \qquad f_2(x) = ax^2+bx.$$

Similarly it follows from Theorem B that $g(x) = ax+b$ is the general continuous solution of equation (4) (same I, same F, $H(x,y,u,v) = (xu+yv)/(x+y)$, $f_1(x) = g(x)$, $f_2(x) = ax+b$).

Note that both the method used in sections 2-4 and the application of uniqueness theorems like A or B make use of the fact that F is internal, but the first uses that also H is internal in a sense, while it is essential in the second that $u \mapsto H(x,y,u,v)$ (or $v \mapsto H(u,v,x,y)$) be strictly monotonic (or at least one-to-one; no continuity supposed).

In subsequent correspondence, H. Bauer mentioned several equations related to (1) (and their solutions), for instance

$$\frac{f(x)+f(y)}{x+y} = \frac{f(\sqrt{xy})}{\sqrt{xy}} \quad (x,y > 0).$$

Here too, Theorem B can be applied:

$$F(x,y) = \sqrt{xy}\,, \quad H(x,y,u,v) = \frac{\sqrt{xy}}{x+y}(u+v),$$

$$f_1(x) = f(x), \quad f_2(x) = ax^{-1}+bx, \quad I =]0,\infty[$$

and all conditions of Theorem B are satisfied, so $f(x) = ax^{-1}+bx$ is the general continuous solution.

Several other applications of Theorem B have been mentioned in [Aczél 1964b].

So the uniqueness theory has its advantages too.

6. Nonexistence of nontrivial solutions of similar functional equations

Note that the above uniqueness theorem (and most other uniqueness theorems in the theory of functional equations) is just that: it states that certain functional equations have under certain conditions *at most one* solution, *not that there exists* a nontrivial solution. This can be seen very clearly on the equation

$$\frac{f(x)+f(y)}{x+y} = \frac{x+y}{2xy} f\left(\frac{2xy}{x+y}\right) \quad (x > 0, y > 0) \tag{25}$$

or, equivalently (with $g(x) := f(x)/x$ as before)

$$\frac{xg(x)+yg(y)}{x+y} = g\left(\frac{2xy}{x+y}\right) \quad (x>0, y>0) \tag{26}$$

about which H. Bauer has asked me repeatedly. As we see, (25) and (26) are quite similar to (1) and (4), respectively, and they satisfy all conditions of Theorem B. So they have *at most* a two-parameter set of solutions. However, we will prove that the only solutions of (25) are given by $f(x) = cx$ (a *one-parameter* set, so $f(\alpha)$ and $f(\beta)$ cannot be arbitrarily prescribed), and that *(26) has no nonconstant solutions.* We will *not* even *need continuity or any other regularity conditions.*

Theorem 3. *The functional equation (26) has no nonconstant solutions and the general solution of (25) is given by* $f(x) = cx$ $(x > 0)$, *where c is an arbitrary constant.*

Proof. The two statements in the theorem are clearly equivalent in view of $g(x) := f(x)/x$, so we will restrict ourselves to equation (26). Actually, we make a further reduction. We introduce new variables and a new function by

$$u := \frac{1}{x}, \quad v := \frac{1}{y}, \quad h(u) := g(\frac{1}{u}) \quad (u>0).$$

Then (26) goes over into

$$h(\frac{u+v}{2}) = \frac{vh(u)+uh(v)}{u+v} \quad (u>0, v>0) \tag{27}$$

and we have to prove that *all solutions of (27) are constant* (even though also (27) satisfies the conditions of Theorem B).

Now notice that (27) is linear (as were most of the functional equations in this paper) and that $h(u) \equiv 1$ satisfies it (as do all constant functions). So together with h every $Ah+b$ satisfies (27) (as was the case with (13)). Therefore, if there existed two positive numbers $\alpha \neq \beta$ such that $h(\alpha) \neq h(\beta)$, we could suppose without loss of generality

$$h(\alpha) = 0, \quad h(\beta) = 1.$$

Let us write

$$\gamma = \frac{\alpha+(\alpha+\beta)/2}{2} \quad \text{and} \quad \delta = \frac{\beta+(\alpha+\beta)/2}{2}.$$

Then

$$\gamma+\delta = \alpha+\beta$$

and, from (27),

$$\begin{aligned}\alpha &= \beta h(\alpha)+\alpha h(\beta) = (\alpha+\beta)h(\frac{\alpha+\beta}{2}) = (\gamma+\delta)h(\frac{\gamma+\delta}{2}) = \delta h(\gamma)+\gamma h(\delta) \\ &= \frac{\beta+(\alpha+\beta)/2}{2}h\left(\frac{\alpha+(\alpha+\beta)/2}{2}\right) + \frac{\alpha+(\alpha+\beta)/2}{2}h\left(\frac{\beta+(\alpha+\beta)/2}{2}\right) \\ &= \frac{\alpha+3\beta}{4}\,\frac{\alpha h((\alpha+\beta)/2)}{\alpha+(\alpha+\beta)/2} + \frac{3\alpha+\beta}{4}\,\frac{\beta h((\alpha+\beta)/2)+(\alpha+\beta)/2}{\beta+(\alpha+\beta)/2} \\ &= \frac{\alpha+3\beta}{2(3\alpha+\beta)}\,\frac{\alpha^2}{\alpha+\beta} + \frac{3\alpha+\beta}{2(\alpha+3\beta)}\left(\frac{\alpha\beta}{\alpha+\beta} + \frac{\alpha+\beta}{2}\right).\end{aligned}$$

Comparing the first and last terms of this chain of equations, a straightforward but tedious calculation leads to

$$0 = \alpha^4-2\alpha^3\beta+2\alpha\beta^3-\beta^4 = (\alpha-\beta)^3(\alpha+\beta).$$

Since both α and β are positive, this could hold only if $\alpha = \beta$ against our supposition. So h is indeed constant and so is g, while f is homogeneous linear. □

Equation (27) can also be solved using results and methods of [Vincze 1962,1963] and of [Chung-Kannappan-Ng 1984].

This research has been supported in part by a Natural Sciences and Engineering Research Council of Canada grant.

References

J. Aczél, 1964a, Zur gemeinsamen Charakterisierung der Entropien α-ter Ordnung und der Shannonschen Entropie bei nicht unbedingt vollständigen Verteilungen. Z. Wahrsch. Verw. Gebiete *3*, 177-183.

J. Aczél, 1964b, Ein Eindeutigkeitssatz in der Theorie der Funktionalgleichungen und einige ihrer Anwendungen. Acta Math. Acad. Sci. Hungar. *15*, 355-362.

J. Aczél, 1966, Lectures on Functional Equations and Their Applications. Academic Press, New York-London.

J. Aczél and Z. Daróczy, 1975, On Measures of Information and Their Characterizations. Academic Press, New York-San Francisco-London.

J. Aczél and M. Hosszú, 1965, Further uniqueness theorems for functional equations. Acta Math. Acad. Sci. Hungar. *16*, 51-55.

H. Bauer and K. Donner, 1984, Korovkin closures in $C_0(X)$. To appear in Notas Mat.

J.K. Chung, Pl. Kannappan, and C.T. Ng, 1984, A generalization of the cosine-sine functional equation on groups. To appear in Linear Algebra Appl.

Z. Daróczy, 1963, Uber die gemeinsame Charakterisierung der zu den nicht vollständigen Verteilungen gehörigen Entropien von Shannon und von Rényi. Z. Wahrsch. Verw. Gebiete *1*, 381-388.

Z. Daróczy, 1964, Mittelwerte und Entropien vollständiger Wahrscheinlichkeitsverteilungen. Acta Math. Acad. Sci. Hungar. *15*, 203-210.

K. Donner, 1982, Extension of Positive Operators and Korovkin Theorems. Lecture Notes in Mathematics, vol. 904. Springer, Berlin-Heidelberg-New York.

G.H. Hardy, J.E. Littlewood and G. Pólya, 1934, Inequalities. University Press, Cambridge.

T.D. Howroyd, 1969, Some uniqueness theorems for functional equations. J. Austral. Math. Soc. *9*, 176-179.

T.D. Howroyd, 1970, The uniqueness of bounded or measurable solutions of some functional equations. J. Austral. Math. Soc. *11*, 186-190.

B. Jessen, 1930, Uber die Verallgemeinerungen des arithmetischen Mittels. Acta Sci. Math. (Szeged) *5*, 108-116.

K. Knopp, 1929, Neuere Sätze über Reihen mit positiven Gliedern. Math. Z. *30*, 387-413.

J.B. Miller, 1970, Aczél's uniqueness theorem and cellular internity. Aequationes Math. *5*, 319-325.

C.T. Ng, 1970, Uniqueness theorems for a general class of functional equations. J. Austral. Math. Soc. *11*, 362-366.

L. Paganoni, 1972, Uniqueness theorems for a general class of functional equations (Italian). Boll. Un. Mat. Ital. *(4) 6*, 450-461.

L. Paganoni, 1974, On the uniqueness of the solutions of a certain class of functional equations (Italian). Rend. Istit. Mat. Univ. Trieste *6*, 77-80.

L. Paganoni, 1976, Uniqueness structure and parametrization for a class of functional equations' solutions. Riv. Mat. Univ. Parma *(4) 2*, 337-345.

