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

Vol. XIII, Nos. 2, 3 April-June 1991 avril-juin

## CONTENTS

# A NOTE ON THE GRANVILLE - HEATH-BROWN THEOREM

Petr FUCHS

*Presented by J.B. Friedlander, F.R.S.C.*

**Abstract.** We consider the possibility of improving the Granville - Heath-Brown theorem.

We say that FLT is true for a positive integer $n$ if the Diophantine equation $x^n + y^n = z^n$ has no solutions in positive integers. Fermat's last theorem states that FLT is true for every $n \geqslant 3$ but this assertion has not been proved yet.

Filaseta [2] derived an important corollary of Faltings' theorem [1].

**Theorem. (Filaseta)** *For every $n \geqslant 3$ there exists a natural number $m = m(n)$ (depending on $n$) such that if $k \geqslant m$ then FLT is true for $kn$.*

Using Filaseta's theorem Granville [3] and Heath-Brown [4] established the following theorem.

**Theorem. (Granville - Heath-Brown)** *For every real number $x$, let $N(x)$ be the number of positive integers $n \leqslant x$ such that FLT is false for $n$. Then*

$$\lim_{x \to \infty} \frac{N(x)}{x} = 0 .$$

We will show that, using only Filaseta's theorem, it is impossible to improve the Granville - Heath-Brown result: we will show that Filaseta's theorem is not sufficient

to prove $\lim_{x\to\infty} \frac{N(x)}{f(x)} = 0$, if the function $f:(0,\infty) \to (0,\infty)$ satisfies the condition $\lim_{x\to\infty} \sup \frac{x}{f(x)} = \infty$.

Let $V$ be the set of all sequences $v:\{1,2,3,\ldots\} \to \{0,1\}$ satisfying the following condition:

> <u>for every $n \geq 3$ there exists a natural number $m = m(n)$ (depending on $n$) such that if $k \leq m$ then $v(kn) = 1$.</u>

For $v \in V$ and a real number $x$ let $N_v(x)$ be the number of positive integers $n \leq x$ such that $v(n) = 0$.

Define the sequence $w:\{1,2,3,\ldots\} \to \{0,1\}$ in this way:

$$w(n) = \begin{cases} 1 & \text{if FLT is true for } n \\ 0 & \text{if FLT is false for } n. \end{cases}$$

Filaseta's theorem states $w \in V$ and, by the Granville - Heath-Brown theorem, $\lim_{x\to\infty} \frac{N_w(x)}{x} = 0$.

Granville and Heath-Brown used only Filaseta's theorem in the proof of their result, that is, only the information that $w \in V$. Their proof, in fact, works for any $v \in V$, so that $\lim_{x\to\infty} \frac{N_v(x)}{x} = 0$ for every $v \in V$.

Now we will prove the following theorem.

**Theorem.** <u>Let $f:(0,\infty) \to (0,\infty)$. Then</u> $\lim_{x\to\infty} \frac{N_v(x)}{f(x)} = 0$ <u>for every $v \in V$ if and only if</u> $\lim_{x\to\infty} \sup \frac{x}{f(x)} < \infty$.

**Proof.** (1) If $\limsup_{x\to\infty} \frac{x}{f(x)} < \infty$ then there exist $x_0$ and $k$ such that if $x \geqslant x_0$ then $\frac{x}{f(x)} \leqslant k$. Therefore

$$\frac{N_v(x)}{f(x)} = \frac{N_v(x)}{x} \cdot \frac{x}{f(x)} \leqslant \frac{N_v(x)}{x} .k \to 0 \quad \text{as} \quad x \to \infty \quad \text{for}$$

every $v \in V$.

(2) If $\limsup_{x\to\infty} \frac{x}{f(x)} = \infty$ then there exists a sequence $\{x_n\}_{n=1}^{\infty}$ of real numbers such that $x_n \to \infty$ and

$$\frac{x_n}{f(x_n)} \to \infty .$$

Let $p_1 < p_2 < p_3 < \ldots$ be the sequence of all odd primes and denote $B_r = \prod_{j=1}^{r} p_j$ for every positive integer $r$. Define sequences $\{n_r\}_{r=1}^{\infty}$, $\{q_r\}_{r=0}^{\infty}$ in the following way:

$q_0 = 0$,

$n_r$ is some positive integer satisfying

$$\frac{x_{n_r}}{f(x_{n_r})} \cdot \prod_{j=1}^{r}(1 - \frac{1}{p_j}) \geqslant 1 \quad \text{and}$$

$$x_{n_r} \geqslant 2.(B_r)^{1+q_{r-1}} ,$$

$q_r$ is the greatest integer satisfying $x_{n_r} \geqslant 2.(B_r)^{q_r}$.

Clearly $\{q_r\}_{r=0}^{\infty}$ is increasing and $2(B_r)^{q_r} \leqslant x_{n_r} < 2(B_{r+1})^{q_{r+1}}$ for every positive integer $r$.

Finally define the sequence $v:\{1,2,3,\ldots\} \to \{0,1\}$ as follows:

for $1 \leq n < 2(B_1)^{q_1}$ : $v(n) = 0$

for $2(B_r)^{q_r} \leq n < 2(B_{r+1})^{q_{r+1}}$ :

$$v(n) = \begin{cases} 0 & \text{if } n, 2B_r \text{ are coprime} \\ 1 & \text{if } n, 2B_r \text{ are not coprime} . \end{cases}$$

It is easy to see that $v \in V$ .

Now choose any $x_{n_r}$ and let $b$ be the integer for which $b.2(B_r)^{q_r} \leq x_{n_r} < (b+1).2(B_r)^{q_r}$. If $c \leq b.2(B_r)^{q_r}$ and $c, 2B_r$ are coprime then $v(c) = 0$ .

So that

$$N_v(b.2(B_r)^{q_r}) \geq \left| \{ c \leq b.2(B_r)^{q_r} \mid c, 2B_r \text{ are coprime} \} \right| =$$

$$= b.\varphi(2(B_r)^{q_r}) = b(B_r)^{q_r} . \prod_{j=1}^{r} (1 - \frac{1}{p_j})$$

and therefore

$$\frac{N_v(x_{n_r})}{f(x_{n_r})} = \frac{N_v(x_{n_r})}{x_{n_r}} . \frac{x_{n_r}}{f(x_{n_r})} > \frac{N_v(b.2(B_r)^{q_r})}{(b+1)2(B_r)^{q_r}} . \frac{x_{n_r}}{f(x_{n_r})} \geq$$

$$\frac{b(B_r)^{q_r} . \prod_{j=1}^{r} (1 - \frac{1}{p_j})}{(b+1)2(B_r)^{q_r}} . \frac{x_{n_r}}{f(x_{n_r})} \geq \frac{b}{(b+1).2} \geq \frac{1}{4} .$$

Therefore we have found $v \in V$, such that $\frac{N_v(x_{n_r})}{f(x_{n_r})} > \frac{1}{4}$ for $r = 1,2,\ldots$ , where $x_{n_r} \to \infty$ as $r \to \infty$ . This means that $\lim_{x \to \infty} \frac{N_v(x)}{x} = 0$ does not hold for our sequence $v$ .

In other words, using only Filaseta's theorem, we are only able to prove properties of w which are common to all $v \in V$. We can sum up our results as follows:

Given any function $f:(0,\infty) \to (0,\infty)$, such that $\limsup_{x\to\infty} \frac{x}{f(x)} = \infty$, Filaseta's theorem is insufficient to deduce that $\lim_{x\to\infty} \frac{N(x)}{f(x)} = 0$. Therefore the result of Granville and Heath-Brown cannot be improved in this manner.

## REFERENCES


1. G.Faltings: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math., 73 (1983), 349-366.
2. M.Filaseta: An application of Faltings' results to Fermat's last theorem, C.R. Math. Rep. Acad. Sci. Canada, 6 (1984), 31-32 .
3. A.Granville: The set of exponents, for which Fermat's last theorem is true, has density one, C. R. Math. Rep. Acad. Sci. Canada, 7 (1985), 55-60 .
4. D.R.Heath-Brown: Fermat's last theorem for "almost all" exponents, Bull. London Math. Soc., 17 (1985), 15-16 .


Received November 20, 1990

Department of Mathematics
Masaryk University

# La clôture séparable du corps des séries formelles généralisées

Ali BENHISSI

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

**Resumé :**

On explicite une clôture séparable du corps des séries formelles généralisées en caractéristique non nulle et on met en évidence un moyen de construction d'éléments algébriques sur ce corps.

**Théorème :**

Soient K un corps de caractéristique p non nulle, de clôture algébrique $\overline{K}$ et de clôture séparable $K_o$ et G un groupe abélien totalement ordonné d'enveloppe divisible $\Delta(G)$.

On note $\widetilde{K}$ le sous-corps de $\overline{K}((T^{\Delta(G)}))$ obtenu par adjonction à $K((T^G))$ de :

i) $K_o$

ii) $T^{g/n}$, où $n \in \mathbb{N}$, $(n,p) = 1$, $g \in G^-$, g non n-divisible.

iii) les racines successives des polynômes irréductibles : $x^p - x - f(T)$.

Alors $\widetilde{K}$ est une clôture séparable de $K((T^G))$.

**Remarques :**

1) Soit $K_1$ le corps obtenu par adjonction à $K((T^G))$ des éléments decrits dans i) et ii).

Pour $n \geq 1$, on définit $K_{n+1}$, comme étant le corps de racines sur $K_n$ des polynômes irréductibles de la forme : $X^p - X - f(T)$, avec $f(T) \in K_n$.

On a : $\overline{K} = \bigcup_{n:1}^{\infty} K_n$.

2) La clôture algébrique de $K((T^G))$ s'obtient à partir de $\widetilde{K}$ par extraction des racines $p^n$ ème :

$$\left( \sum_{\alpha} a_\alpha T^\alpha \right)^{1/p^n} = \sum_{\alpha} a^{1/p^n} T^{\frac{\alpha}{p^n}}.$$

**Proposition :**

Soient L/K une extension de corps, $G \subset G'$ deux groupes abéliens totalement ordonnés et

$f \in L((T^{G'}))$ algébrique sur $K((T^G))$ :

$f^{n+1} = \sum_{i:0}^{n} g_i f^i$, où les $g_i \in K((T^G))$.

On suppose que f est tous les $g_i$ sont de valuations strictement positives.

Soit $(\lambda_n)_{n\in\mathbf{N}}$ une suite d'éléments de K.

Alors la série de Neumann : $\sum_{m:0}^{\infty} \lambda_m f^m$ de $L((T^{G'}))$ est algébrique sur $K((T^G))$.

**Remarque :**

Supposons $f \in L((T^{G'}))$ algébrique sur $K((T^G))$ : $f^{n+1} = \sum_{i:0}^{n} g_i f^i$, avec

$\min \{ v(g_i) / 0 \le i \le n \} = -\beta \le 0$ et $v(f) > 0$,

v étant la valuation naturelle de $L((T^{G'}))$. Soit $\alpha > \beta \ge 0$ dans G.

Alors : $(T^\alpha f)^{n+1} = \sum_{i:0}^{n} T^{(n-i+1)\alpha} g_i (T^\alpha f)^i$ , avec

$v(T^{(n-i+1)\alpha} g_i) = (n-i+1)\alpha + v(g_i) \ge (n-i+1)\alpha - \beta = (n-i)\alpha + \alpha - \beta > 0.$

On peut appliquer la proposition : pour toute suite $(\lambda_n)_{n\in\mathbf{N}}$ d'éléments de K, la série :

$\sum_{m:0}^{\infty} \lambda_m (T^\alpha f)^m$ est algébrique sur $K((T^G))$.

**Exemples :**

Soit K un corps de caractéristique p non nulle.

1) Soient s un élément négatif d'un groupe abélien totalement ordonné G et x un élément de K

algébrique sur son corps premier $\mathbb{F}_p$.

La série : $f = \sum_{i:1}^{\infty} x^i T^{\frac{s}{i} - s}$ est algébrique sur $K((T^G))$. Il existe $\alpha \in G_+$ tel que pour toute

suite $(\lambda_n)_{n\in\mathbb{N}}$ d'éléments de K , la série $\sum_{n:0}^{\infty} \lambda_n (T^\alpha f)^n$ est algébrique sur $K((T^G))$.

2) La série $f = \sum_{i:1}^{\infty} T^{1-p^{-i}}$ de $K((T^{Q}))$ est racine du polynôme :

$X^{p} - T^{p-1} X - T^{p-1} \in K((T))[X]$. Donc pour toute suite $(\lambda_n)_{n\in N}$ de K,

la série $\sum_{n:0}^{\infty} \lambda_n \left( \sum_{i:1}^{\infty} T^{1-p^{-i}} \right)^n$ est algébrique sur K((T)).

3) La série : $f = \sum_{n:0}^{\infty} (-1)^n T^{\rho_n}$, où $\rho_n = \dfrac{p^{n+1}-1}{(p-1)p^n}$, est racine de $X^{p} + T X + 1$ .

Donc $\sum_{m:0}^{\infty} \lambda_m \left( \sum_{n:0}^{\infty} (-1)^n T^{\rho_n+1} \right)^m$ est algébrique sur K((T)).

4) Soient $0 < n \le m$ deux entiers. La série $f = \sum_{i:1}^{\infty} T^{1-\frac{n}{mp^i}}$ est racine de

$X^{p^m} - T^{p^m-1} X - \sum_{i:0}^{m-1} T^{1-\frac{np^i}{m}}$ .

Soit $\alpha = \begin{cases} 0 \text{ si } \dfrac{np^{m-1}}{m} < 1 \\ \text{un entier} > \dfrac{np^{m-1}}{m} - 1 \quad \text{sinon} \end{cases}$

Alors pour toute suite $(\lambda_n)_{n\in IN}$ de K, la série $\sum_{n:0}^{\infty} \lambda_n (T^{\alpha} f)^n$ est algébrique sur $K((T^{1/m}))$, donc sur K((T)).

Received September 20, 1990

Faculté des Sciences de Monastir
Département de Mathathématiques
5019 Monastir , TUNISIE.

# SUR LE GROUPE DES CLASSES D'UN ANNEAU INTEGRE

Driss KOUR EL ABIDINE

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

***ABSTRACT**: In this paper we are interested in a generalization of Nagata's theorem [12] to a new class of domains other than Krull domains, the Mori domains and the PVMD domains (Theorem 1).*

## INTRODUCTION

Dans [4] et [5], on définit pour un anneau R intègre son groupe des classes Cl(R) = T(R)/P(R), où T(R) est l'ensemble des t-idéaux t-inversibles et P(R) est l'ensemble des idéaux fractionnaires principaux.

Soient R un anneau intègre et S une partie multiplicative de R. Si R est un anneau de Krull et S est engendrée par des éléments premiers, le théorème de Nagata affirme que $Cl(R_S) \approx Cl(R)$ [[12], Th.6.3].

S.Gabelli et M.Roitman ont montré le même résultat si R est un anneau 1-acc (Un anneau R est un 1-acc si et seulement si il vérifie la condition de chaînes ascendantes pour les idéaux principaux) [9]. Parmi les anneaux qui sont 1-acc, on trouvera les anneaux de Mori [8].

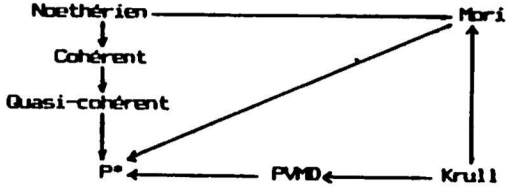
Si R est un anneau pseudo-prufférien (ou un PVMD), d'après [[1],Th.2.3] et [[11],Prop2.14], on peut déduire que $Cl(R_S) \approx Cl(R)$.

On désigne par P* la propriété suivante: Pour tout $I \in I_v(R)$ (L'ensemble des idéaux de type fini ), $I^{-1} \in D_v(R)$ (L'ensemble des idéaux v-fini), où $I^{-1}=R:I=(x\in Frac(R), xI\subset R)$. Si R vérifie P*, on montre aussi que $Cl(R_S)\approx Cl(R)$(théorème 1).

Mathematics Subject Classification: Primary 13 A 05; Secondary 13 B 20, 13 B 25.
Key words: Class-groups; krull domain.

On remarque que les anneaux de Krull, de Mori et PVMD vérifient P*.

On rappelle, qu'un R est dit cohérent si et seulement si l'intersection de deux idéaux de type fini est un idéal de type fini [10]. L'anneau R est dit quasi-cohérent si et seulement si pour tout I un idéal de type fini de R, R:I est de type fini [3]. L'anneau R est dit de Mori [8] si et seulement si il vérifie la condition de chaînes ascendantes pour les idéaux entiers divisoriels. L'anneau R est dit de Krull si et seulement si R est un anneau de Mori complètement intégralement clos [7]. L'anneau R est dit un PVMD si et seulement si $D_f(R)$ est un v-groupe [13]. Pour mettre en évidence l'utilité d'étudier la propriété P*, nous donnons un diagramme complet entre les classes d'anneaux vérifiant P* :




NOTATION - TERMINOLOGIE

Soient R un anneau intègre et F(R) l'ensemble des idéaux fractionnaires de R. Etant donné I un idéal fractionnaire de F(R), on note: $I_v = R:(R:I)$ et $I_t = \cup J_v$, où J parcourt l'ensemble des idéaux de type fini contenus dans I. On dit que: - I est un t-idéal si $I = I_t$. - I est un idéal divisoriel v-fini (ou simplement v-fini) si $I = J_v$ où J est un idéal de type fini contenu dans I. On note: Cart(R) est l'ensemble des idéaux inversibles de R, $\mathcal{G}(R)$ est l'ensemble des t-idéaux de R, D(R) est l'ensemble des idéaux divisoriels de R, $D_f(R)$ est

l'ensemble des idéaux (divisoriels) v-fini de R, $I_f(R)$ est l'ensemble des idéaux de type fini de R et P(R) est l'ensemble des idéaux principaux de R.

On définit dans $\mathcal{G}(R)$, l'opération $I.J = (IJ)_t$. On dit qu'un t-idéal I est t-inversible dans $\mathcal{G}(R)$, s'il existe un t-idéal J tel que $(IJ)_t = R$. Désignons par T(R) l'ensemble des t-idéaux t-inversibles de R. Comme dans [4] et [5], on appelle le groupe des classes de l'anneau R, le groupe Cl(R)= T(R)/P(R)

Tous les anneaux considérés, sont supposés commutatifs, intègres et unitaires.

## 1] Sur une généralisation du théorème de Nagata

On aura besoin de quelques résultats classiques, qu'on va les citer sans démonstration mais avec une référence précise.

**Définition:** Soient R un anneau intègre et I un idéal de R. On dit que I est transportable [4] et [11], si pour toute extension plate de R on a: $(R:I)B = B:IB$.

**Proposition 1.** *Soient R un anneau et B est une extension plate de R et I un idéal de R:*

*a) Si I est transportable, alors : $(I_vB)_v = (IB)_v$.*

*b) Si I et $I^{-1}$ sont transportables, alors $(IB)_v = I_vB$.*

*c) Si I est transportable, alors $I_v$ est transportable.*

*d) Tout idéal v-fini ou de type fini est transportable.*

*e) Si I et J sont v-fini, alors IJ est transportable.*

*Voir [11], lemme 2.6 page 69.*

**Théorème 1.** *Soit R un anneau intègre vérifiant $P^*$. Si S est une partie multiplicative engendrée par des éléments premiers de R, alors $Cl(R_S) \simeq Cl(R)$.*

Lemme 1. *Soit $R$ un anneau intègre. Si $S$ est une partie multiplicative engendrée par des éléments premiers de $R$, alors pour tout $I \in D_f(R)$ tel que $I^{-1} \in D_f(R)$, on a: $IR_S$ est principal si et seulement si $I$ est principal.*

**Preuve:** La démonstration de ce lemme, repose sur un résultat de D.D.ANDERSON et D.F.ANDERSON [[1], Th.2.3].

**Preuve du théorème 1:**

D'après le lemme 1, il suffit de montrer que l'application $\mu$ définie par : $Cl(R) \longrightarrow Cl(R_S)$, $[I] \longmapsto [IR_S]$ est surjective.

Soit $I \in T(R_S)$, un t-idéal t-inversible de $R_S$. On peut écrire $I = (JR_S)_v$, où $J$ est un idéal de type fini de $R$. De même $I^{-1} = (J_1R_S)_v$, où $J_1$ est un idéal de type fini de $R$. On a : $(II^{-1})_t = (II^{-1})_v = (JJ_1R_S)_v = R_S$. Posons $K = JJ_1$. Puisque $R$ vérifie $P^*$, $K^{-1} \in D_f(R)$. D'après la proposition 1, on déduit que $K$ et $K^{-1}$ sont transportables et ce qui donne d'après (b) prop 1), $(KR_S)_v = K_vR_S$. Ça découle du lemme1 que $K_v$ est principal. Par conséquent, il existe $d \in Frac(R)$ tel que $K_v = (JJ_1)_v = dR$. D'où $(J.J_1/d)_v = (J.J_1/d)_t = (J_t.J_1/d)_t = (J_v.J_1/d)_t = R$, ce qui donne que $J_v \in T(R)$. Finalement, on obtient $I = (JR_S)_v = J_vR_S$ (prop 1), car $J$ et $J^{-1}$ sont transportables. D'où $\mu$ est surjective.

Remarque .

a) Si $R$ est un anneau de Mori, donc $R$ vérifie $P^*$, en particulier les anneaux noethériens et les anneaux de Krull. Ainsi, on retrouve le théorème de Nagata [[12],Th.6.3].

b) Il y a une grande classe d'anneaux vérifiant le théorème 1 autres que les anneaux de Mori, on trouvera Les anneaux quasi-

cohérents [3], en particulier les anneaux cohérents [10].

■

Pour compléter le contenu de ce travail, il est intéressant de donner des exemples vérifiant $P^*$ qui ne sont pas des anneaux 1-acc (En particulier non de Mori ), ni PVMD ( voir exemple 1). Aussi, de donner des exemples vérifiant $P^*$ qui ne sont pas quasi-cohérents (voir exemple 2).

**Exemple 1.** Soit A un anneau noethérien non intégralement clos. Considérons l'anneau $R = A[X]+YK[Y]$, où $K = Frac(A[X])$. La suite $(Y.1/X) \subsetneq (Y.1/X^2) \subsetneq \ldots (Y.1/X^n) \subsetneq (Y.1/X^{n+1}) \subsetneq \ldots$ n'est pas stationnaire dans R, car X n'est pas inversible dans R, ce qui montre que R n'est pas un 1-acc. On a:

a) R est un anneau cohérent [6], par suite il vérifie $P^*$.

b) R n'est pas un 1-aac, donc non de Mori.

c) R n'est pas un PVMD [2].

■

**Exemple 2.** Soient K un corps et $(X_n)_{n\geq 1}$ des indéterminées sur le corps K. Considérons l'anneau $B = K[X_nX_m]_{(n\geq 1, m\geq 1)}$. L'anneau $C = K[X_n]_{n\geq 1}$ est entier sur B car $X_n^2 \in B$. On remarque que $B = C \cap Frac(B)$ ( Frac(B) désigne le corps des fractions de B ), d'après [[7], prop 2], B est anneau de Krull. L'idéal $p = X_1C \in X^1(C)$ ( $X^1(C)$ désigne l'ensemble des idéaux premiers de C de hauteurs 1), donc $q = p \cap B \in X^1(B)$. D'après [[12],Lemme3.3], $q \in D(B)$. On remarque que $q = (\Sigma X_1X_nB)_{n\geq 1}$ n'est pas de type fini. Posons $I = B:q$. Puisque B est de Mori, il existe $J \in I_v(B)$ tel que $J \subset I$ et $B:J = B:I = B:(B:q) = q_v = q$. Finalement, on obtient $J \in I_v(B)$ et $J^{-1} \notin I_v(B)$, ce qui montre que B n'est pas quasi-cohérent, par contre B vérifie $P^*$.

■

BIBLIOGRAPHIE

[1] D.D.ANDERSON and D.F.ANDERSON. Some remarks on star operations and the class group, J.Pure Appl.Algebra 51 (1988), 27 - 33.

[2] D.F.ANDERSON and A.RYCKAERT. The Class Group of "D+M", J.Pure Appl.Algebra 52 (1988) 199 - 212.

[3] V.BARUCCI, D.F.ANDERSON and D.E.DOBBS. Coherent Mori Domains and the Principal Ideal Theorem, Comm.Algebra, 15(6), 1119 - 1156 (1987).

[4] A.BOUVIER. Le groupe des classes d'un anneau intègre, 107ème Congrès National des sociétés Savantes Brest,(1982), fasc V,(85-92).

[5] A.BOUVIER and M.ZAFRULLAH. On The Class Group of an integral domain, Preprint.

[6] J.BREWER and E.RUTTER. "D+M" construction with general overring, Michigan Math.J 23 (1976), 33-42.