L. Paganoni, 1978, On uniqueness structures: some conditions and applications. Rend. Circ. Mat. Palermo *(2) 27*, 41-52.

S. Paganoni Marzegalli, 1971, Uniqueness theorems for the functional equation $f[F(x,y)]=H[f(x),f(y);x,y]$ in metric spaces (Italian). Atti Accad. Naz. Lincei Rend. Cl. Sci. Fiz. Mat. Natur. *(8) 50*, 438-443.

A. Rényi, 1960a, Some fundamental problems in information theory (Hungarian). Magyar Tud. Akad. Mat. Fiz. Oszt. Közl. *10*, 251-282.

A. Rényi, 1960b, On measures of entropy and information. In Proc. 4th Berkeley Symp. Math. Statist. and Probab. Berkeley 1960, Vol. I, pp. 547-561, Univ. of Calif. Press, Berkeley, 1961.

T. Van der Pyl, 1976, Axiomatique de l'information d'ordre α de type β. C.R. Math. Acad. Sci. Paris Sér. A Math. *282*, 1031-1033.

E. Vincze, 1962, Eine allgemeinere Methode in der Theorie der Funktionalgleichungen. II. Publ. Math. Debrecen *9*, 314-323.

E. Vincze, 1963, Eine allgemeinere Method in der Theorie der Funktionalgleichungen. III. Publ. Math. Debrecen *10*, 283-318.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada
N2L 3G1

Received July 20, 1984.

C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

A NOTE ON THE FIRST CASE OF FERMAT'S LAST THEOREM

T. AGOH

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

1. Let p be an odd prime, B_m the Bernoulli number in the even suffix notation, and $f_m(u)$ the Mirimanoff polynomial, i.e., $f_m(u) = \sum_{k=1}^{p-1} k^{m-1} u^k$.

It is well known that if the equation

$$x^p + y^p + z^p = 0 \tag{1}$$

holds for integers x, y, z prime to each other in the first case (i.e., in the case $p \nmid xyz$), then

$$f_{p-1}(t) \equiv 0 \pmod p,$$

$$B_{2i} f_{p-2i}(t) \equiv 0 \pmod p, \quad i = 1, 2, \ldots, (p-3)/2,$$

where $t \in H = \{-x/y, -y/x, -y/z, -z/y, -z/x, -x/z\}$. We can further deduce from these congruences that (see e.g. [4])

$$\begin{aligned} &f_{p-1}(t) \equiv 0 \pmod p, \\ &f_i(t) f_{p-i}(t) \equiv 0 \pmod p, \quad i = 2, 3, \ldots, (p-1)/2. \end{aligned} \tag{2}$$

In the present paper we shall mainly study the p-divisibility properties for the values of consecutive Mirimanoff polynomials at $u = t \in H$, under the assumption for which the equation (1) holds in the first case.

2. We now define the following polynomials in $\mathbf{Q}[u]$: For $m \geq 0$ and $k \geq 1$,

$$A_k^{(m)}(u) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^m u^{k-i} \quad (0^0 = 1;\ 0^m = 0 \text{ if } m \neq 0).$$

We can state the following basic properties for $A_k^{(m)}(u)$:

Lemma 1. Let $m \geq 1$ and $k \geq 2$. Then, it follows that

$$\text{(i)} \quad A_k^{(m)}(u) = k\{A_k^{(m-1)}(u) + A_{k-1}^{(m-1)}(u)\},$$

$$\text{(ii)} \quad A_k^{(m)}(u) = u \sum_{i=0}^{m} \binom{m}{i} A_{k-1}^{(i)}(u) - A_{k-1}^{(m)}(u).$$

Proof. Let $g(u, v) = u e^v - 1$ and $g^k(u, v) = \{g(u, v)\}^k$. Then, we have

$$\begin{aligned} A_k^{(m)}(u) &= [\partial^m/\partial v^m\{g^k(u, v)\}]_{v=0} \\ &= k\,[\partial^{m-1}/\partial v^{m-1}\{g^k(u, v) + g^{k-1}(u, v)\}]_{v=0} \\ &= k\{A_k^{(m-1)}(u) + A_{k-1}^{(m-1)}(u)\}. \end{aligned}$$

And also,

$$\begin{aligned} A_k^{(m)}(u) &= [\partial^m/\partial v^m\{g^k(u, v)\}]_{v=0} \\ &= u\,[\partial^m/\partial v^m\{g^{k-1}(u, v)\, e^v\}]_{v=0} \\ &\quad - [\partial^m/\partial v^m\{g^{k-1}(u, v)\}]_{v=0} \\ &= u \sum_{i=0}^{m} \binom{m}{i} A_{k-1}^{(i)}(u) - A_{k-1}^{(m)}(u). \end{aligned}$$

||

Lemma 2. Let $m \ge 1$ and $k \ge 1$. If $b_k^{(m)} = A_k^{(m)}(1)$, then

$$A_k^{(m)}(u) = \sum_{i=1}^{r} \binom{k}{i} b_i^{(m)} u^i (u - 1)^{k-i},$$

where $r = k$ if $k \le m$, m if $k > m$.

Proof. Since $g(u, v) = (e^v - 1)u + u - 1$ and

$$b_k^{(m)} = [d^m/dv^m\{(e^v - 1)^k\}]_{v=0},$$

we can deduce that

$$\begin{aligned} A_k^{(m)}(u) &= [\partial^m/\partial v^m\{g^k(u, v)\}]_{v=0} \\ &= [\partial^m/\partial v^m\{\sum_{i=0}^{k} \binom{k}{i} (e^v - 1)^i u^i (u - 1)^{k-i}\}]_{v=0} \end{aligned}$$

$$= \sum_{i=1}^{k} \binom{k}{i} b_i^{(m)} u^i (u-1)^{k-i}.$$

If $i > m$, then $b_i^{(m)} = 0$ (see e.g. [1]). So the result follows. ||

Lemma 3. Let $m \geq 1$ and $\alpha \in \mathbb{Z}_p$ (the ring of all rational numbers which are p-integral). Then,

$$f_{m+1}(\alpha) \equiv A_{p-1}^{(m)}(\alpha) \equiv \sum_{i=1}^{r'} (-1)^i b_i^{(m)} \alpha^i (\alpha - 1)^{p-1-i} \pmod{p}, \qquad (3)$$

where $r' = p-1$ if $m \geq p-1$, m if $m < p-1$. In particular,

$$f_1(\alpha) \equiv A_{p-1}^{(0)}(\alpha) - 1 \pmod{p}.$$

Proof. Since $\binom{p-1}{i} \equiv (-1)^i \pmod{p}$ for $i = 0, 1, \dots, p-2$, we have

$$\begin{aligned} A_{p-1}^{(m)}(\alpha) &= [d^m/dv^m\{g^{p-1}(\alpha, v)\}]_{v=0} \\ &= \sum_{i=0}^{p-2} (-1)^i \binom{p-1}{i} (p-1-i)^m \alpha^{p-1-i} \\ &\equiv f_{m+1}(\alpha) \pmod{p}. \end{aligned}$$

The other assertions are immediate by Lemma 2 and direct calculations. ||

Lemma 4. Let $m \geq 1$, $p-2 \geq n \geq 1$ and $\alpha \in \mathbb{Z}_p$. If $A_{p-1}^{(i)}(\alpha) \equiv 0 \pmod{p}$ for all $i = m, m+1, \dots, m+n$, then

$$A_{p-1-n}^{(m)}(\alpha) \equiv 0 \pmod{p}.$$

Proof. By (i) of Lemma 1 we have

$$A_{p-1}^{(i+1)}(u) = (p-1)\{A_{p-1}^{(i)}(u) + A_{p-2}^{(i)}(u)\}.$$

Since $p \nmid p-1$, our assumptions give

$$A_{p-2}^{(i')}(\alpha) \equiv 0 \pmod{p}, \quad i' = m, m+1, \dots, m+n-1.$$

Similarly, by making use of the relation

$$A_{p-2}^{(i'+1)}(u) = (p-2)\{A_{p-2}^{(i')}(u) + A_{p-3}^{(i')}(u)\},$$

it follows that

$$A_{p-3}^{(i'')}(\alpha) \equiv 0 \pmod p, \quad i'' = m, m+1, \dots, m+n-2.$$

By repeating this procedure n-times, we arrive at the congruence indicated in the statement. ||

Assume that the equation (1) holds for integers x, y, z prime to each other in the first case. If $i \geq 2$ is not so large, then it may be possible to show that $f_i(t) \not\equiv 0 \pmod p$ for $t \in H$ (see e.g. [2, 3]). We can state the following theorem:

Theorem 1. *If the equation (1) holds for the first case, and if* $f_i(t) \not\equiv 0 \pmod p$ *for* $t \in H$ *and for* $i = 2, 3, \dots, k$ *(where* $2 \leq k \leq p-2$*), then it follows that*

$$A_{p-1-k}^{(p-1-k)}(t) \equiv \sum_{i=1}^{p-1-k} \binom{p-1-k}{i} b_i^{(p-1-k)} t^i (t-1)^{p-1-k-i}$$
$$\equiv 0 \pmod p.$$

Proof. In view of the congruences (3), we have $f_i(t) \equiv 0 \pmod p$ for $i = p-k, p-k+1, \dots, p-1$. Also, $f_p(t) = (t^p - t)/(t-1) \equiv 0 \pmod p$ since $t \not\equiv 0 \pmod p$. Hence, by Lemma 3 we have $A_{p-1}^{(i')}(t) \equiv 0 \pmod p$ for $i' = p-1-k, p-k, \dots, p-1$. By taking $m = p-1-k$, $n = k$ and $\alpha = t \in H$ in Lemma 4, it follows that $A_{p-1-k}^{(p-1-k)}(t) \equiv 0 \pmod p$. So, by Lemma 2 we can give the congruence required above. ||

3. Let $f_m(u)$ be the Mirimanoff polynomial and $f_m^{(n)}(u) = d^n/du^n\{f_m(u)\}$.

Lemma 5. *Let* $m \geq 1$. *Then, it follows that*

(i) $f_{m+1}(u) = u f_m'(u)$,

(ii) $(1-u) f_{m+1}(u) = u - p^m u^p + u \sum_{i=1}^{m} \binom{m}{i} f_{m+1-i}(u)$.