[7] FOSSUM.R . The divisor class group of a Krull domain, Springer-Verlag, 1973.

[8] S.GABELLI. On divisorial ideal in polynomial rings over Mori Domains, Comm.Algebra 15 (11) 2349-2370 (1987).

[9] S.GABELLI and M.ROITMAN: On Nagata's theorem, to appear in J.Pure Appl.Algebra.

[10] J.P.LAFON. Les formalismes fondamentaux de l'algèbre commutative, Herman, 1974.

[11] A.RYCKAERT. Sur le groupe des classes et le groupe local d'un anneau intègre. Thèse de Doctorat, université Claude Bernard Lyon 1 (1986).

[12] P.SAMUEL. Lectures on unique factorisation domain, Tata Institut, Bombay 1964.

[13] M.ZAFRULLAH. On finite conductor domains, Manuscipta Math.24, 191-204, (1978).

Je tiens à remercier D.F.Anderson et S.Gabelli pour les informations qu'ils m'ont communiquées par lettre.

Département de Mathématique
Université Claude Bernard Lyon 1
43, Boulevard du 11 Novembre 1918
69622 Villeurbanne FRANCE

Received July 16, 1990

# Fixed Point Subalgebras Of The Rotation Algebra

Carla FARSI and Neil WATLING

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

**ABSTRACT:** Here we classsify the fixed point subalgebras of the rotation algabra $\mathcal{A}_\theta$ under the automorphisms induced by $SL(2,\mathbb{Z})$ in the standard representation. We then give a general characterization of those fixed point subalgebras for $\theta$ rational.

In this note we are concerned with the fixed point subalgebras of the rotation algebra $\mathcal{A}_\theta$, the universal $C^*$- algebra generated by two unitaries $u$ and $v$ satisfying $vu = \rho uv$ with $\rho = e^{2\pi i\theta}$ and $0 \leq \theta < 1$, induced by $SL(2,\mathbb{Z})$, where any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$ gives the automorphism $\tau_A$ of $\mathcal{A}_\theta$

$$\tau_A(u) = e^{ac\pi i\theta}u^a v^c,\ \tau_A(v) = e^{bd\pi i\theta}u^b v^d.$$

These subalgebras are interesting for several reasons. Firstly, are any AF algebras? This would provide another example of an AF algebra which is a subalgebra of a non-AF algebra. Secondly, concerning mathematical physics, they may provide more information about the almost Mathieu operator, $H = U + U^* + \beta(V + V^*)$. For example, $H$ is an element of the fixed point subalgebra induced by $-I \in SL(2,\mathbb{Z})$, so knowledge of this algebra would be desirable. This special case was considered in [1] and [2] with computation of the $K$-theory for $\theta$ irrational in [7].

## 1 The Action of $SL(2,Z)$ on $\mathcal{A}_\theta$

**Definition 1.0.1** *Define $T$, $R$, $U \in SL(2,\mathbb{Z})$ by,*

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \; U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

**Remark 1.0.2** *We have,*

$$T^2 = -I_2, \; T^3 = -T, \; T^4 = I_2,$$

$$R^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \; R^3 = -I_2, \; R^4 = -R, \; R^5 = -R^2, \; R^6 = I_2.$$

*Note also that* $\mathrm{Trace}(T) = 0$, $\mathrm{Trace}(R) = 1$, $\mathrm{Trace}(R^2) = -1$ *and* $\mathrm{Trace}(U) = 2$.

**Remark 1.0.3** *We will also call* $\tau_T$ *the 'square root of the flip',* $\tau_{T^2}$ *the 'flip',* $\tau_R$ *the 'cube root of the flip' and* $\tau_{R^2}$ *the 'cubic automorphism' (c.f. [2], [3], [4], [5]).*

The following theorem classifies all the finite order elements of $SL(2,\mathbb{Z})$ up to conjugacy class. (See [8] for a proof.)

**Theorem 1.0.4** *The finite order elements of* $SL(2,\mathbb{Z})$ *have* $\mathrm{Trace} = 0, \pm 1, \pm 2$. *If* $A \in SL(2,\mathbb{Z})$ *then,*

1. *If* $\mathrm{Trace}(A) = 0$, *then* $A$ *is conjugate in* $SL(2,\mathbb{Z})$ *to* $\pm T$.
2. *If* $|\mathrm{Trace}(A)| = 1$, *then* $A$ *is conjugate in* $SL(2,\mathbb{Z})$ *to* $\pm R$ *or* $\pm R^2$.
3. *If* $|\mathrm{Trace}(A)| = 2$, *and* $A^n \neq I_2$ *for any* $n \in \mathbb{Z}$, *then* $A$ *is conjugate in* $SL(2,\mathbb{Z})$ *to* $\pm U^n$ *for some* $n \in \mathbb{Z}$.
4. *If* $|\mathrm{Trace}(A)| = 2$, *and* $A^n = I_2$ *for some* $n \in \mathbb{Z}$, *then* $A = \pm I_2$.

**Definition 1.0.5** *If* $A \in SL(2,\mathbb{Z})$, *we define* $\mathcal{A}_\theta^A$ *to be the fixed point subalgebra of the automorphism* $\tau_A$ *of* $\mathcal{A}_\theta$.

**Lemma 1.0.6** *Let $A, B \in SL(2,\mathbb{Z})$. Then,*

1. *If $A$ is conjugate to $B$ in $SL(2,\mathbb{Z})$, then $\mathcal{A}_\theta^A \cong \mathcal{A}_\theta^B$.*
2. *If $A^n = B$ for some $n \in \mathbb{Z}$, then $\mathcal{A}_\theta^A$ is a subalgebra of $\mathcal{A}_\theta^B$.*

We can now classify all the fixed point subalgebras $\mathcal{A}_\theta^A$, where $A$ is a finite order element of $SL(2,\mathbb{Z})$.

**Theorem 1.0.7** *1. Let $A \in SL(2,\mathbb{Z})$ with $\mathrm{Trace}(A) = 0$. Then $\mathcal{A}_\theta^A \cong \mathcal{A}_\theta^T$.*

2. *Let $A \in SL(2,\mathbb{Z})$ with $|\mathrm{Trace}(A)| = 1$. Then $\mathcal{A}_\theta^A \cong \mathcal{A}_\theta^R$ or $\mathcal{A}_\theta^A \cong \mathcal{A}_\theta^{R^2}$ (which in turn are not isomorphic).*
3. *Let $A \in SL(2,\mathbb{Z})$ with $A^n = I_2$ for some $n \in \mathbb{Z}$ and $\mathrm{Trace}(A) = +2, -2$. Then $\mathcal{A}_\theta^A$ is isomorphic to $\mathcal{A}_\theta$ and $\mathcal{A}_\theta^{T^2}$ respectively.*

**Proof.** For part 1., by Theorem 1.0.4 $A$ is conjugate in $SL(2,\mathbb{Z})$ to either $T$ or $-T$. By Lemma 1.0.6 and Remark 1.0.2 we are done. 2. and 3. follow similarly.□

# 2 Fixed Point Algebras

We firstly describe the situation for the infinite order elements of $SL(2,\mathbb{Z})$.

**Theorem 2.0.8** *1. If $A \in SL(2,\mathbb{Z})$ with $|\mathrm{Trace}(A)| > 2$, then $\mathcal{A}_\theta^A \cong \mathbb{C}$.*

2. *If $A \in SL(2,\mathbb{Z})$, $A \neq I_2$, with $\mathrm{Trace}(A) = +2$, then $\mathcal{A}_\theta^A \cong C(S^1)$.*
3. *If $A \in SL(2,\mathbb{Z})$, $A \neq -I_2$, with $\mathrm{Trace}(A) = -2$, then $\mathcal{A}_\theta^A \cong C([-2,+2])$.*

For the proof of this theorem see [6] and also [9] for 1. in the irrational case. Now we will describe explicitly the fixed point algebras $\mathcal{A}_\theta^T$, $\mathcal{A}_\theta^{R^2}$, $\mathcal{A}_\theta^R$ of Section 1 when $\theta$

is rational. Note that $\mathcal{A}_\theta^{T^2}$ was described in [2]. The proof of the following theorem is given in [3], [4], [5].

**Theorem 2.0.9** *Let $\theta = p/q$, with $p, q$ coprime positive integers and let $\Omega_i$, $i = 0,1,2$ be any three distinct points of the 2-sphere $S^2$. Then the fixed point subalgebras of the square root of the flip $\tau_T$, $\mathcal{A}_\theta^T$, the cubic automorphism $\tau_{R^2}$, $\mathcal{A}_\theta^{R^2}$, and the cube root of the flip $\tau_R$, $\mathcal{A}_\theta^R$, are isomorphic to the following subalgebras of the $C^*$-algebra $C(S^2, M_q)$:*

$$\begin{aligned}
\mathcal{A}_\theta^T &= \{f \in C(S^2, M_q) \mid f(\Omega_i) \text{ commutes with } P_i^j,\ i = 0,1,2,\ j = 0,1,2\},\\
\mathcal{A}_\theta^{R^2} &= \{f \in C(S^2, M_q) \mid f(\Omega_i) \text{ commutes with } Q_i^j,\ i = 0,1,2,\ j = 0,1\},\\
\mathcal{A}_\theta^R &= \{f \in C(S^2, M_q) \mid f(\Omega_i) \text{ commutes with } S_i^j,\ i = 0,1,2,\ j = 0,1,2,3,4\},
\end{aligned}$$

*where $P_i^j$, $Q_i^j$ and $S_i^j$ are orthogonal families of self-adjoint projections in $M_q$. Their dimensions are given in the following tables, where $q$ is modulo 12 unless otherwise stated:*

| $\mathcal{A}_\theta^T$ | $q \equiv 0 (\mathrm{mod}4)$ | $q \equiv 1 (\mathrm{mod}4)$ | $q \equiv 2 (\mathrm{mod}4)$ | $q \equiv 3 (\mathrm{mod}4)$ |
|---|---|---|---|---|
| $P_0^0$ | $\frac{q}{2}$ | $\frac{q-1}{2}$ | $\frac{q}{2}$ | $\frac{q-1}{2}$ |
| $P_0^1$ | 0 | 0 | 0 | 0 |
| $P_0^2$ | 0 | 0 | 0 | 0 |
| $P_1^0$ | $\frac{q}{4}$ | $\frac{q-1}{4}$ | $\frac{q+2}{4}$ | $\frac{q+1}{4}$ |
| $P_1^1$ | $\frac{q-4}{4}$ | $\frac{q-1}{4}$ | $\frac{q-2}{4}$ | $\frac{q-3}{4}$ |
| $P_1^2$ | $\frac{q}{4}$ | $\frac{q-1}{4}$ | $\frac{q-2}{4}$ | $\frac{q+1}{4}$ |
| $P_2^0$ | $\frac{q}{4}$ | $\frac{q-1}{4}$ | $\frac{q-2}{4}$ | $\frac{q+1}{4}$ |
| $P_2^1$ | $\frac{q}{4}$ | $\frac{q-1}{4}$ | $\frac{q-2}{4}$ | $\frac{q-3}{4}$ |
| $P_2^2$ | $\frac{q}{4}$ | $\frac{q-1}{4}$ | $\frac{q+2}{4}$ | $\frac{q+1}{4}$ |

| $\mathcal{A}_\theta^{R^2}$ | $q \equiv 0, 6$ | $q \equiv 1, 5, 7, 11$ | $q \equiv 2, 4, 8, 10$ | $q \equiv 3, 9$ |
|---|---|---|---|---|
| $Q_0^0$ | $\frac{q}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q}{3}$ |
| $Q_0^1$ | $\frac{q}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q+2(q\|3)}{3}$ | $\frac{q}{3}$ |
| $Q_1^0$ | $\frac{q}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q+2(q\|3)}{3}$ | $\frac{q+3}{3}$ |
| $Q_1^1$ | $\frac{q}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q-3}{3}$ |
| $Q_2^0$ | $\frac{q}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q}{3}$ |
| $Q_2^1$ | $\frac{q}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q+2(q\|3)}{3}$ | $\frac{q}{3}$ |

| $\mathcal{A}_\theta^{R}$ | $q \equiv 0,6$ | $q \equiv 1, 5, 7, 11$ | $q \equiv 2, 4, 8, 10$ | $q \equiv 3, 9$ |
|---|---|---|---|---|
| $S_0^0$ | $\frac{q-6}{6}$ | $\frac{q-3+2(q\|3)}{6}$ | $\frac{q+3-(q\|3)}{6}$ | $\frac{q-3}{6}$ |
| $S_0^1$ | $\frac{q}{6}$ | $\frac{q-(q\|3)}{6}$ | $\frac{q-3-(q\|3)}{6}$ | $\frac{q-3}{6}$ |
| $S_0^2$ | $\frac{q}{6}$ | $\frac{q-(q\|3)}{6}$ | $\frac{q-3-(q\|3)}{6}$ | $\frac{q-3}{6}$ |
| $S_0^3$ | $\frac{q}{6}$ | $\frac{q-(q\|3)}{6}$ | $\frac{q+2(q\|3)}{6}$ | $\frac{q+3}{6}$ |
| $S_0^4$ | $\frac{q}{6}$ | $\frac{q-(q\|3)}{6}$ | $\frac{q+2(q\|3)}{6}$ | $\frac{q+3}{6}$ |
| $S_1^0$ | $\frac{q}{2}$ | $\frac{q-1}{2}$ | $\frac{q}{2}$ | $\frac{q-1}{2}$ |
| $S_1^1$ | 0 | 0 | 0 | 0 |
| $S_1^2$ | 0 | 0 | 0 | 0 |
| $S_1^3$ | 0 | 0 | 0 | 0 |
| $S_1^4$ | 0 | 0 | 0 | 0 |
| $S_2^0$ | $\frac{q}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q}{3}$ |
| $S_2^1$ | $\frac{q}{3}$ | $\frac{q-(q\|3)}{3}$ | $\frac{q+2(q\|3)}{3}$ | $\frac{q}{3}$ |
| $S_2^2$ | 0 | 0 | 0 | 0 |
| $S_2^3$ | 0 | 0 | 0 | 0 |
| $S_2^4$ | 0 | 0 | 0 | 0 |

**Corollary 2.0.10** *Let $\theta = p/q$, where $p, q$ are coprime positive integers. Then the $K$-theory of $\mathcal{A}_\theta^T$, $\mathcal{A}_\theta^{R^2}$, $\mathcal{A}_\theta^R$, is given by,*

| | $q=1$ | $q=2$ | $q=3$ | $q=4$ | $q=5$ | $q=6$ | $q>6$ |
|---|---|---|---|---|---|---|---|
| $K_0(\mathcal{A}_\theta^T)$ | $\mathbb{Z}^2$ | $\mathbb{Z}^5$ | $\mathbb{Z}^7$ | $\mathbb{Z}^8$ | $\mathbb{Z}^9$ | $\mathbb{Z}^9$ | $\mathbb{Z}^9$ |
| $K_0(\mathcal{A}_\theta^{R^2})$ | $\mathbb{Z}^2$ | $\mathbb{Z}^5$ | $\mathbb{Z}^7$ | $\mathbb{Z}^8$ | $\mathbb{Z}^8$ | $\mathbb{Z}^8$ | $\mathbb{Z}^8$ |
| $K_0(\mathcal{A}_\theta^R)$ | $\mathbb{Z}^2$ | $\mathbb{Z}^5$ | $\mathbb{Z}^7$ | $\mathbb{Z}^8$ | $\mathbb{Z}^9$ | $\mathbb{Z}^9$ | $\mathbb{Z}^{10}$ |

*and,*

$$K_1(\mathcal{A}_\theta^T) = 0,\ K_1(\mathcal{A}_\theta^{R^2}) = 0,\ K_1(\mathcal{A}_\theta^R) = 0.$$

# 3 References


[1 ] O. Bratteli, G.A. Elliott, D.E. Evans and A. Kishimoto, *Non commutative spheres I*, Int. Jour. of Math., to appear.

[2 ] O. Bratteli, G.A. Elliott, D.E. Evans and A. Kishimoto, *Non commutative spheres II, Rational Rotations*, J. Operator Theory, to appear.

[3 ] C. Farsi and N. Watling, *Quartic algebras*, Can. J. Math, to appear.

[4 ] C. Farsi and N. Watling, *Cubic algebras*, preprint.

[5 ] C. Farsi and N. Watling, *Elliptic algebras*, preprint.

[6 ] C. Farsi and N. Watling, *Irrational quartic algebras*, in preparation.

[7 ] A. Kumjian, *On the K-theory of the symmetrized non-commutative torus*, C. R. Math. Rep. Acad. Sci. Canada 12 (1990), 87-89.

[8 ] B. Schoeneberg, *Elliptic modular functions*, Springer–Verlag, New York, 1974.

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



Carla Farsi, Department of Mathematics, University of Toronto, Toronto, M5S 1A1.

Neil Watling, Department of Mathematics, SUNY at Buffalo, Buffalo, New York 14214.


Received March 25, 1991

# A POLYNOMIAL DECOMPOSITION ALGORITHM OVER FACTORIAL DOMAINS

Jaime Gutiérrez

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

**Abstract**.- In this paper we present an algorithm to decompose a polynomial $f(X) \in D[X]$, where D is a factorial domain. In particular we solve a generalization of the decomposition problem to multivariate polynomials. The given algorithms only work when the characteristic of D does not divide the degree of $f(X)$.

**§1. Introduction**.- The functional decomposition problem over F[X] (F a field) can be stated as follows: given $f(X) \in F[X]$ of degree $n=rs$, to determine whether there exist $g(X), h(X) \in F[X]$ of degrees r,s respectively, such that $f(X)=g(X) \circ h(X)=g(h(X))$ and, in the affirmative case, to compute them. For some time, this problem was considered to be *computationally hard*, but since 1987 there are several polynomial-time algorithms working in the "tame" case, i.e. when the characteristic of F does not divide r, ( see Gathen el al. (1987), (Gutiérrez el al.(1988)).

Regarding extensions of this important problem, recently Kozen & Landau (1989) have found (in the tame case) a solution when the polynomial f(X) has coefficients in a commutative ring, but assuming that the polynomial involved is monic.

On the other hand several generalizations of the decomposition problem have been posed for multivariate polynomials, see Barton & Zippel(1985). This seems more difficult than the decomposition

of univariate polynomials, but even partial solutions would be an aid to algebraic simplification and evaluation problems. Gathen (1987) solves the following problem: given $f(X) \in F[X_1,\ldots,X_m]$ of (total) degree $n=rs$, and $r$ not divisible by the characteristic of the field $F$, to determine when there exist $g(X)\in F[X]$ and $h(X)\in F[X_1,\ldots,X_m]$ of degrees $r,s$ respectively, such that $f(X_1,\ldots,X_m)=g(h(X_1,\ldots,X_m))$ and, in the affirmative case, to compute them.

Now, we remark that solving *in all generality* the problem of decomposition of polynomials in one variable over a factorial domain will imply the solution of the decomposition problem for polynomials in several variables over a field, in a sense different to the one above stated by Gathen, namely, considering the given polynomial as a polynomial having as coefficients polynomials in one less variable and proceeding to an iterative decomposition, once an ordering has been choosen in the variable (c.f. Definition 2.1 below). Moreover, every decomposition in the sense of Gathen is also a decomposition in the new sense of definition 2.1, but no conversely, as shown by the following example:

$$f(X,Y) = ((X^3+1)Y^2+ 2XY+ X^2+1)\circ(Y^2+Y+X) =$$
$$= (X^3+1)(Y^2+Y+X)^2 + 2X(Y^2+Y+X)+ X^2+1$$

is a decomposition in our sense but the polynomial $f$ is "indecomposable" according to Gathen's criterion. The solution of the decomposition problem for factorial domains is precisely the content of §3 of this paper. Besides we study and solve the more general problem of finding (and defining) a complete decomposition in indecomposable elements, stating some uniqueness results concerning this decomposition. As a consequence we can

recover Gathen's decomposition and clarify also some of the concepts of Kozen&Landau with regard to complete decompositions (which were obscure to us as they were stated over non neccessarily integrity domains, see Remark 2.2).

§2. Some general results.- Throughout this paper, we denote by D an unique factorization domain and by K its field of fractions. We consider the near-ring $(D[X],+,\circ)$, see Pilz (1983). The units in the near-ring D[X] are the linear polynomials $\alpha X+\beta$, where $\alpha$ is an unit in the ring D. As usual $D_0[X]$ will denote the set of all polynomials over R whose constant term is zero.

**Definitions 2.1.**- As in ring theory, we say that an element $f(X)\in D[X]$ is *indecomposable* provided that :

i) f(X) is non-constant and non-unit in the near-ring D[X].

ii) $f(X)= g(X)\circ h(X)$, $(g(X),h(X)\in R[X])$ implies g(X) or h(X) is an unit. Otherwise we say f(X) is *decomposable*.

A *complete decomposition* of f(X) is a set of polynomials $f_1(X),\ldots,f_r(X)\in D[X]$ such that $f(X)=f_1(X)\circ\ldots\circ f_r(X)$ and the $f_i(X)$'s are indecomposable.♦

If D=F is a field, every polynomial f(X) has complete decomposition in F[X], with a strong uniqueness property (see Gutiérrez et al. (1989) or Gathen (1987)).

**Remark 2.2.** Obviously the Definition 2.1 may be extended over an arbitrary commutative ring. Kozen&Landau give a "similarity" definition for an arbitrary commutative ring but this one does

not agree with Definition 2.1 when D is not an integral domain. In fact, if we take as $R=Z_4$ the ring of integers modulo 4: then $2X^4+X^3=X^3\circ(2X^2+X)$ is a decomposition ("tame case") in the sense of Kozen&Landau, but notice that $2X^2+X$ is an unit in $Z_4[X]$. Nevertheless Kozen&Landau's proof of their decomposition theorem over monic polynomials seems to use implicitly a concept of decomposable element that agrees with our Definition 2.1.

§3.**Decomposition over factorial domains**.- In this section we prove our main result, i.e. that if D is a factorial domain, then every polynomial in D[X] has a complete decomposition. The key lemma for proving the complete decomposition of f(X) is:

**Lemma 3.1**. Let $g(X),h(X)\in D_0[X]$ be primitive polynomials, then their composition is primitive.

**Theorem 3.2**. If $f(X)\in D_0[X]$ is primitive then f(X) is indecomposable in D[X] iff f(X) is indecomposable in K[X]. ♦

An immediate consequence of Theorem 3.2 is the complete decomposition of f(X).

**Algorithm**

Input: $f(X)=a_nX^n+a_{n-1}X^{n-1}+.....+a_1X+a_0 \in D[X]$ of degree n=rs, and r not divisible by the characteristic of D.

Output: $g(X),h(X)\in D[X]$ with $f(X)=g(X)\circ h(X)$ and $\deg(g(X))=r$, if such a decomposition exits; and "*no decomposition*" otherwise.

**A.1.** Find $\alpha,\beta\in D$ such that $f(X)=(\alpha X+\beta)\circ f'(X)$ where $f'(X)$ is primitive. Take $\alpha=$ G.c.d$(a_n,a_{n-1},\ldots,a_1)$, $\beta=a_0$.

**A.2.** Use the standard decomposition algorithm over $K[X]$, with input $f'(X)$. If no decomposition of $f'(X)$ in $K[X]$ exist, return "no decomposition".

If $f'(X)=g'(X)\circ h'(X)$ is returned with $h'(X)\in K_0[X]$ and monic, $h'(X)= X^s + (b_{s-1}/c_{s-1})X^{s-1}+\ldots\ldots+(b_1/c_1)X$, return $g(X)=(\alpha X+\beta)\circ g'(X)\circ(1/\delta)X$ and $h(X)=\delta X\circ h'(X)$, where

$$\delta=\text{L.c.m.}(c_{s-1},\ c_{s-2},\ldots,c_1\ ).$$

Using Lemma 3.1 and Theorem 3.2 we see that the algorithm correctly determines whether $f(X)\in D[X]$ has a decomposition with the required degrees, and if so, computes a decomposition.