Proof. Since the first assertion is trivial, we give the proof of (ii) only. If $h(u, v) = 1 + \sum_{i=1}^{p-1} (u e^{v})^{i}$, then $h(u, v) = 1 - (u e^{v})^{p} + u e^{v} h(u, v)$. Noting that $h(u, 0) = f_1(u) + 1$, we have, if $m \geq 1$,

$$\begin{aligned} f_{m+1}(u) &= [\partial^{m}/\partial v^{m}\{h(u, v)\}]_{v=0} \\ &= - u^{p} [d^{m}/dv^{m}\{e^{pv}\}]_{v=0} + u [\partial^{m}/\partial v^{m}\{e^{v} h(u, v)\}]_{v=0} \\ &= - p^{m} u^{p} + u \{ \sum_{i=0}^{m} \binom{m}{i} f_{m+1-i}(u) + 1\}, \end{aligned}$$

which gives the relation (ii). ||

Using (i) of Lemma 5 succesively, we obtain, if $m \geq 1$ and $n \geq 1$,

$$f_{m+n+1}(u) = f_{m+n}(u) + \sum_{i=1}^{n} c_{i,n} u^{i+1} f_{m}^{(i+1)}(u), \tag{4}$$

where $c_{i,n}$ $(i = 1, 2, \ldots, n)$ are integers. In particular, $c_{n,n} = 1$ for all $n \geq 1$. We can state

Theorem 2. If the equation (1) holds for the first case, and if $f_i(t) \not\equiv 0 \pmod{p}$ for $t \in H$ and for $i = 2, 3, \ldots, k$ (where $2 \leq k \leq p - 2$), then it follows that $f_{p-1-k}^{(k+1)}(t) \equiv 0 \pmod{p}$.

Proof. By the congruences (2) we can deduce $f_i(t) \equiv 0 \pmod{p}$ for $i = p - k, p - k + 1, \ldots, p - 1$. Also we have $f_p(t) \equiv 0 \pmod{p}$. First, take $m = p - 1 - k$, $n = 1$ and $u = t \in H$ in (4):

$$f_{p-k+1}(t) = f_{p-k}(t) + c_{1,1} t^{2} f''_{p-1-k}(t).$$

Since $c_{1,1} = 1$ and $t \not\equiv 0 \pmod{p}$, we can give $f''_{p-1-k}(t) \equiv 0 \pmod{p}$. Next, observe (4) for $m = p - 1 - k$, $n = 2$ and $u = t \in H$:

$$f_{p-k+2}(t) = f_{p-k+1}(t) + c_{1,2} t^{2} f''_{p-1-k}(t) + c_{2,2} t^{3} f_{p-1-k}^{(3)}(t).$$

Noting that $c_{2,2} = 1$ and $t \not\equiv 0 \pmod{p}$, it can be deduced from $f''_{p-1-k}(t) \equiv 0 \pmod{p}$ that $f_{p-1-k}^{(3)}(t) \equiv 0 \pmod{p}$. By repeating these methods k-times, we have the congruence required in the statement. ||

REFERENCES

1. T. Agoh: On the first case of Fermat's last theorem, J. Reine Angew. Math., 314(1980), 21 - 28.
2. W. Keller and G. Loh: The criteria of Kummer and Mirimanoff extended to include 22 consecutive irregular pairs, to appear.
3. T. Morishima: Über die Fermatsche Vermutung, Proc. Imp. Acad. Japan, 8(1932), 63 - 66.
4. P. Ribenboim: 13 lectures on Fermat's last theorem, Springer - Verlag, New York - Berlin - Heidelberg, 1979.

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

Received July 13, 1984

C.R. Math Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

COVERS OF PROSUPERSOLVABLE GROUPS

Luis Ribes

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

Let $\gamma : H \longrightarrow G$ be an epimorphism of profinite groups. We sav that it is a *Frattini cover* of G, if $\ker \gamma \leq \Phi(H)$, where $\Phi(H)$ is the Frattini subgroup of H, i.e., the intersection of the open subgroups of H. Such covers are easily obtainable: given an epimorphism $\rho : K \longrightarrow G$, by Zorn's lemma, there is a minimal (closed) subgroup H of K with $\rho(H) = G$. Then $\rho_{|H} : H \longrightarrow G$ is a Frattini cover of G (cf. [1], [2]). Among all the covers of G, there is one which is universal in an obvious sense, namely the *universal Frattini cover* of G, denoted $\gamma : \tilde{G} \longrightarrow G$, and characterized by the fact that $\tilde{G}$ is a projective profinite group. (I follow the terminologv of [3].) The universal Frattini cover is unique up to isomorphisms commutinq with γ (cf. [1], [2]).

In this note we announce a result that describes the structure of $\tilde{G}$ for a class of aroups G that includes prosupersolvable groups. The details will appear elsewhere.

§1. THE RESULTS

Theorem. Let $p_1,\dots,p_n$ *be distinct prime numbers, and* $t_1,\dots,t_n$ *natural numbers. Let* G *be a profinite group that admits a subnormal series* $G = G_0 \rhd G_1 \rhd \dots \rhd G_n = 1$, *where* G_{i-1}/G_i *is a pro-*p_i*-group with minimal number of generators* t_i $(i = 1,\dots,n)$. *Let* $\bar G$ *be any profinite group admitting a subnormal series* $\bar G = \bar G_0 \rhd \bar G_1 \rhd \dots \rhd \bar G_n = 1$ *with* each $\bar G_{i-1}/\bar G_i$ *a free pro-*p_i*-group of rank* t_i. *Then any epimorphism* $\gamma : \bar G \longrightarrow G$ *is a universal Frattini cover of* G.

Corollary. Let G be a prosupersolvable group, and let $p_1,p_2,\dots$ be the primes that divide the order of G. Let $t_i < \infty$ $(i = 1,2,\dots)$ be the minimal number of generators of a p_i-Sylow subgroup of G. Let $\bar G$ be any prosupersolvable group whose order is divisible precisely by the primes $p_1,p_2,\dots,$ and suppose that the p_i-Sylow subgroups of $\bar G$ are free pro-p_i of rank t_i $(i = 1,2,\dots)$. Then any epimorphism $\gamma : \bar G \longrightarrow G$ is a universal Frattini cover of G.

These results allow the construction of universal Frattini covers of several classes of groups. For example if $D_n = \langle x,y \mid x^2 \, . \, y^n \, , \, (xy)^2 \rangle$ is the dihedral group of order $2n$, with n odd, its universal Frattini cover is $\tilde D_n = (Z_{p_1} \times \dots \times Z_{p_t}) \rtimes Z_2$ where Z_p is the additive group of p-adic number, $p_1, \dots p_t$ are the primes dividing n, and the action of Z_2 on Z_{p_i} is given by $x_2 \cdot x_i = -x_i$, where x_2 is a generator of Z_2 and x_i a generator of Z_{p_i}.

§2. THE PROOFS

The proof of Theorem 1 is done by induction on n. The case $n=1$ is very simple, and the main step from $n-1$ to n is based on the following two results.

(I) Let $\underline{C}$ be a class of finite groups closed under extensions and saturated, i.e., if T is a finite group and $T/\Phi(T) \in \underline{C}$, then $T \in \underline{C}$. Then any Frattini cover of a pro-$\underline{C}$-group is also pro-$\underline{C}$.

(II) Let $G = K \rtimes H$ be a semidirect product of profinite groups K and H, with $(|K|, |H|) = 1$. Let $\bar{G} = \tilde{K} \rtimes \tilde{H}$ be a semidirect product of the universal Frattini covers of K and H. Then any epimorphism $\gamma : \bar{G} \longrightarrow G$ is a universal Frattini cover of G.

The proof of (I) is not hard. To check (II) one observes first that $\bar{G}$ is projective since its p-Sylow subgroups are free. Using (I) one sees that the universal Frattini cover $\tilde{G}$ of G must be a semidirect product of $\tilde{K}$ and $\tilde{H}$. That in fact it coincides with $\bar{G}$ follows from the existence of an epimorphism from $\bar{G}$ to G, and the fact that $\bar{G}$ is projective.

To prove the Corollary one observes that $G = \varprojlim G_i$, where each G_i is a finitely generated prosupersolvable group whose order involves only finitely manv primes. Then using the simple fact that $\tilde{G} = \varprojlim \tilde{G}_i$, and the Theorem, the result follows.