If we suppose that G.c.d.(deg(f(X)),characteristic(D))=1, we obtain an algorithm to find a complete decomposition of $f(X)$.♦

**Corollary 3.3** Let $f(X)\in D[X]$, with G.c.d.(deg(f(X)),char(D))=1. The following holds:

(i) If $f(X)=g(X)\circ h(X)=g'(X)\circ h'(X)$ with deg(h(X))=deg(h'(X)) and $h(X),h'(X)\in D_0[X]$, then $h(X)$ and $h'(X)$ are associated in $K[X]$. (In particular, if they are indecomposable polynomials, then they are associated in $D[X]$)

(ii) If $f(X)=m_1(X)\circ m_2(X)\circ\ldots\circ m_r(X)\circ g_1(X)\circ g_2(X)\circ\ldots\circ g_u(X)$ and

$$f(X)=n_1(X)\circ n_2(X)\circ\ldots\circ n_s(X)\circ h_1(X)\circ h_2(X)\circ\ldots\circ h_v(X)$$ are

two complete decomposition of $f(X)$ with $\deg(m_i(X))=\deg(n_i(X))=1$ and $\deg(g_j(X))>1$, $\deg(h_j(X)>1$, then,

$m_1(X)\circ m_2(X)\circ\ldots\circ m_r(X)=n_1(X)\circ n_2(X)\circ\ldots\circ n_s(X)$ and r=s. Moreover,

$g_1(X) \circ g_2(X) \circ \ldots \circ g_u(X) = h_1(X) \circ h_2(X) \circ \ldots \circ h_v(X)$, $u=v$ and the sequences $\langle \deg(g_j(X)) \rangle$, $\langle \deg(h_j(X)) \rangle$ are permutations of each other.

*Proof*. Use Theorem 3.2. and the results about the "uniqueness" of a decomposition of a polynomial over a field, see Schinzel (1982) and Gutiérrez et al. or Gathen) ♦

## References

[1] Barton, R. & Zippel, R.: *Polynomial Decomposition algorithms*. J. Symbolic Computation 1, 159-168 (1985)

[2] Gathen, J. von zur.: *Functional decomposition of polynomials: the tame case*.Tech.Rep.13/1987,SFB124,Universität Saarbrücken (1987)

[3] Gathen,J.von zur&Kozen,D.&Landau,S.: *Functional decomposition of polynomials*. Proc. 28th Ann. IEEE Symp.Found. Comp. Sci.,127-131 (1987)

[4] Gutiérrez, J. & Recio, T. & Ruiz de Velasco, C.: *Polynomial decomposition algorithm of almost quadratic complexity*. Proc. of AAECC-6. (1988) L. N. Comp. Science, 357. Springer-Verlag, 471-476 (1989)

[5] Kozen, D. & Landau, S.: *Polynomial Decomposition Algorithms*. J. Symbolic Computation 7, 445-456 (1989)

[6] Pilz, G.: *Near-Rings*. 2nd revised Ed. Amsterdam, North- Holland Pub. Co. (1983)

[7] Schinzel, A. : *Selected Topics on polynomials*. Ann. Arbor, University of Michigan Press, (1982)

Received December 4, 1989

Depto. de Matemáticas, Estadística y Computación
Universidad de Cantabria, 39071-Santander, Spain

# An Approach to Wieferich's Condition

Masaharu Yamada

*Presented by J.B. Friedlander, F.R.S.C.*

The paper shows that the Wieferich condition for the first case of Fermat's Last Theorem, namely, $p^2$ divides $2^{p-1}-1$, can be deduced from just the first two of the Kummer-Mirimanoff congruences, rather than all of them as is usually done.

## 1. Some Preliminaries

Let p be an odd prime larger than 3. Let an integer q be the Fermat quotient with base 2 defined by $q=(2^{p-1}-1)/p$. Let $B_r$ be the Bernoulli numbers defined by

$B_r=\sum_{i=0}^{r}\binom{r}{i}B_i$ with $B_0=1$, then for $r < p-1$, all of them are p-integral, whereas $pB_{p-1} \equiv -1 \pmod p$.[1, von Staudt]

Let $F_j(X)$ be the Mirimanoff polynomials defined by

$$F_j(X)=\sum_{k=1}^{p-1}k^{j-1}(-X)^k, \text{ where } j=1,2,3,\cdots.$$

If a solution of a polynomial congruence such as $F_j(u)\equiv 0 \pmod p$ is not congruent to 0, -1 mod p, then the solution is

called a nontrivial zero of the congruence.

Let $L_k(X)=\sum_{i=1}^{b} g_{2i}(p-2i)^{k-1}B_{2i}F_{p-2i+1}(X)$,

and $M_k(X)=\sum_{i=1}^{b} g_{2i}(p-2i)^{k}B_{2i}F_{p-2i}(X)$,

where $g_{2i}=\binom{p-1}{2i}(2^{2i}-1)$ and $b=(p-3)/2$.

Let w be an integer defined by $w=((p-1)!+1)/p$. [1,Wilson]

Since $2qpB_{p-1}\equiv -2q+2pq(1+w) \pmod{p^2}$ and $F_{p-1}(1)\equiv -2q+2pqw \pmod{p^2}$ can be deduced from Lehmer's formulas [2], then

(1) $F_{p-1}(1) \equiv -2q \pmod{p}$ and $F_{p-1}(1) \equiv 2qpB_{p-1}-2pq \pmod{p^2}$.

Let $F(X)=\sum_{i=1}^{p-2} c_i X^i$ with integers $c_i=\binom{p-1}{i}-(-1)^i)/p$, which is related to $F_j(X)$ as follows.

(2) $F_1(X)=(X+1)^{p-1}-1-pF(X)$, and

(3) $F_{p-1}(X)\equiv -(X+1)F(X) \pmod{p}$.

Let $\Gamma$ be the following operator on polynomials of $Z_p[X]$:

$\Gamma(G) = XdG/dX$.

Since $F_{j+1}(X)=\Gamma[F_j(X)]$, then we obtain from (2)

(4) $F_2(X)\equiv -X(X+1)^{p-2} \pmod{p}$, and $F_3(X)\equiv X(X-1)(X+1)^{p-3} \pmod{p}$.

Also, from the definition

(5) $L_k(X)=\Gamma[M_{k-1}(X)]$.

Differentiate $-X^pF_2(X^{-1})+F_2(X)=pF_1(X)$, we obtain

(6) $(-1)^{j-1}X^pF_j(X^{-1})+F_j(X)\equiv(j-1)pF_{j-1}(X) \pmod{p^2}$, so that,

(7) $-X^pL_k(X^{-1})+L_k(X)\equiv pM_k(X) \pmod{p^2}$.

There is an identity [3,VIII-(3.2)], which is rewritten in our words as

(8) $$F_{p-1}(1)X^p=\frac{1}{2}(X+1)F_{p-1}(X)+\frac{X-1}{p-1}M_0(X)-\frac{2q}{p-1}(pB_{p-1})F_1(X).$$

Operating $\Gamma$ on both sides, we obtain

(9) $$F_{p-1}(1)(p-1)X^{p+1}-F_{p-1}(1)pX^p=-XF_{p-1}(X)+\frac{1}{2}(X^2-1)F_p(X)$$
$$+\frac{(X-1)^2}{p-1}L_1(X)+\frac{2qpB_{p-1}}{p-1}XF_1(X)-\frac{2qpB_{p-1}}{p-1}(X-1)F_2(X).$$

## 2. Common Zeros of $F_{p-1}(u)\equiv F_{p-2}(u)\equiv 0 \pmod p$

**Definition.** For a fixed p, let D be the set of all the nontrivial common zeros of $F_{p-1}(u)\equiv 0$ and $F_{p-2}(u)\equiv 0 \bmod p$.

**Lemma.** If $D \equiv u \pmod p$, then $D \equiv -u-1 \pmod p$.

**Proof.** The following is a formula of Mirimanoff cited from [3,VIII-(1.29)], and rewritten in our words.

$$-\frac{1}{2}[F_{p-1}(X)]^2 \equiv F_{p-2}(X)+(X+1)^{2p}F_{p-2}\left(\frac{X}{-X-1}\right) \pmod p.$$

Put X=u, and take account of (6), then

(10) $$F_{p-2}\left(\frac{u}{-u-1}\right)\equiv F_{p-2}\left(\frac{-u-1}{u}\right)\equiv 0 \pmod p.$$

There exists another Mirimanoff's formula [3,VIII-(1.26)]

such that

(11) $F_{p-2}(X) \equiv -X^p F_{p-2}(-1-X^{-1}) + F_{p-2}(-1-X) \pmod{p}$.

Put X=u, and take account of (10), then

$$F_{p-2}(-1-u) \equiv 0 \pmod{p}.$$

Next, since $F_{p-1}(X) \equiv -(X+1)F(X) \pmod{p}$ from (3), and since $(-X-1)F(X)=[(-X-1)^p+X^p+1]/p=XF(-X-1)$ from the definition of F(X), then

$$F_{p-1}(X) \equiv F_{p-1}(-X-1) \pmod{p},$$

which implies that $F_{p-1}(-u-1) \equiv 0 \pmod{p}$ for X=u.

Theorem.(a) If D is not empty for a given p, then $q=(2^{p-1}-1)/p \equiv 0 \pmod{p}$.(b)If $q \equiv 0 \pmod{p}$, then D is not empty.

Proof. Proof of (a).

The last lemma assures the existence of an element $u \neq D$ satisfying $u \neq 1 \pmod{p}$, so that, we assume $u \neq 1 \pmod{p}$ in the later part of the former proof.

Let q=np+r for some $n, r \in Z$, it follows from Lehmer's formulas (See, the vicinity of (1)) that

$$F_{p-1}(1) \equiv -2r-2p(n-wr) \pmod{p^2} \text{ and}$$

$$2qpB_{p-1} \equiv -2r-2p(n-wr-r) \pmod{p^2}.$$

Under the constraint of $p|F_{p-1}(u)$, the identity (9)

yields (using (2) and (4))

$$2ru^{p+1}+2p(n-wr)u^2-2pr(u^2-u)$$

$$\equiv -uF_{p-1}(u)+(1/2)(u^2-1)F_p(u)-(1+p)(u-1)^2L_1(u)$$

$$+2ruF_1(u)-2r(u-1)F_2(u)+2p(n-wr)(u-1)u/(u+1) \pmod{p^2}.$$

Replace u for $u^{-1}$, multiply $u^{p+2}$, and subtract the result from the original congruence. Then we obtain

$$2ru(u^p-1)-4pr(u^2-u)\equiv -p(u-1)^2M_1(u)-2r(u^2-1)F_2(u) \pmod{p^2},$$

where a relation $p|F_{p-2}(u)$ is used.

Dividing the result by u-1, and rearranging, we obtain

$$-p(u-1)M_1(u)\equiv 2r(u^p+u^{p-1}+\cdots+u)-4pru+2r(u+1)F_2(u) \pmod{p^2}.$$

Replace u for u+mp with an arbitrary integer m, expand the result, and take the difference of both, then we obtain

$$2r\{(p-1)u^{p-2}+(p-2)u^{p-3}+\cdots+1\}+2rF_2(u)+2r(u+1)F_3(u)/u$$
$$\equiv 0 \pmod{p}.$$

Since the contents inside the brackets may be written as $F_2(-u)/u$, then the congruence yields

$$2r\{F_2(-u)+uF_2(u)+(u+1)F_3(u)\}\equiv 0 \pmod{p}.$$

On account of (4), we obtain $-4ru^2/(u^2-1)\equiv 0 \pmod{p}$, which reduces $r\equiv 0 \pmod{p}$, that is, q is a multiple of p.

Proof of (b).

We obtain $F_{p-1}(1)\equiv 0$ and $F_{p-2}(1)\equiv 0 \pmod{p}$, by putting

$X=1$ on (I) and (II), respectively. That is, D includes 1, so that, D is not empty.

Corollary.

The Wieferich condition, namely, $p|q$, can be satisfied, if and only if a nontrivial zero exits between the first two of the Kummer-Mirimanoff congruences such as $F_{p-1}(u) \equiv F_2(u)F_{p-2}(u) \equiv 0 \pmod{p}$.

## References

1. See, for instance, G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford, fifth edition, 1984.

2. E. Lehmer, "On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson", Annals of Math. v. 39, 1938, pp. 350-359.

3. P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer, New York, 1979.

Received December 15, 1990

Faculty of Engineering
Ibaraki University
4-12-1 Nakanarusawa Machi,
Hitachi, Japan 316

# A LATTICE THEORETIC LOOK AT SOME RING THEORETICAL RADICALS

Isidore Fleischer

*Presented by J. Lambek, F.R.S.C.*

The system of (left–or bi–) ideals of a ring is closed under arbitrary intersection: it thus forms a complete lattice (indeed, a complete $\bigcap$–subsemilattice of the powerset of the ring.) It is also equipped with an ideal multiplication which distributes over join and for which a ring with 1 acts as a (left) identity. Certain properties of the radicals commonly studied do not appeal to the elements of the ring, thus can be formulated purely in this ideal lattice. A similar treatment can be carried through for the lattice of left congruences in semigroups; rather than a multiplication, this admits a residuation by elements. Radicals in lattice-ordered groups are defined by closure operators on the lattice of convex subgroups. The following attempts a consistently lattice theoretic study of these radicals. Chapter 1 operates in a complete join semilattice; in Chapter 2 this semilattice is in addition assumed to have a join–distributive multiplication; while Chapter 3 indicates some connections with the more familiar formulations using elements.

Chapter 1. Here we will be in the setting of a complete join semilattice $L$ with largest element E. Meets (written intersection $\bigcap$) exist when the terms have a common lower bound.

Call an element $J$ *small* [BH] if $H \neq E \longrightarrow H \vee J \neq E$ and call it I–*small* if $H \vee I \neq E \longrightarrow H \vee J \neq E$. Note that it suffices to formulate it for $H \supseteq I$, i.e., the $I$-small are just the superfluous mod $I$. The $I$-small form an ideal: $H \vee I \neq E \longrightarrow H \vee I \vee J \neq E \longrightarrow H \vee I \vee J \vee J' \neq E$.

The proposed *radical* is $\sqrt{I} = \bigvee\{J{:}J \text{ is I–small}\}$. This is increasing, $\sqrt{I} \supseteq I$, since $I$ is $I$-small, and isotone: $J \subseteq I \longrightarrow \sqrt{J} \subseteq \sqrt{I}$ since every $J$-small is $I$-small. It is not yet a closure operator since it lacks idempotence. Also, $\sqrt{I}$ could be $E$ for some $I \neq E$ unless $E$ were compact. By iterating the $\sqrt{\ }$ operation, one eventually reaches the smallest closure $\geq \sqrt{\ }$ (in the pointwise order of selfmaps on $L$); and if $E$ were compact, it would still be the closure only of itself. However, this can be achieved under weaker hypotheses, as we now show.

A maximal $M$ which includes $I$, includes every $I$-small $J$ – hence also $\sqrt{I}$ (and all its iterates). Indeed, $E \neq M \supseteq I$ entails $M \vee J \neq E$, hence $= M$ whence $J \subseteq M$. A partial converse: Every compact $C \subseteq \bigcap M \supseteq I$ is $I$-small (hence $\subseteq \sqrt{I}$). For suppose not: Then $H \vee C = E$ for some $I \subseteq H \neq E$. Surely $H$ does not $\supseteq C$, hence (by Zorn) is included in an $M$ maximal for not $\supseteq C$. This $M$ is maximal (since anything strictly larger includes both $H$ and $C$) and does not $\supseteq C$.

Thus, $\bar{I} = \bigcap M \supseteq I$, which is clearly a closure operator, is $\geq \sqrt{I}$. To have these coincide, it suffices to postulate that every $H \neq E$ is $\subseteq$ in some maximal $M$. For if $I \subseteq H \subseteq M$ then $H \vee \bar{I} \subseteq M \vee \bar{I} = M \neq E$ and so $\bar{I}$ would be $I$-small. As such, $\bar{I} \neq E$ for $I \neq E$; conversely, this entails that $I \subseteq$ some $M$. Moreoever, $\sqrt{I}$ is then the largest closure which does not send an $I \neq E$ to $E$; for if $\bar{I}'$ were another such, then $E = H \vee \bar{I}' \subseteq \overline{H \vee I}'$ only for $H \vee I = E$ whence $\bar{I}'$ would be $I$-small.

In summary: In a complete join semilattice with greatest $E$, in which each $H \neq E$ is contained in a maximal $M$, the join $\sqrt{I}$ of the $I$-small $J$ is itself $I$-small and coincides with the intersection of the maximal $M \supseteq I$. $\sqrt{\ }$ may also be characterized as the largest closure operator sending no $I \neq E$ to $E$.

Chapter 2. Now the join semilattice $L$ is to come equipped with a multiplication. Since this is to model the usual multiplication of left ideals in a ring, it is associative; the distributivity of ring multiplication over addition makes it appropriate to postulate the distributivity of this multiplication over (even infinite) joins (in each factor – of course this makes it isotone); finally, left multiplication is decreasing, $IJ \subseteq J$, which would already follow from only $EJ \subseteq J$. Equality could be postulated in rings with unit, in which it would be consistent to require also $IE \supseteq I$. The maximal elements then enjoy a property of primeness: if $IJ \subseteq M$ then $I$ or $J \subseteq M$: for if $I$ and $J$ are not $\subseteq M$ then $E = M \vee I \subseteq M \vee I(M \vee J) \subseteq M \vee IJ$, hence $IJ$ is not $\subseteq M$. Thus the $M$'s $\supseteq IJ$ are in the union of those $\supseteq I$ or $J$ whence $\sqrt{IJ} \supseteq \sqrt{I} \cap \sqrt{J}$; there will be equality by the isotoneness of $\sqrt{\ }$ when $IJ \subseteq I$. The $I$'s for which this inequality, i.e., $IE \subseteq I$, holds may be termed *bi-elements*. They include $E$ and are closed under arbitrary intersection and join: $(\bigcap I_\alpha)E \subseteq I_\alpha E \subseteq I_\alpha$, $(\bigvee I_\alpha)E = \bigvee I_\alpha E \subseteq \bigvee I_\alpha$.

There is enough structure to define the quotient $J{:}I \equiv \bigvee\{K{:}KI \subseteq J\}$; when it exists (i.e., there are such $K$) it is a bi-element since $J \supseteq KI \supseteq K(EI) = (KE)I$. If $J \supseteq$ a bi-element $I$, $J{:}E$ (hence all quotients of $J$) exist; conversely, if $J{:}E$ exists then since $(J{:}E)E^2 \subseteq (J{:}E)E \subseteq J$, $J{:}E$ is a bi-element $\subseteq J$. Moreoever, every other bi-element $I \subseteq J$ is $\subseteq J{:}E$ since $IE \subseteq I$. Now call $J$ *left-primitive* if there is some maximal $M \supseteq J$ for which $M{:}E = J$. This permits characterizing $\sqrt{I}$ for bi-elements $I$ as $\bigcap$ primitive $J \supseteq I$: indeed $I \subseteq M$ maximal only if $I \subseteq M{:}E$ primitive $\subseteq M$. In rings, primitive bi-ideals may in turn be characterized as annihilators of simple modules $E/M$. If $E^2 = E$, these simple modules are even "irreducible" (= the action by $E$ is not identically 0), i.e., the annihilator of $E/M$, $M{:}E, \neq E$. In rings without unit it can happen that $E^2 \subseteq M$, i.e., $M{:}E = E$; there one restricts to modular maximal $M$. (A modular $J \supseteq$ the bi-ideal $J{:}E$; conversely a (strictly [J, p. 5]) cyclic module has nontrivial $E$-action only if the annihilator of any generator $g$ is modular: for if there is an $e \in E$ such that $g = eg$ then $r - re \in 0{:}g$ for all $r$).

The above radical in the (semi)lattice of (modular) left ideals will be identified in Chapter 3 as the Jacobson radical in rings; if on the other hand one applies Chapter 1 to the subsemilattice of bi-elements, one will find for rings the (larger) Brown-McCoy radical. In fact, this is the largest closure operator not sending any $I \neq E$ to $E$ in the subsemilattice of bi-ideals; and it preserves $\cap$ even sending products to meet. The smallest closure operator with the latter property is the lattice analogue of the Baer lower nil radical, to which we turn next.

We ask for the smallest order-strengthening in the subsemilattice of bi-elements which converts product to $\supseteq$ meet. It must identify every power $J^n$ with $J$, hence bring $J$ under $I$ whenever $J^n \subseteq I$. We are thus led to set $I^* \equiv \bigvee\{J : \text{some } J^n \subseteq I\}$. This is increasing (since $I^1 \subseteq I$) and isotone in $I$; $(J \vee K)^{m+n} \subseteq J^m \vee K^n$ by multiplicative distributivity and since these are bi-elements — thus the join is updirected and the dominance of meet by product, $I^* \cap J^* \subseteq (IJ)^*$, holds — since $K^m \subseteq I, K^n \subseteq J$ entail $K^{m+n} \subseteq IJ$ — equality holding by isotoneness: $(IJ)^* \subseteq (I \cap J)^* \subseteq I^* \cap J^*$ - Unfortunately, this operator is not idempotent. In general, for any increasing meet-preserving self-map, its self-iterate $I \longrightarrow I^{**}$ is again such; and so is the (pointwise) join of an ascending chain of such when meet is (join-)continuous; i.e., distributes across updirected join. Then one attains the smallest product-to-meet converting closure operator (hence complete join-preserving) by iterating $I \longrightarrow I^*$. If $E$ is compact, its exclusion from the image of $I's \neq E$ will be maintained by the iteration. The requisite meet-continuity is a consequence of compact join-generation [B, Lemma 2, p. 187] since if $I \cap \bigvee J_\alpha$ is the join of compact $K$, then each of these is $\subseteq$ some $I \cap J_\alpha \subseteq \bigvee I \cap J_\alpha$. This property of compact join-generation also ensures [K, Theorem A] that every (nilpotent) radical element $I = \sqrt{I}$ is the intersection of primes $\supseteq I$.

In summary: In a compactly join-generated multiplicative semilattice, the smallest closure operator in the subsemilattice of bi-elements which sends product to meet is obtained by iterating $\bigvee\{J : \text{some } J^n \subseteq I\}$ and coincides with the intersection of the primes $\supseteq I$. It is the universal multiplicative join morphism to a meet continuous semilattice. A compact $E$ will not be reached from below.

The condition that a complete lattice be multiplicative with meet as product is that (finite) meets distribute across (even infinite) joins. One encounters this situation in lattice ordered groups, where the lattice of "solid" (= convex lattice) subgroups enjoys this property [BKW Prop. 2.2.9]. In any complete lattice the completely meet-irreducibles are just those maximal for not dominating some element; if the lattice is compactly join-generated, every element is an intersection of completely meet-irreducibles. The solid subgroup lattice is so generated (since an updirected join of solid subgroups is their set theoretic union); by distributivity the finitely meet-irreducibles coincide with the primes and so the Baer radical operator is the identity. (Also follows from the fact that

every element is idempotent). One gets a non-trivial radical by taking the intersection of "closed" primes for some closure operator on the solid subgroup lattice. When this is the order-closure—i.e., assigns the smallest containing solid subgroup closed for existent suprema—one gets the "distributive radical". Indeed, a poset is completely distributive if, for any subsets $S$ having $\bigvee$'s, $y \not\geq x \leq$ all $\bigvee S$ entails the existence of a choice function $f(S) \in S$ such that $\bigwedge_S f(S)$ exists and is not $\leq y$. When $\bigwedge_S \bigvee S$ exists it suffices to take this for $x$, and then the condition just states that $x$ also $= \bigvee_f \bigwedge f(S)$ and dually. In a completely distributive group the identity subgroup's distributive radical is itself: for if $x$ were $\bigvee S$ for some $S \subseteq P$ for every prime $P$, then $x = \bigvee_f \bigwedge f(S)$ where each $\bigwedge f(S) \in \bigcap P$, the identity. Conversely, the quotient map modulo a closed subgroup preserves all existent extrema: since the elements in the group mapping $\leq$ the unit—hence those mapping $\leq$ any quotient element—are closed; and modulo a prime, the order is total: for disjoint positive elements in the quotient would have disjoint polars which yield a meet-reduction of the kernel. Thus, modulo every closed prime one gets a complete surjection onto a chain. Therefore, a group with trivial distributive radical is competely subdirectly embeddable in a product of chains, hence is completely distributive.

The system of left congruences in a semigroup does not of course carry a natural multiplication – it does however admit a "residuation" by elements of the semigroup: $sxCtx$ is, for every left congruence $C$ and element $x$, a left congruence which is appropriately designated $C{:}x$. This operation preserves infinitary meet in $C$ and is multiplicative in $x - C{:}xy = C{:}y{:}x$. One could thus model this system by a complete lattice equipped with a multiplicative meet-preserving action by a semigroup. The bi-elements are now defined as those $C \subseteq$ each of their $C{:}x - C \cap \bigcap C{:}x$ is the largest bi-element $\subseteq C$. Observe that $C{:}x$ as congruence is exactly the annihilator of ( = the pairs in $S$ equalized by) the image of $x$ in $S/C$ : thus this largest bi-element represents the annihilator of $S/C$, the cyclic $S$-set having a generator with annihilator $C$; it coincides with the bi-element $\bigcap C{:}x$ when this quotient $S$-set is strictly cyclic. This coincidence could be taken as the abstract analogue of strict cyclicity of quotient i.e., of "modularity" of $C$.