REFERENCES

1. J. Cossey, O.H. Kegel and L.G. Kovacs, Maximal Frattini extensions, *Arch. der Math.* 35 (1980) 210-217.
2. D. Haran and A. Lubotzky, Embedding covers and the theory of Frobenius fields, *Israel J. Math.* 41 (1983) 181-202.
3. M. Jarden, Field Arithmetic, to appear.

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

Received July 17, 1984

C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

THE GEOMETRY OF MULTIVALENT WEAKLY CLOSE-TO-CONVEX FUNCTIONS

A. Lyzzaik and D. Styer

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

ABSTRACT

Based on a generalized concept of linear accessibility, a geometric characterization for the class of multivalent weakly close-to-convex functions is given. It is shown that this class is "almost" linearly accessible. This work generalizes Lewandowski's Criterion for univalent close-to-convex functions.

1. INTRODUCTION

In 1965 A.E. Livingston wrote a paper on multivalent close-to-convex functions [4]. The classes that Livingston considered, K(p), were not closed under uniform convergence on compact subsets of the unit disc. In 1972 D. Styer [8] gave several characterizations, which we shall call weakly close-to-convex functions, of the closures of Livingston's classes. These we designate $K_w(p)$. However, none of these characterizations is geometric in nature. Lyzzaik [5] has recently applied the concept of linear accessibility to p-sheeted surfaces, and has shown that Livingston's close-to-convex functions are linearly accessible.

Theorem 1 (Lyzzaik). Each function $f \in K(p)$ can be written as a composition, $f = P \circ h$, where P is a polynomial of degree p and $h \in S$, the class of normalized univalent functions. Furthermore, letting $\mathbb{B}$ stand for the unit disc, $\mathbb{C} - h(\mathbb{B})$ can be written as a union of closed "semi-lines" ℓ that satisfy:

1) P maps each ℓ one-to-one onto a closed Euclidean semi-line,
2) The initial point of each ℓ lies on $h(\mathbb{B})$, the boundary of $h(\mathbb{B})$, and
3) Any two such "semi-lines" have disjoint interiors.

In this paper we give a complete geometric characterization of weakly-close-to-convex functions. This will show that they are "almost", but not completely linearly accessible in the above sense.

2. BASIC DEFINITIONS

A function f regular in $\mathbb{B}$ is p-valent if it admits each complex number at most p times, and some number exactly p times. If f is 1-valent, $f(0) = 0$, and $f'(0) = 1$, then f is called a normalized univalent function. Let S denote the class of all such functions.

Definition. Let $S_a(p)$ be the class of functions f regular in $\mathbb{B}$, with p zeros there (counting multiplicity), and such that $\operatorname{Re}(zf'/f) > 0$ for all z in some annulus $\{z : \rho < |z| < 1\}$. $S_a(p)$ is the class of all p-valent annular starlike functions (see Hummel [2]).

We next define the class of close-to-convex functions of order p, as given by Livingston [4].

Definition. Let $K(p)$ be the class of functions F regular in $\mathbb{B}$, with $F(0) = 0$, such that there is a function $f \in S_a(p)$ for which $\mathrm{Re}(zF'/f) > 0$ for all z in some annulus $\{z : \rho < |z| < 1\}$.

Definition. Let $K_w(p)$, the class of weakly close-to-convex functions, be all non-zero functions in the closure of $K(p)$, in the the topology of uniform convergence on compact subsets of $\mathbb{B}$ (see Styer [8]).

These are the functions that we will characterize geometrically. In order to do this we will use Theorem 9.1 of Lyzzaik [5]:

Theorem 2. If $f \in K_w(p)$, then $f = P \circ h$, where P is a polynomial of degree at most p and $h \in S$.

Most of the work in this paper is involved with ruling the complement of $h(\mathbb{B})$ in the domain of P.

Definition. A (connected) curve ℓ in the domain of a polynomial P is called a line if P maps ℓ one-to-one onto a straight line. We define rays (closed semilines) and segments (closed intervals) similarly.

Note that a line or ray may pass through critical points of P, and that the interior of any line segment is two sided. Also, if two lines, rays or segments ℓ, ℓ' intersect in more than one point, the intersection must be a line, ray or a segment. Otherwise, $\ell \cup \ell'$ would contain the boundary of some bounded region, an impossibility since $P(\ell \cup \ell')$ is a subset of a line.

Definition. Suppose that ℓ and ℓ' are non-disjoint lines, rays, or segments for which $\ell \quad \ell'$ lies interior to both of them. ℓ and ℓ' are said to *cross* if any neighborhood of $\ell \cap \ell'$, $\ell - \ell'$ contains points on both sides of ℓ'.

Definition. Let f be a nonconstant function regular in $\mathbb{B}$ such that $f(0) = 0$ and $f = P \circ h$ where P is a polynomial of degree $q \leq p$, and $h \in S$. f is called *weakly linearly accessible of order* p if $\mathbb{C} - h(\mathbb{B})$ is a union of rays such that each starts at $\partial h(\mathbb{B})$, and no two of the rays cross.

We close this section by stating the main theorem.

Theorem 3. *A function is weakly close-to-convex of order p if and only if it is weakly linearly accessible of order p. Furthermore, if a function f is weakly close-to-convex, the composition $f = P \circ \phi$ may be chosen such that $Cl(\phi(\mathbb{B})$ contains all the critical points of P.*

3. THE NEW GEOMETRY FOR $\mathbb{C}$

It is instructive to compare this theorem with the theorem of Lewandowski [3] that a univalent function f with $f(0) = 0$ is close-to-convex if and only if $\mathbb{C} - f(\mathbb{B})$ is the union of rays such that the corresponding open rays are disjoint (i.e. f is linearly accessible). It is clear that such rays do not cross, and thus f is weakly linearly accessible. On the other hand, suppose that f is weakly linearly accessible of order 1. Choose any two rays ℓ, ℓ' from a weakly linearly accessible ruling of $\mathbb{C} - f(\mathbb{B})$. Since ℓ and ℓ' do not cross, either the corresponding open rays are disjoint, or one is a subset of the other. By a result of Sheill-Small [7], f is linearly accessible.

The interesting feature is that when $p > 1$, we may have two non-crossing rays in the geometry determined by P, and yet their interiors will not be disjoint and one will not be a subset of the other. This is the critical difference, topologically, between the new geometry and Euclidean geometry of straight lines in $\mathbb{C}$. There can be lines that meet only at a critical point of P, and yet these lines need not cross. The key to our solution to this problem is that only finitely many noncrossing lines may meet at a point.

Proposition. Let A be a set of open line segments that meet at a point ζ, and do not cross. Suppose, also, that the open line segments in A are pairwise distinct in any neighborhood of ζ. Then A is a finite set. If there are at least two such open line segments, then ζ is a critical point of P.

The proof that a weakly linearly accessible function of order p is weakly close-to-convex of order p is much easier than the other half of the theorem. We use the given ruling of $\mathbb{C} - h(\mathbb{B})$ for some weakly linearly accessible function, $f = P \circ h$, of order p, to select a sequence of functions $(f_n)_{n=1}^{\infty}$ such that $f_n \to f$ uniformly on every compact subset of $\mathbb{B}$. Then we show using a generalized form of the Schwarz-Christoffel transformation (see [1]) that each $f_n \in K_w(p)$. Since $K_w(p)$ is closed in the topology of uniform convergence on compact subsets of $\mathbb{B}$, $f \in K_w(p)$

Suppose $f \in K_w(p)$ be of the form $P \circ h$ where P is a polynomial of degree at most p and h is a univalent function. Part of the success in proving the second half of the theorem is that the decomposition $f = P \circ h$ reduces our work to that of ruling the complement of the image of h, albeit, in a new geometry. One might conclude that the entire problem is of a univalent nature. In a possibly surprising way that this is not true, the fact that contributes significantly to the difficulty in the proof. For a detailed proof of the theorem see [6].

References

1. A.W. Goodman, On the Schwarz-Christoffel transformation and p-valent functions, Trans. Amer. Math. Soc. 68(1950), 204-223.
2. J.A. Hummel, Multivalent starlike functions, J. Analyse Math. 18(1967), 133-160.
3. Z. Lewandowski, Sur l'identite de certaines classes de fontiones univalentes, II, Ann. Univ. Mariae Curie-Sklodowska Sect. A, 14 (1960), 19-46.
4. A.E. Livingston, p-valent close-to-convex functions, Trans. Amer. Math. Soc. 115(1965), 161-179.
5. A. Lyzzaik, Multivalent linearly accessible functions and close-to convex functions, Proc. London Math. Soc. (3), 44(1982).
6. _________ and D. Styer, The geometry of multivalent close-to-convex functions, to appear.
7. T. Sheil-Small, On linear accessibility and the conformal mapping of convex domains, J. Analyse Math. 25(1972), 259-276.
8. D. Styer, Close-to-convex multivalent functions with respect to weakly starlike functions, Trans. Amer. Math. Soc. 169(1972), 105-112.

Abdallah Lyzzaik
Dept. of Math. Sciences
University of Petroleum & Minerals
Dhahran, Saudi Arabia

David Styer
Dept. of Math. Sciences
University of Cincinnati
Cincinnati, Ohio 45221, USA

Received August 14, 1984

C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

ON PLANES OF THE LENZ-BARLOTTI CLASS I6

II. A CONFIGURATION AND ITS AUTOMORPHISMS

Peter Scherk, FRSC

1. Let A denote an affine plane of class I6, let π_0 be the pencil of the axes of its axial affinities. Thus there is a one-one correspondence $x \leftrightarrow \pi(x)$ between the lines $x \in \pi_0$ and the pencils $\neq \pi_0$ of parallel lines such that every affinity with the axis x has the pencil of traces $\pi(x)$.

If XIx, let h_X denote the line in $\pi(x)$ through the point X. Then $h_X\phi = h_{X\phi}$ for every point X and every collineation ϕ.

There is a translation τ characterized by the relation

$$AIhB \leftrightarrow BIh_{A\tau} \qquad \text{if } A \neq B .$$

It commutes with every collineation; cf. [1].

2. Let $[\infty], [0], [1]$ denote three mutually distinct lines in π_0 and let α be the affinity with the axis $[\infty]$ mapping $[0]$ onto $[1]$. The affinity β with the axis $[0]$ shall map $[\infty]$ onto $[1]$. Then $\operatorname{ord}\alpha = \operatorname{ord}\beta$ is either infinite or a prime number. We assume

$$2 < \operatorname{ord}\alpha = p < \infty \quad .$$

Then τ is involutory.

Let $F_p = \{r, s, \ldots\}$ denote the prime field of characteristic p; $F_p^* = F_p \setminus \{0\} = \{i, j, k, \ldots\}$; $\bar{F}_p = F_p \cup \{\infty\} = \{n, m, \ldots\}$. Then α^r and β^r are well defined for every r. Let $[r] = [0]\alpha^r$. Then $[i] = [\infty]\beta^{1/i}$.

The powers of α and β generate a group G which is isomorphic to the two-dimensional special linear group over F_p. Hence its centre consists of the identity and of an involutory translation σ. There are no other translations in G. Its axial affinities are the powers of α and of the elements $\alpha^{-r}\beta\alpha^{r}$.

3. Starting with an arbitrary point $(\infty,1^{(0)})$ on $[\infty]$, we construct our configuration $\mathfrak{C} \subset A$: Associate a different copy $F_p^{*(\lambda)} = \{i^{(\lambda)}, j^{(\lambda)}, k^{(\lambda)}, \dots\}$ of F_p^* with each $\lambda \in \mathbb{Z}$. Then $\mathfrak{C}$ consists of the points $(n,i^{(\lambda)})$ and the lines $[n]$ and $[n,i^{(\lambda)}] = h_{(n,i^{(\lambda)})}$. (Here n and the $i^{(\lambda)}$ range through $\bar{F}_p$ and the $F_p^{*(\lambda)}$, resp.) We have

$$(n,i^{(\lambda)}) = (m,k^{(\mu)}) \Leftrightarrow n=m,\ i=k,\ \text{ and } \begin{cases} \lambda \equiv \mu \pmod 4 & \sigma \neq \tau \\ & \text{if} \\ \lambda \equiv \mu \pmod 2 & \sigma = \tau \end{cases}.$$

Thus $\mathfrak{C}$ contains exactly $4(p^2-1)$ or exactly $2(p^2-1)$ mutually distinct points depending on whether $\sigma \neq \tau$ or $\sigma = \tau$.

The incidences in $\mathfrak{C}$ are given by

$$(n,i^{(\lambda)})\, I\, [n,i^{(\lambda)}],\ [\infty,i^{(\lambda)}],\ [n] \qquad \text{for all } i,n,\lambda,$$
$$[r,-i^{(\lambda)}]\, I\, (r,-i^{(\lambda)}),\ (\infty,i^{(\lambda+2)}),\ (r+ik,k^{(\lambda+1)})$$

for all i,k,r,λ. The action of G on $\mathfrak{C}$ is determined by

$$(0,i^{(\lambda)})\alpha^{r} = (r,i^{(\lambda)}) \quad \text{and} \quad (\infty,i^{(\lambda)})\beta^{\frac{1}{k}} = (k,(\tfrac{k}{i})^{(\lambda-1)}).$$

Thus $\mathfrak{C}G = \mathfrak{C}$. Note that $(n,i^{(\lambda)})\sigma = (n,-i^{(\lambda)})$ and $(n,i^{(\lambda)})\tau = (n,-i^{(\lambda+2)})$.

The G-orbits of $\mathfrak{C}$ are the sets

$$\mathfrak{Q}^{(\lambda)} = \{(r,i^{(\lambda)}) \mid r,i\} \cup \{(\infty, i^{(\lambda+1)}) \mid i\}.$$

4. A collineation ψ in $\mathbb{C}$ is a pair of bijections of the sets of the points and lines of $\mathbb{C}$ onto themselves which preserve incidence and satisfy $h_X\psi = h_{X\psi}$ for every point X in $\mathbb{C}$. The collineations in $\mathbb{C}$ form a group $\overline{G}$ containing G and τ with the centre

$$Z(\overline{G}) = \begin{cases} \{1,\sigma,\tau,\sigma\tau\} & \sigma \neq \tau \\ & \text{if} \\ \{1,\tau\} & \sigma = \tau \end{cases} .$$

The collineation ψ has the axis $x \in \mathbb{C}$ if every point of $\mathbb{C}$ on x is a fixed point of ψ. Such a collineation is an axial affinity in G.

A collineation in $\mathbb{C}$ is a translation in $\mathbb{C}$ if it maps every line of $\mathbb{C}$ onto a parallel line. It has the fixed set $\{[n] | n\}$ unless it is the identity. The group $\overline{T}$ of these translations is the centralizer of G in $\overline{G}$.

5. Let

$$\xi_j : \begin{cases} (n, i^{(\lambda)}) \mapsto \begin{cases} (nj, (ij)^{(\lambda)}) \\ (nj, i^{(\lambda)}) \end{cases} \text{ if } \lambda \text{ is } \begin{matrix} \text{even,} \\ \text{odd} \end{matrix} \\ \\ [n] \mapsto [nj] \\ h_X \mapsto h_{X\xi_j} \qquad \text{for every point } X \in \mathbb{C} , \end{cases}$$

Each ξ_j is a collineation in $\mathbb{C}$. It satisfies

$$\xi_j^{-1} \alpha \xi_j = \alpha^j \quad \text{and} \quad \xi_j^{-1} \beta \xi_j = \beta^{1/j} .$$

The group $K = \{\phi\xi_j \mid \phi\epsilon G, j\epsilon F_p^*\}$ is mapped isomorphically onto the full linear group $L(2,F_p)$ by

$$\alpha \mapsto \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \quad \beta \mapsto \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \quad \xi_j \mapsto \begin{pmatrix}1 & 0\\ 0 & j\end{pmatrix}.$$

Its centre consists of the translations in $\mathbb{C}$

$$\upsilon_j\,(n, i^{(\lambda)}) \mapsto \begin{cases}(n,(ij)^{(\lambda)}) & \text{if } \lambda \text{ is even}\\ (n,(i/j)^{(\lambda)}) & \text{if } \lambda \text{ is odd.}\end{cases}$$

The sets $\mathbb{Q}^{(\lambda)}$ are also the K-orbits of $\mathbb{C}$.

6. We define a translation ω in $\mathbb{C}$ through

$$\omega : \begin{cases}(n,i^{(\lambda)}) \mapsto (n,i^{(\lambda+1)})\\ [n,i^{(\lambda)}] \mapsto [n,i^{(\lambda+1)}]\\ [n] \mapsto [n]\,.\end{cases}$$

It satisfies $\omega^2 = \sigma\tau$ (thus $w^4 = 1$) and $\upsilon_j\omega = \omega\upsilon_j^{-1}$.

Every $\upsilon\epsilon\overline{T}$ has the form $\upsilon = \upsilon_j\omega^\lambda$ where j and w^λ are uniquely determined by υ. Thus $\overline{T}$ acts transitively on the points in $\mathbb{C}$ on any line $[n]$, and the order of $\overline{T}$ is equal to the number of these points, i.e. to $4(p-1)$ if $\sigma\neq\tau$ and to $2(p-1)$ if $\sigma=\tau$.

Every $\psi\epsilon\overline{G}$ has a decomposition $\psi=\phi\xi j\omega^\lambda$ where $\phi\epsilon G$, $j\epsilon F_p^*$ and ω^λ are uniquely determined by ψ. The group $\overline{G}$ acts transitively on $\mathbb{C}$.

REFERENCE

[1] P.Scherk, On planes of class I6. C.R. Math. Rep. Acad. Sci. Canada-Vol.III(1981) No.6, 333-335.

Received September 15, 1984

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

C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

A NUMBER OF BLOCKS OF TWISTED GROUP ALGEBRAS

G. Karpilovsky

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

Abstract Let G be a finite group, let F be an arbitrary field of characteristic $p > 0$ and let $\alpha \in Z^2(G,F^*)$. Denote by $F^\alpha G$ the corresponding twisted group algebra of G over F. The paper is devoted to the problem of determining the number of blocks of $F^\alpha G$ of a given defect in terms of natural invariants associated with G and α. The special case of the main result where $\alpha = 1$ encompasses theorems due to Brauer and Nesbitt [1], Gow [3], Kawada [5] and Michler [6], originally proved by diverse methods.