Chapter 3. In a semilattice of submodules of a module $E$, $I \vee J = I + J$, the set of pairwise sums of elements from $I$ and $J$. Thus $H \vee J = E$ just when $H + J$ includes any set of generators of $E$ and if $E$ has a single generator, say $e$, this comes to $e - J$ meeting $H$: In a module generated by $e$, $J$ is $I$-small just when $e-J$ is disjoint from all $H(\neq E) \supseteq I$, i.e., each $e - j$ is included in no such $H$: the submodule generated by $e - j$ and $I$ is all of $E$. In a unitary module over a ring with unit 1, this says: there exists an $r$ such that $(1 - r)(e - j) - e \in I$, or $rj \equiv re + j(I)$. This "left quasi-regularity modulo I" can serve to characterize the elements of $I$-small submodules even over rings without unit: for if $e - j \in H \supseteq I$ then so does $re - rj$, hence $j$ and so $e$; conversely, if $j$

belongs to an $I$-small and $e - j \in R(e - j) + I$ then this $= E$ hence $j \in R(e - j) + I$.

In the lattice of bi-ideals of a ring with unit, $J$ will be $I$-small just when the bi-ideal generated by each $(1 - j)$ and $I$ is $E$. The bi-ideal generated by $(1 - j)$ is obtained by adjoining to the generated left ideal, $E(1 - j)$, the latter's right multiples, thus all finite sums $\Sigma st - sjt$; that 1 belongs to this ideal $+I$ thus comes to $j \in \{r - rj + \Sigma st - sjt + I\}$, which is a two-sided "quasi-regular" (called "weakly" in [BH]) form usable also in rings without unit (indeed it is left quasi-regularity mod the bi-ideal $\Sigma st - sjt + I$). The belonging of $j$ to the bi-ideal in brackets entails the latter's coincidence with $E$; an overideal of $\{\ \}$ maximal for excluding $j$ is maximal; modulo such the ring is simple with, as image of $j$, a right unit; this is also a left unit, since $(1 - \overline{j})\overline{E}$ is a bi-ideal (being left-annihilated by $\overline{E}$) $\neq \overline{E}$ (else some $\overline{r} - \overline{j}\overline{r} = \overline{j}$ whence $\overline{0} = \overline{r}\overline{j} = \overline{r}$, contradicting $\overline{j} \neq \overline{0}$). This yields the description of the Brown-McCoy radical.

In a commutative lattice-ordered group the join of solid (i.e., convex lattice) subgroups is again their algebraic sum, hence $I \vee J$ is again the set of pairwise sums of elements and when $E$ has a single generator $e$ — known here as a "strong unit" — the $I$-small $J$ are those consisting of $j$'s for which $e - j$ generates (convexly) all of $E$ over $I$. Similarly, the join of convex ideals in a lattice-ordered ring is their algebraic sum and so in such a ring the $I$-small left ideals $J$ just consist of $j$'s for which the convex left ideal generated by $E(1 - j)$ and $I$ is $E$ — this comes to $j$ in this ideal. Note that the solid ideals of a lattice-ordered ring form a multiplicative lattice [BKW 8.2] which is a complete sublattice of the solid subgroup lattice, hence is compactly join-generated with meets distributing across (even infinite) joins. The "$l$-radical" of [BKW 8.6.1] is the above $I^*$, the join of nilpotents (mod $I$), in this lattice; its non-idempotence is noted p.166 and its inclusion in the $\bigcap$ of the containing primes — the "$P$-radical" — in 8.6.16. Hence this is a special case of the story developed lattice theoretically in Chapter 2 above.

## References


[1] F. W Anderson and K. R. Fuller *Rings and Categories of Modules*, 1974, Springer, New York.

[2] G. Birkhoff *Lattice Theory, 3rd edition*, 1967, A.M.S. Colloq. Publ. No. 25, Providence.

[3] B. Banaschewski and R. Harting, *Lattice aspects of radical ideals and choice principles*, Proc. London Math. Soc. (3) 50 (1985), 385-404.

[4] T.S. Blyth and M.F. Janowitz, *Residuation Theory*, 1972, Pergamon Press, Oxford.

[5] A. Bigard, K. Keimel and S. Wolfenstein, *Groupes et Anneaux Réticulés*, 1977, L.N. in Math, No. 608, Springer, Berlin.

[6] A.H. Clifford and G.B. Preston, *The Algebraic Theory of Semigroups, Volume II, Mathematical Surverys, Number 7*, American Mathematical Society, 1967.

[7] N.J. Divinsky, *Rings and Radicals*, 1965, London.

[8] M.Gray, *A Radical Approach to Algebra* 1970, Addison-Wesley Publishing Co.

[9] N. Jacobson, *Structure of Rings*, 1964, A.M.S. Colloq. Publ. No. 37, Providence.

[10] K. Keimel, *A unified theory of minimal prime ideals*, Acta. Math. Acad. Sci. Hungar. 23 1972, 51-69.

[11] R. Mlitz, *Radicals and interpolation in universal algebra in Radical Theory, L. Márki, R. Wiegandt eds.*, Colloq. Bolyai No. 38, 1985, 297-331, Budapest.

[12] E.N.Roiz and B.M. Schein, *Radicals of semigroups*, Semigroup Forum 16, 1978, 199-344.

[13] F.A. Szasz, *Radicals of Rings*, 1981, J. Wiley, Chichester.

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

Received April 23, 1991

# SUR LA CONTINUITE DES HOMOMORPHISMES D'ALGEBRES

M. EL AZHARI

*Presented by M.D. Choi, F.R.S.C.*

Résumé. Nous donnons un théorème de continuité automatique (théorème II.1) dont la démonstration repose essentiellement sur la généralisation de la technique de DO.Sin.Sya. Comme conséquence, nous obtenons deux théorèmes de T.Husain et S.B.Ng (théorème 1 de [2] et théorème 1 de [3]).

## I. Préliminaires

Soit E une algèbre sur le corps $\mathbb{K}$ ( = $\mathbb{R}$ ou $\mathbb{C}$), on dit souvent que E est une $\mathbb{K}$-algèbre. Si E est munie d'une topologie $\tau$ compatible avec sa structure d'espace vectoriel et pour laquelle la multiplication est séparément continue, on dit que $(E, \tau)$ est une algèbre topologique.

Une algèbre localement convexe (en abrégé a.l.c) est une algèbre topologique munie d'une topologie d'espace localement convexe.

Soit $(E, \tau)$ une algèbre topologique. On dit que $(E, \tau)$ est une algèbre localement multiplicativement convexe (en abrégé a.l.m.c) si $\tau$ est définie par une famille $(p_\lambda)_\lambda$ de semi-normes d'espace vectoriel vérifiant en outre $p_\lambda(xy) \leq p_\lambda(x)\, p_\lambda(y)$ pour tout $\lambda$ et tous x,y de A.

## II. Résultats.

Théorème II.1. Soient A,B deux $\mathbb{R}$-espaces vectoriels topologiques, A étant métrisable et complet. Soient $s : A \to A$, $h : B \to B$ deux fonctions tel que s est continue et $s(0) = 0$. Considérons $I_h = \{g \in B^* : g(h(x)) = g(x)^2$ pour tout x de B $\}$

( $B^*$ dual algébrique de B) et supposons que $I_h$ est non vide.

On suppose que B satisfait à la condition

(P) pour toute suite $\{y_n\} \subset B$ , $y_n \neq 0$ , $y_n \not\longrightarrow 0$ il existe $f \in I_h$ tel que $f(y_n) \not\longrightarrow 0$

alors toute application linéaire T de A dans B telle que $T(s(x)) = h(Tx)$ pour tout x de A, est continue.

Preuve : Supposons que T n'est pas continue. Il existe une suite $\{x_n\}_{n \geq 1} \subset A$, $x_n \longrightarrow 0$ mais $Tx_n \not\longrightarrow 0$. On peut supposer que $x_n \neq 0$ et $Tx_n \neq 0$ pour tout $n \geq 1$. Par hypothèse, il existe $f \in I_h$ tel que $f(Tx_n) \not\longrightarrow 0$. On peut construire à partir de la suite $(x_n)_n$ , une suite $(a_m)_m$ telle que $\inf_m f(Ta_m) = \varepsilon > 0$ .

On a $\varepsilon^{-1} a_m \longrightarrow 0$ ainsi $s(\varepsilon^{-1} a_m) \longrightarrow 0$ car s est continue.

Posons $y_m = s(\varepsilon^{-1} a_m)$ pour tout $m \geq 1$ .

Alors
$$f(Ty_m) = f(T(s(\varepsilon^{-1} a_m))) = f(h(T(\varepsilon^{-1} a_m))) = f(T(\varepsilon^{-1} a_m))^2 \geq 1 \quad \text{pour tout } m \geq 1$$

On définit $g_k : A^{k+1} \longrightarrow A$ pour $k \geq 0$

$g_0(b_1) = b_1$

$g_1(b_1, b_2) = b_1 + s(b_2)$

$\vdots$

$g_k(b_1, \ldots, b_{k+1}) = g_1(b_1, g_{k-1}(b_2, \ldots, b_{k+1}))$

En utilisant la même construction faite dans [5] , on peut définir une sous-suite $(z_k)_{k \geq 0}$ de $(y_m)_{m \geq 1}$ tel que pour tout $k \geq 0$ $(g_{p-k}(z_k, \ldots, z_p))_{p \geq k}$ est une suite de Cauchy.

Soit $c_k = \lim_{p\to\infty} g_{p-k}(z_k,\dots,z_p)$

par définition $g_{p-k}(z_k,\dots,z_p)=z_k + s(g_{p-(k+1)}(z_{k+1},\dots,z_p))$

On obtient $c_k = z_k + s(c_{k+1})$

ainsi $Tc_k = Tz_k + T(s(c_{k+1}))$

On a
$$\begin{aligned} f(Tc_k) &= f(Tz_k) + f(T(s(c_{k+1}))) \\ &= f(Tz_k) + f(h(Tc_{k+1})) \\ &= f(Tz_k) + (f(Tc_{k+1}))^2 \\ &\geqslant 1 + f(Tc_{k+1})^2 \qquad \text{pour tout } k\geqslant 0 \end{aligned}$$

d'où
$$\begin{aligned} f(Tc_0) &\geqslant 1 + f(Tc_1)^2 \\ &\geqslant 2 + f(Tc_2)^2 \\ &\vdots \\ &\geqslant k + f(Tc_k)^2 \end{aligned}$$

i.e $f(Tc_0)\geqslant k$ pour tout $k\geqslant 0$

ce qui est absurde.

Comme conséquence , on a :

Théorème II.2. Soient A,B deux $\mathbb{R}$-algèbres topologiques, A métrisable et complète. On suppose que B satisfait à la condition (D) pour toute suite $\{y_n\}\subset B$ , $y_n\neq 0$ , $y_n\not\longrightarrow 0$ il éxiste un caractère f de B tel que $f(y_n)\not\longrightarrow 0$ .
Alors toute application linéaire $T : A\longrightarrow B$ vérifiant $T(x^2) = (Tx)^2$ pour tout x de A, est continue.

Preuve. On considère $s : A\longrightarrow A$, $x \longrightarrow x^2$ et $h : B\longrightarrow B$, $x \longrightarrow x^2$

remarquons que f de la condition (D) est dans $I_h$. On applique alors le théorème II.1.

Théorème II.3. Soit A une IR-a.l.m.c. séquentiellement complète. Soit B une IR-algèbre topologique satisfaisant à la condition (D) du théorème II.2. Alors toute application linéaire T de A dans B vérifiant $T(x^2) = (Tx)^2$, $x \in A$, est bornée.

Preuve. On applique le théorème II.2 et le théorème de structure de M.Akkar ( [1] ) affirmant que si A est une a.l.m.c. séquentiellement complète, alors A est bornologiquement limite inductive d'a.l.m.c. métrisables et complètes.

Remarques 1. Les théorèmes II.2 et II.3 sont des améliorations des théorèmes 1 de [2] et 1 de [3] .

2. Dans l'énoncé du théorème II.1, on peut remplacer IR par un corps archimédien.

3. $\mathbb{C}$ est une IR-algèbre de Banach, mais $\mathbb{C}$ ne satisfait pas à la condition (D) car le seul caractère réel de $\mathbb{C}$ est l'application nulle de $\mathbb{C}$ dans IR.

4. On peut remplacer B dans les théorèmes II.2 et II.3 par IR ; c'est une IR-algèbre de Banach qui satisfait à la condition (D).

Remerciements. Je remercie Messieurs les Professeurs M.Akkar et M.Oudadess pour l'aide précieuse qu'ils m'ont apportés durant l'élaboration de ce travail.