The groundwork for the present discussion is incorporated in the author's forthcoming monograph (Karpilovsky [4]). Let G be a finite group, let F be an arbitrary field of characteristic $p > 0$ and let $\alpha \in Z^2(G,F^*)$. Denote by $F^\alpha G$ the corresponding twisted group algebra of G over F. An interesting question in α-representation theory is to determine the number of blocks of $F^\alpha G$ of a given defect in terms of natural invariants associated with G and α. This is a formidable task even for the case where $\alpha = 1$. Among other difficulties, the counting of blocks of $F^\alpha G$ is complicated by the following two facts which have no counterpart in the ordinary case.

(i) If H is a subgroup of G, then an $\alpha|H$-regular element h of H need not be α-regular.

(ii) If P is a normal p-subgroup of G, then it is not always possible to find $\beta \in Z^2(G/P, F^*)$ such that $F^\alpha G$ admits a homomorphism into $F^\beta(G/P)$. In fact, the proof of many results concerning the number of blocks of ordinary group algebras relies heavily on the availability of the natural homomorphism $FG \to F(G/P)$. This homomorphism for twisted group algebras is, in general, no longer available even in the simplest case where $G = P$.

The difficulty arising from (i) in some cases is overcome by the fortunate fact discovered by Reynolds [7] which ensures that any $\alpha|H$-regular element h of H is α-regular provided $H = N_G(P)$ where P is a defect group of the H-conjugacy class containing h. If F is perfect or, more generally, if F is replaced by its suitable finite purely inseparable field extension E, then it will be shown that it is always possible to find $\beta \in Z^2(G/P, E^*)$ such that $E^{\alpha}G$ admits a homomorphism into $E^{\beta}(G/P)$. It is this fact together with the property that finite purely inseparable field extensions do not change the block idempotents that will allow us to overcome the difficulties of (ii).

Our aim in this paper is to announce the following theorem which provides generalizations to twisted group algebras of results due to Brauer and Nesbitt [1], Gow [3], Kawada [5] and Michler [6]. The idea of the proof rests on replacing F by its suitable finite purely inseparable field extension, extending the Conlon-Reynolds correspondence for an arbitrary α and on providing a through analysis of certain ideals of $F^{\alpha}G$. Details will appear elsewhere.

Theorem. Let F be a field of characteristic $p > 0$, let G be a group of order $p^m n$, $(n,p) = 1$, and let $\alpha \in Z^2(G, F^*)$. For each $d \in \{0, 1, \dots, m\}$, let c_d and ℓ_d denote respectively the number of α-regular conjugacy classes of p'-elements of G of defect d and the number of blocks of $F^{\alpha}G$ of defect d. Then the following properties hold:

(i) For all $d \in \{0, 1, \dots, m\}$, $\ell_d < c_d$.

(ii) The equality $\ell_d = c_d$ is true if F is algebraically closed and at least one of the following conditions holds:

(a) p does not divide $(P.C_G(P) : P)$, where P is a defect group of a block of defect d

(b) (Conlon [2]) $d = m$

(c) $N_G(P)/P$ *has a normal* p*-complement*

(d) G *has a normal* p*-complement*

(e) $d = m - 1$ *and* p *is the smallest prime divisor of* $|G|$

(f) $d = m - 2$, G *is of odd order and* p *is the smallest divisor of* $|G|$.

References

1. R. Brauer and C. Nesbitt, On the modular characters of groups, Ann. of Math. 42 (1941), 556-590.
2. S.B. Conlon, Twisted group algebras and their representations, J. Austral. Math. Soc. 4 (1964), 152-173.
3. R. Gow, A note on p-blocks of a finite group, J. London Math. Soc. (2) 18, (1978), 61-64.
4. G. Karpilovsky, Projective Representations of Finite Groups, Marcel Dekker, Pure and Applied Mathematics, A series of Monographs and Textbooks, New York (in the press).
5. Y. Kawada, On blocks of group algebras of finite groups, Science Reports of the Tokyo Kyoiku Daigaku A, 9 (1966), 87-110.
6. G. Michler, Blocks and centres of group algebras, Lecture on rings and modules, Lecture Notes in Mathematics, 246, Springer, Berlin, (1972), 429-563.
7. W.F. Reynolds, Block idempotents of twisted group algebras, Proc. Amer. Math. Soc. 17 (1966), 280-282.

Received September 26, 1984

Professor G Karpilovsky
Department of Mathematics
University of the Witwatersrand
1 Jan Smuts Avenue
Johannesburg 2001
South Africa

C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

AN INEQUALITY FOR GENERALIZED LAGUERRE POLYNOMIALS

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

The generalized Laguerre polynomial of degree $L_n^{(\alpha)}$ is defined for $x \geq 0$, $\alpha \in \mathbb{C}$ by

$$(1) \qquad L_n^{(\alpha)}(x) = e^x x^{-\alpha} \frac{d^n}{dx^n} (x^{n+\alpha} e^{-x})/n!$$

or equivalently by the generating function

$$(2) \qquad \sum_{n=0}^{\infty} L_n^{(\alpha)}(x)\, t^n = (1-t)^{-\alpha-1} e^{-xt/(1-t)}, \quad |t| < 1$$

Explicitly $L_n^{(\alpha)}$ is given by the formula

$$(3) \qquad L_n^{(\alpha)}(x) = \sum_{m=0}^{n} \binom{n+\alpha}{n-m} (-x)^m/m!$$

which follows from (1) on applying Leibniz' rule. When $\alpha = 0$, $L_n^{(\alpha)}$ is referred to as the Laguerre polynomial of degree n and is denoted by L_n.

The properties of these polynomials have been extensively studied; see [4; Chapter V] or [1;§10.13]. Three such properties that we shall need later are

$$(4) \qquad \sum_{m=0}^{n} (\alpha-\beta)_m L_{n-m}^{(\beta)}(x)/m! = L_n^{(\alpha)}(x),$$

$$(5) \qquad \sum_{m=0}^{n} L_m^{(\alpha)}(x) L_{n-m}^{(\beta)}(y) = L_n^{(\alpha+\beta+1)}(x+y),$$

both of which follow easily from (2), and

(6) $$\int_0^\infty e^{-st}\, t^{\alpha}\, L_n^{(\alpha)}(t)\,dt = \Gamma(\alpha+n+1)\ (s-1)^n/(n!\,s^{\alpha+n+1}),$$

Re $\alpha>-1$, Re $s>0$,

which follows easily from (3).

Inequalities for generalized Laguerre polynomial are of use in determining the convergence of series involving the polynomials. The basic such inequality,

(7) $$|L_n(x)| \le e^{\frac{1}{2}x},$$

was discovered by Szego [3], as was also the inequality

(8) $$|L_n^{(\alpha)}(x)| \le (\alpha+1)_n\ e^{\frac{1}{2}x}/n!,\ \alpha \ge 0.$$

Inequality (8) can also be derived from (7) and (4) using the relation

(9) $$\sum_{m=0}^{n} (\alpha)_m/m! = (\alpha+1)_{n/n!}$$

For $-1<\alpha<0$, the inequality

(10) $$|L_n^{(\alpha)}(x)| \le (2-((\alpha+1)_n/n!))\,e^{\frac{1}{2}x}$$

can be proved in much the same way, but is clearly not as satisfactory an inequality as (7), since, from (3), $L_n^{(\alpha)}(0) = (\alpha+1)_n/n!$ so that (7) is exact at $x=0$, while (10) obviously is not.

In this note we shall prove that if $\alpha \le 0$, then

(11) $$|L_n^{(\alpha)}(x)| \le 2^{-\alpha} e^{\frac{1}{2}x} .$$

This inequality, when $-1 < \alpha < 0$, is better than (10), at least for large n, since if $-1 < \alpha < 0$, $(\alpha+1)_n/n! \to 0$. However it is not exact at $x = 0$ either. Nor is it best possible. For example, if H_n denotes the Hermite polynomial of degree n, then from [1; 10.13(2)],

(12) $$H_{2m}(x) = (-1)^m 2^{2m} m!\, L_m^{(-\frac{1}{2})}(x^2),$$ and thus from (12) and (10),

(13) $$|H_{2m}(x)| \le 2^{2m+\frac{1}{2}} m!\, e^{\frac{1}{2}x^2} .$$

However, from [1;10.18(19)],

(14) $$|H_{2m}(x)| \le k 2^m ((2m)!)^{\frac{1}{2}} e^{\frac{1}{2}x^2} ,$$

where k is a constant of approximate value 1.086435. The estimate (14) is a better estimate than (13) since as $m \to \infty$, $2^{2m+\frac{1}{2}} m! \sim \pi^{\frac{1}{2}} 2^{2m+1} m^{m+\frac{1}{2}} e^{-m}$, while $2^m((2m)!)^{\frac{1}{2}} \sim \pi^{\frac{1}{4}} 2^{2m+\frac{1}{2}} m^{m+\frac{1}{4}} e^{-m}$.

Nevertheless, inequality (10) seems worthy of note and of proving, for it seems to be the only inequality for $|L_n^{(\alpha)}(x)|$, valid for all $\alpha < 0$, and uniform in n. To prove (10) we use the relation,

(15) $$(\Gamma(\mu))^{-1} \int_x^\infty (t-x)^{\mu-1} e^{-t} L_n^{(\nu)}(t)\,dt = e^{-x} L_n^{(\nu-\mu)}(x), \quad \operatorname{Re}\mu > 0,$$

which we will prove below. This relation, which gives the Weyl fractional integral of $e^{-x}L_n^{(\nu)}(x)$, is certainly not well known; it does not appear in [1] or [4] or [2;§13.2] for example.

The proof of (15) is as follows. Setting $t = y+x$, then from (5) with $\alpha = \nu - \mu$, $\beta = \mu - 1$, $(\Gamma(\mu))^{-1} \int_x^\infty (t-x)^{\mu-1} e^{-t} L_n^{(\nu)}(t)\,dt$

$$= (\Gamma(\mu))^{-1} e^{-x} \int_0^\infty y^{\mu-1} e^{-y} L_n^{(\nu)}(x+y)\,dy$$

$$= (\Gamma(\mu))^{-1} e^{-x} \sum_{m=0}^{n} L_m^{(\nu-\mu)}(x) \int_0^\infty y^{\mu-1} e^{-y} L_{n-m}^{(\mu-1)}(y)\,dy.$$

But from (6), with $s = 1$, since $\operatorname{Re}\mu > 0$

$$(\Gamma(\mu))^{-1} \int_0^\infty y^{\mu-1} e^{-y} L_{n-m}^{(\mu-1)}(y)\,dy = \begin{cases} 0, & n \neq m \\ 1, & n = m \end{cases},$$

and (15) follows.

Inequality (10) for $\alpha < 0$ now follows from (15) using (7), for if $\alpha < 0$,

$$|L_n^{(\alpha)}(x)| \le (\Gamma(-\alpha))^{-1} e^x \int_x^\infty (t-x)^{-\alpha-1} e^{-t} |L_n(t)|\,dt$$

$$\le (\Gamma(-\alpha))^{-1} e^x \int_x^\infty (t-x)^{-\alpha-1} e^{-\frac{1}{2}t}\,dt$$

$$= (\Gamma(-\alpha)^{-1}) e^{\frac{1}{2}x} \int_0^\infty y^{-\alpha-1} e^{-\frac{1}{2}y}\,dy = 2^{-\alpha} e^{\frac{1}{2}x}.$$

For $\alpha = 0$, (10) and (7) coincide.

Actually, since (15) holds for complex ν and μ such that $\operatorname{Re}\mu > 0$, it can be used to derive the inequality

$$|L_n^{(\alpha)}(x)| \le \Gamma(-\operatorname{Re}\alpha)\, 2^{-\operatorname{Re}\alpha} e^{\frac{1}{2}x} / |\Gamma(-\alpha)|, \quad \operatorname{Re}\alpha < 0,$$

but such inequalities for non-real α seem of little interest.

References

1. A. Erdelyi et al., Higher transcental functions II, New York (McGraw-Hill), 1953.

2. __________________, Tables of integral transforms II, New York (McGraw-Hill), 1954.

3. G. Szego, Ein Beitrag zur Theorie der Polynome von Laguerre und Jacobi, Math. Zeit. 1 (1918), 341-356.

4. G. Szego, Orthogonal polynomials (4th edition), A.M.S. Colloquim publication XXIII, Providence (A.M.S.), 1975.

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

Received October 12, 1984

C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

ON HOMOLOGIES AND ELATIONS OF THE SAME ORDER

M. D'Angelo

Presented by Peter Scherk, F.R.S.C.

Abstract If a projective plane of Lenz class $\geq$ IV admits both an elation and a homology of finite order, then these orders are relatively prime (in particular, they are distinct).

1. INTRODUCTION: Consider an elation ε of order s in a finite projective plane of order n. Of the n+1 points on a line (other than the axis) through the centre, one is kept fixed while the remaining n are partitioned into orbits each consisting of s points. Hence s divides n. Similarly the order t of any homology η must divide n-1. Thus s and t must be relatively prime. Does this remain true in infinite planes? Equivalently, we ask whether a projective plane can admit non-trivial elations and homologies with the same prime order p (if p is common prime divisor of s and t, we may replace ε and η by $\varepsilon^{s/p}$ and $\eta^{t/p}$). This question was answered negatively by Burn [1] for the case p = 2, except perhaps for planes of Lenz-Barlotti classes I1 and I2. We show that the answer is negative for any p, provided the plane is of Lenz class $\geq$ IV.

For definitions and basic properties not explicitly referred to, see [3], chapters 3 and 4, and [2].

2. PRELIMINARY RESULTS: Let $\mathfrak{P}$ be a projective plane and p a prime number.

2.1 Let ε_0 and η_0 be an elation and a homology with a common axis [with a common centre]; $\varepsilon_0 \neq 1 \neq \eta_0$. The group $G = \langle \varepsilon_0, \eta_0 \rangle$ consists of perspective collineations with the same axis [with the same centre]. Clearly the elations in G form a normal subgroup N of G. Each $\gamma \in G$ can be written in the form

$$(1) \qquad \gamma = \varepsilon_0^{a_1} \eta_0^{b_1} \varepsilon_0^{a_2} \eta_0^{b_2} \ldots \varepsilon_0^{a_n} \eta_0^{b_n},$$

where n is some positive integer and $a_1, \ldots, a_n$, $b_1, \ldots, b_n$ are integers. The integer $s = s(\gamma) = b_1 + b_2 + \ldots + b_n$ evidently depends not only on γ but also on the representation (1). However, (1) may be rewritten as follows:

$$(2) \begin{cases} \gamma = \varepsilon \eta_0^{s}, \text{ where} \\ \varepsilon = \varepsilon_0^{a_1} \eta_0^{b_1} \varepsilon_0^{a_2} \eta_0^{b_2} \ldots \varepsilon_0^{a_n} \eta_0^{b_n - s} \\ \quad = \varepsilon_0^{a_1} \cdot (\eta_0^{b_1} \varepsilon_0 \eta_0^{-b_1})^{a_2} \cdot (\eta_0^{(b_1+b_2)} \varepsilon_0 \eta_0^{-(b_1+b_2)})^{a_3} \cdot \ldots \cdot \\ \quad (\eta_0^{(b_1+\ldots+b_{n-1})} \varepsilon_0 \eta_0^{-(b_1+\ldots+b_{n-1})})^{a_n}. \end{cases}$$

Thus ε is an elation.

From now on <u>we assume</u> $\eta_0^{p} = 1$; thus $\eta_0^{s} = 1$ if and only if $s \equiv 0 \pmod p$. Hence (2) then yields:

2.2 PROPOSITION: (i) $N = \{\gamma \in G : s(\gamma) \equiv 0 \pmod p\}$. (ii) N <u>is generated by the</u> p <u>elations</u>: $\varepsilon_t = \eta_0^{-t} \varepsilon_0 \eta_0^{t}$ $(t=0, 1, \ldots, p-1)$.

2.3 The homology η_0 induces the automorphism

$$\tilde{\eta}_0 : \begin{cases} N \to N \\ \varepsilon \mapsto \eta_0^{-1}\varepsilon\eta_0 . \end{cases}$$

As η_0 has the order p, so does the automorphism $\tilde{\eta}_0$.

2.4 PROPOSITION: Suppose $\eta_0^p = \varepsilon_0^p = 1$. Then N is infinite and non-abelian.

PROOF: (i) The orbit of any elation $\varepsilon \neq 1$ under the automorphism $\tilde{\eta}_0$ of 2.3 consists of the p distinct elations $\eta_0^{-t}\varepsilon\eta_0^t$ $(t=0,1,\dots,p-1)$, all of them distinct from 1. Thus if N were finite, the order of N would be $\equiv 1 \pmod p$. On the other hand, ord N would have to be divisible by ord $\varepsilon_0 = p$; contradiction.

(ii) With ε_0, each elation $\eta_0^{-t}\varepsilon_0\eta_0^t$ has the order p. Thus 2.2 (ii) implies that an abelian N would have to be finite. This contradicts (i).

3. Our goal is

3.1 THEOREM: Suppose the projective plane $\mathfrak{P}$ admits an elation ε and a homology η of the same prime order p. Then

(i) $\mathfrak{P}$ is infinite;

(ii) $\mathfrak{P}$ is of Lenz class $\leq$ III.

3.2 COROLLARY: Suppose that in a projective plane of Lenz class $\geq$ IV, the elation ε and the homology η have the finite orders s and t respectively. Then s and t are relatively prime (cf. 1).

We recall the following fact (cf. [4], p.25, Thms. 19 and 20).

3.3 LEMMA: *Suppose there are elations* $\neq 1$ *with the same axis* ℓ *but distinct centres*. *Then*

(i) *the group of the elations with the axis* ℓ *is abelian*;

(ii) *if one elation* $\neq 1$ *in this group has finite order*, *this order is prime and all elations* $\neq 1$ *with the axis* ℓ *have this same order*.

In the following, let ε be an (E,e)-elation and let η be an (H,h)-homology in $\mathfrak{P}$. We study the following statement:

(3) ε *and* η *have the same order* p.

3.4 LEMMA: *If* $\mathfrak{P}$ *has two translation lines*, *then* (3) *is false*.

PROOF: Let L denote the intersection of the two translation lines. Then every line through L is a translation line. Assume (3).

Case (i): There is another point L' such that every line through L' is a translation line. Then for any point L" ($\neq$ L') there is an elation mapping L to L". Thus every line through L" is a translation line. .

Choose first L" = E. Then by the dual of 3.3 (i), the group of the elations with the centre E is abelian. Now take L" $\neq$ E,H. Then some elation τ with its axis through L" will map H onto E. Thus both the elation ε and the homology $\tau^{-1}\eta\tau$ have the centre E and the order p. By 2.4, there is a non-abelian group of elations with the centre E; contradiction.

Case (ii): L is the only point such that every line through it is a translation line. Then L must be a fixed point of every collineation of $\mathfrak{P}$; in particular, $L^{\varepsilon} = L^{\eta} = L$. Thus e I L and either h I L or H = L.

Subcase (a): h I L. Then some elation τ with its axis through L maps h onto e. Both the elation ε and the homology $\tau^{-1}\eta\tau$ have the axis e and the order p. Hence by 2.4, there is a non-abelian group of elations with that axis. This contradicts 3.3 (i).

Subcase (b): H = L. Choose any (H,e)-elation $\varepsilon_0 \neq 1$. As $\varepsilon^p = 1$, 3.3 (ii) implies $\varepsilon_0^p = 1$. Applying 2.4 to ε_0 and $\eta_0 = \eta$ we obtain again a contradiction.

3.5 REMARK: The proof of 3.4 could be shortened by applying [3], Theorem 6.18 (and hence the Skornyakov-San Soucie Theorem; cf. [3], Theorem 6.16).

3.6 LEMMA: *Let* $\mathfrak{P}$ *have the translation line* ℓ. *Then* (3) *implies*

(i) E I ℓ *and either* $\ell = h$ *or* ℓ I H;

(ii) char $\mathfrak{P}$ = p.

PROOF: Assume (3). By 3.4, ℓ is the only translation line of $\mathfrak{P}$. Hence $\ell^{\varepsilon} = \ell^{\eta} = \ell$, from which (i) follows. By 3.3 and its dual we have (ii).

PROOF OF 3.1: Assume (3). The first assertion has been proved in 1.

Assume that $\mathfrak{P}$ is either of Lenz class $\geq$ V or of Lenz class IVa. Then $\mathfrak{P}$ has a translation line ℓ. By 3.6 and the dual of 3.3, we may assume $e = \ell$. Thus by 3.6 (i), either e = h or e I H. If e = h, every group of elations with the axis e is abelian; cf. 3.3 (i). If e I H, we may choose E = H and every group of elations with the centre E is abelian; cf. 3.3 and the dual of 3.3 (i). In either case, 2.4 yields a contradiction.

The case of Lenz class IVb is dual to IVa.

REFERENCES

[1] R. P. Burn: The coexistence of involutory elations and homologies. Math. Zeitschr. 103 (1968), pp. 195-200.

[2] P. Dembowski: Finite Geometries. Springer, New York 1968.

[3] D. Hughes and F. C. Piper: Projective Planes. Springer, New York 1973.

[4] P. Scherk and R. Lingenberg: Rudiments of Plane Affine Geometry. University of Toronto Press, Toronto 1975.

Marianopolis College
3880 Côte-des-Neiges
Montréal, Québec
Canada H3H 1W1

Received October 31, 1984

C.R. Math. Rep. Acad. Sci. Canada - Vol. VI, No. 6, December 1984 décembre

THE PRODUCT OF UNITARY REFLECTIONS.

A.J. Coleman*

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

The product of the generating reflections of the Weyl group plays a very significant role in the theory of Lie groups. It has been named the COXETER OPERATOR since Coxeter made great use of it in his discussion of finite groups generated by reflections - see, for example, his Regular Complex Polytopes, pp. 87, 150. However, Killing, in 1889, employed such products in his discussion of the classification of simple Lie Algebras.

In the generalization from real to unitary reflection groups the notion of a reflection was extended to denote any unitary operation which leaves fixed the elements of a subspace of codimension one. Thus a reflection, R , is characterized by a pair $(a,\underline{e})$ and is defined by

$$R\underline{x} = \underline{x} - a\langle\underline{x}|\underline{e}\rangle\underline{e} \quad ,$$

where a is a complex number, $\underline{e}$ is a unit vector and $\langle x|e\rangle$ denotes the hermitian product in our n-dimensional space.

We say that R is proper if it is not the identity and is invertible or, equivalently, if a is neither 0 nor 1. The eigenvalues of R are $1-a$, and 1 with multiplicity $n-1$. That R is unitary is equivalent to $1-a$ having absolute value 1. In a unitary reflection of period p , $(1-a)^p = 1$.

---

* Research supported by NSERC Grant A-2990

Let R_i be characterized by a_i and $\underline{e}_i$, V_k be the subspace spanned by $\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_k$, $S_k = R_1 R_2 \ldots R_k$, and $S^k =$ the inverse of S_k. Finally, we shall say that <u>a set of reflections is linearly independent</u> if their corresponding vectors $\underline{e}_i$ are linearly independent.

With the notation thus established we can formulate the main result of the present paper.

<u>THEOREM</u>. <u>The product of a set of proper linearly independent reflections has no fixed point, other than the null vector, in the space spanned by its vectors.</u>

In other words, if $\underline{e}_i$ are linearly independent, the origin is the only point in V_n fixed under the action of S_n. We shall prove this by induction on the dimension.

Since $a \neq 0$, the theorem is trivial for $n = 1$, since it merely means that no complex number except zero is fixed when it is multiplied by $1-a$.

Suppose the theorem is true for S_{n-1} and suppose that S_n has a fixed point $\underline{x} \neq 0$. Then

$$S_n \underline{x} = \underline{x}$$

and therefore,

$$R_n \underline{x} = S^{n-1} \underline{x} \quad .$$

Choose an orthonormal basis in which S^{n-1} is diagonal and the first $n-1$ basis vectors span V_{n-1}. Since $\underline{e}_n$ is not contained in V_{n-1}, if $\underline{e}_n = [u_i]$, u_n is not zero. Since the last coordinate axis is fixed under S_{n-1} and therefore also S^{n-1} the last element in the diagonal matrix for S^{n-1} is 1.

Equating the n-th coordinates of the two sides of the preceding equation, we conclude that

$$a_n \langle \underline{x} | \underline{e}_n \rangle u_n = 0 \quad .$$

Thus, since neither a_n nor u_n is zero it follows that $\langle \underline{x} | \underline{e}_n \rangle$ vanishes and hence $\underline{x}$ is fixed under R_n and therefore also under S^{n-1} and S_{n-1} . Now $\underline{x} = \underline{v} + \underline{w}$ where $\underline{v}$ lies in V_{n-1} and $\underline{w}$ is perpendicular to V_{n-1} that is the direction of the n-axis. Since $\underline{w}$ is fixed under S_{n-1} so is $\underline{v}$.

By the induction assumption it follows that $\underline{v} = 0$, so $\underline{x} = \underline{w}$ and thus $\bar{x}_n u_n = \langle \underline{w} | \underline{e}_n \rangle = 0$. This implies that $x_n = 0$ whereas $\underline{v} = 0$ means that $x_i = 0$ for $0 < i < n$, so $\underline{x} = 0$ and the only fixed point of S_n is the origin.

****

It is perhaps worth remarking that the proofs of this result of which I was previously aware[1,2] applied only to real reflection groups and assumed properties of the relevant Dynkin diagram. The above argument evidently clears away some of redundant underbrush. In fact, the essential hypothesis - that the $\underline{e}_i$ are linearly independent - was one which both Killing and Cartan[3] employed in their discussion of the same product.

1. N. Bourbaki, Fas. 34, Groups et Algèbres de Lie,
P. 118, Ch. V, §6, 2.
2. A.J. Coleman, Can. Jl. Math. 10, 349-356 (1958).
3. E. Cartan, Thesis 1894, P. 58; Collected Works,
Part I, Vol. 1, P. 188.

Queen's University
Kingston, Ontario K7L 3N6

Received October 31, 1984

Mailing Addresses

1. J. Aczél
   Department of Pure Mathematics
   University of Waterloo
   Waterloo, Ontario, Canada, N2L 3G1

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

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

4. M. D'Angelo
   Département de Mathematiques
   Marianopolis College
   3880 Côtes-des-Neiges
   Montréal, Québec, Canada, H3H 1W1

5. G. Karpilovsky
   Department of Mathematics
   University of the Witwatersrand
   1 Jan Smuts Ave.
   Johannesburg 2001, South Africa

6. A. Lyzzaik
   Department of Mathematical Science
   University of Petroleum and Minerals
   Dharhran, Saudi Arabia

7. L. Ribes
   Department of Mathematics and Statistics
   Carleton University
   Ottawa, Canada, K1S 5B6

8. P.G. Rooney
   Department of Mathematics
   University of Toronto
   Toronto, Ontario, Canada M5S 1A1

9. P. Scherk
   Department of Mathematics
   University of Toronto
   Toronto, Ontario, Canada, M5S 1A1

10. D. Styer
    Department of Mathematical Sciences
    University of Cincinnati
    Cincinnati, Ohio 45221, U.S.A.

INDEX - Volume VI