Références

[1] M.Akkar. "Sur la structure des algèbres topologiques localement multiplicativement convexes". C.R.Acad.Sc.Paris 279 (1974), Serie A, 941-944.

[2] T.Husain and S.B.Ng. "On continuity of algebra homomorphisms and uniqueness of metric topology". Math.Zeit., 139(1974), 1-4.

[3] T.Husain and S.B.Ng. "Boundedness of multiplicative linear functionals". Canad.Math.Bull.Vol.17(2), (1974), 213-215.

[4] E.A.Michael. "Locally multiplicatively convex topological algebras". Mem.Amer.Math.Soc.11 (1952).

[5] S.B.Ng and S.Warner. "Continuity of positive and multiplicative functionals". Duke Math.J.39(1972), 281-284.

[6] Do.Sin.Sya. "On semi normed rings with an involution". Izv. Akad. Nauk, SSSR,t.23 (1959), 509-528.

Ecole Normale Supérieure
Avenue Oued Akreuch
Takaddoum, Rabat
B.P. 5118, Maroc.

Received March 14, 1991

# Values of Bernoulli polynomials and Hurwitz's zeta function at rational points

GERT ALMKVIST AND ARNE MEURMAN

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

The *Bernoulli polynomials* $B_n(t)$ are defined by

$$\frac{xe^{tx}}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n(t)x^n}{n!}.$$

Then $B_n(0) = B_n$ are the *Bernoulli numbers.*

During his work on asymptotic formulas for the number of plane partitions [1], the first author found that for odd $n \geq 3$ it seemed as if

$$k^n B_n(h/k)$$

was always an integer. For even $n$ this was not the case. But by redefining the Bernoulli polynomials as follows we get a general statement.

DEFINITION 1. $\tilde{B}_n(t) = B_n(t) - B_n$.

Thus for odd $n \geq 3$ we have $\tilde{B}_n(t) = B_n(t)$.

THEOREM 2. *Let $h$ and $k$ be positive integers. Then*

$$k^n \tilde{B}_n(h/k)$$

*is an integer.*

Before we start the proof we make some remarks.

REMARK 3: If $h$ is an integer then $\tilde{B}_n(h)/n$ is an integer, see [4, p. 6].

PROOF: $\tilde{B}_n(h)/n = \sum_{r=1}^{h-1} r^n$ if $h \geq 1$.

Otherwise $\tilde{B}_n(0) = 0$ and $\tilde{B}_n(h) = (-1)^n \tilde{B}_n(-h)$.

REMARK 4: It is sufficient to prove the theorem for $h = 1$.

PROOF: It follows from the addition formula

$$B_n(x + y) = \sum_{m=0}^{n} \binom{n}{m} B_m(x) y^{n-m}.$$

REMARK 5: We have the following remarkable formula

$$\sum_{n=1}^{\infty} k^n \tilde{B}_n(1/k)\frac{x^n}{n!} = kx\left(\sum_{n=0}^{\infty}\frac{\tilde{B}_{n+1}(k)}{n+1}\frac{x^n}{n!}\right)^{-1}.$$

PROOF: We have

$$\sum_{n=1}^{\infty}\tilde{B}_n(1/k)\frac{(kx)^n}{n!} = \frac{kx(e^{kx/k}-1)}{e^{kx}-1} = kx\left(\frac{e^{kx}-1}{e^x-1}\right)^{-1}$$

$$= kx\left(x^{-1}\sum_{m=1}^{\infty}\tilde{B}_m(k)\frac{x^m}{m!}\right)^{-1} = kx\left(\sum_{n=0}^{\infty}\frac{\tilde{B}_{n+1}(k)}{n+1}\cdot\frac{x^n}{n!}\right)^{-1}.$$

Unfortunately it seems impossible to prove the theorem directly from this formula.

PROOF OF THEOREM 2: By Remark 1 $\tilde{B}_n(x)/n$ is a polynomial that takes integer values on the integers. Hence it is a linear integral combination of $\binom{x}{m}$:s (see Stanley [5] p. 38). We identify the coefficients.

LEMMA 6. *If $n \geq 2$, then*

$$\tilde{B}_n(t) = n\sum_{j=1}^{n-1} j!S(n-1,j)\binom{t}{j+1}$$

*where $S(n,m)$ is the Stirling number of the second kind.*

PROOF: See Rademacher [4] p. 9. His

$$A_{q,j} = j!S(q,j).$$

It follows that

$$k^n\tilde{B}_n(1/k) = \sum_{j=1}^{n-1} n\frac{S(n-1,j)k^{n-j-1}}{j+1}(1-k)(1-2k)\ldots(1-jk).$$

We want to show that each term in the sum is an integer.

Assume that $j+1 = p^a f$ where $p$ is a prime and $(p,f)=1$. We want to prove that the numerator of the $j$-th term is divisible by $p^a$.

Case 1. $(p,k)=1$.

Then there exists $r \leq j$ such that $rk \equiv 1 \mod p^a$ and hence $p^a$ divides $1-rk$.

Case 2. $p|k$.

If $j = n-1$ then $j+1 = n$ and we are done. Otherwise

$$n-j-1 = b \geq 1.$$

Since $p|k$ we have $p^b|k^{n-j-1}$ and we have to show that

$$p^{a-b}|S(n-1,j) = S(fp^a+b-1, fp^a-1).$$

LEMMA 7. *For $n, r \geq 1$ we have*

$$S(n, n-r) = \sum_{s=r+1}^{2r} c(s, s-r)\binom{n}{s}$$

*where the $c(s, s-r)$:s are integers.*

PROOF: Put $m = n - r$. Then $S(n, m)$ is the number of partitions of an $n$ element set $\Omega$ into $m$ nonempty subsets, say

$$\Omega = A_1 \cup \cdots \cup A_m \qquad \text{(disjoint union)}.$$

Let $n - s$ of the $A_j$:s be singletons. They are determined by their union, that can be chosen in

$$\binom{n}{n-s} = \binom{n}{s}$$

ways. Hence we obtain

$$S(n, n-r) = \sum_{s} c(s, s-r)\binom{n}{s}$$

where $c(s, s-r)$ is the number of partitions of an $s$ element set into $s - r$ subsets all of cardinality $\geq 2$. From $m < n$ we obtain $s > 0$ and hence $c(s, s-r) \neq 0$ only if $s > r$. Since $s - r$ disjoint subsets of cardinality $\geq 2$ has cardinality $\geq 2(s-r)$ we get (if $c(s, s-r) \neq 0$)

$$2(s-r) \leq s \qquad \text{i.e.} \qquad s \leq 2r.$$

END OF THE PROOF OF THEOREM 2: To finish the proof we notice that the numerators in the binomial coefficients in the expansion of

$$S(fp^a + b - 1, fp^a - 1)$$

contain the factor $fp^a$. The denominator $s!$ contains

$$v_p(s!) = [s/p] + [s/p^2] + \cdots \leq \frac{s}{p(1-1/p)} = \frac{s}{p-1} \leq \frac{s}{2} \leq b$$

factors of $p$ if $p \geq 3$. If $p = 2$, then $v_2(s!) \leq s - 1$ and the numerator

$$(f \cdot 2^a + b - 1) \ldots f \cdot 2^a \cdot (f \cdot 2^a - 1) \ldots (f2^a + b - s)$$

contains at least $a + [s/2] - 1$ factors 2 and

$$a + [s/2] - 1 - (s-1) \geq a - b.$$

Hence the theorem is proved. Q.E.D.

EXAMPLE 8: For $k = 4$ we get for odd $n$

$$4^n B_n(1/4) = -nE_{n-1}$$

where $E_n$ are the Euler numbers defined by

$$\frac{1}{\cosh x} = \sum_{n=0}^{\infty} \frac{E_n x^n}{n!}.$$

**The Hurwitz zeta function.**

The *Hurwitz zeta function* $\zeta(s,a)$ is defined by

$$\zeta(s,a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s}$$

(see Apostol [2] p. 251). Thus $\zeta(s,1) = \zeta(s)$ is the Riemann zeta function. The connection between $\zeta(s,a)$ and the Bernoulli polynomials is given by

$$\zeta(1-s,a) = B_s(a)/s \text{ for } s \in \mathbf{N}$$

(see [2] p. 264). Hence Theorem 2 implies

THEOREM 9. *For odd* $n \geq 3$,

$$nk^n\zeta(1-n,h/k)$$

*is an integer.*

To get some results for positive $s$ we can use the functional equation for $\zeta(s,h/k)$ (see [2] p 261)

$$\zeta(1-s,h/k) = \frac{2\Gamma(s)}{(2\pi k)^s} \sum_{r=1}^{k} \cos(\pi s/2 - 2\pi rh/k)\zeta(s,r/k)$$

Multiplying by $sk^s$ we get

PROPOSITION 10. *For odd* $s \geq 3$ *and* $k \geq 2$ *we have*

$$\sum_{r=1}^{k-1} \sin(2\pi rh/k)\zeta(s,r/k) = (-1)^{(s-1)/2}\frac{(2\pi)^s}{2\cdot s!}k^s B_s(h/k) = \frac{(2\pi)^s}{2\cdot s!}\cdot \textit{integer}.$$

REMARK 11: The matrix

$$(\sin(2\pi rh/k))$$

$r,h = 1,\ldots,k-1$ is not invertible so we cannot compute the $\zeta(s,h/k)$ explicitly. Thus for $k=4$ we get for odd $s \geq 3$ only one equation

$$\zeta(s,1/4) - \zeta(s,3/4) = \frac{(2\pi)^s}{2\Gamma(s)}|E_{s-1}|$$

**A definite integral.**

For Re $s > 1$ we have ([2] p. 251)

$$\zeta(s,a) = \frac{1}{\Gamma(s)}\int_0^{\infty} \frac{x^{s-1}e^{-ax}}{1-e^{-x}}dx.$$

Substituting this into the functional equation for $\zeta(s,a)$ we get

$$\zeta(1-s,h/k) = \frac{2\Gamma(s)}{(2\pi k)^2}\sum_{r=1}^{k}\cos(\pi s/2 - 2\pi rh/k)\zeta(s,r/k)$$

$$= \frac{2}{(2\pi k)^s}\mathrm{Re}\left\{e^{\pi si/2}\sum_{r=1}^{k}e^{-2\pi rhi/k}\int_0^\infty \frac{x^{s-1}e^{-rx/k}}{1-e^{-x}}dx\right\}$$

$$= \frac{1}{(2\pi k)^s}\int_0^\infty \frac{x^{s-1}(\cos(\pi s/2 - 2\pi h/k) - e^{-x/k}\cos(\pi s/2))}{\cosh(x/k)-\cos(2\pi h/k)}dx.$$

Assume now that $s$ is an odd integer $\geq 3$. The substitution $x \mapsto 2\pi x$ gives

$$k^s\zeta(1-s,h/k) = (-1)^{(s-1)/2}\int_0^\infty \frac{x^{s-1}\sin(2\pi h/k)}{\cosh(2\pi x/k)-\cos(2\pi h/k)}dx.$$

Hence if $k \geq 2$ and $h < k$

$$\int_0^\infty \frac{x^{s-1}}{\cosh(2\pi x/k)-\cos(2\pi h/k)}dx = (-1)^{(s+1)/2}\frac{k^sB_s(h/k)}{s\sin(2\pi h/k)} = \frac{\text{integer}}{s\sin(2\pi h/k)}.$$

This result is already in Bierens de Haan [3] p. 129, Formulas 88.5 and 88.6.

Finally we give a couple of elementary formulations of some of our results. Let $a$ and $b$ be positive integers.

1. Define

$$f(x) = \frac{ax(e^{bx}-1)}{e^{ax}-1}.$$

Then $f^{(n)}(0)$ is an integer for all $n$.

2. Let

$$\frac{ax}{2}\cdot\frac{\sinh(b-a/2)x}{\sinh(ax/2)} = \sum_{n=1}^{\infty}\frac{c_nx^n}{n!}.$$

Then $c_n$ is an integer for $n \geq 3$.

## References

1. G. Almkvist, *A rather exact asymptotic formula for the number of plane partitions*, to appear in "Contemporary Mathematics," volume dedicated to the memory of Emil Grosswald.
2. T.M. Apostol, "Introduction to analytic number theory," Springer Verlag, New York, 1976.
3. D. Bierens de Haan, "Nouvelles tables d'intégrales définis," Leiden, 1867.
4. H. Rademacher, "Topics in analytic number theory," Springer Verlag, New York, 1973.
5. R.P. Stanley, "Enumerative combinatorics," Vol. 1, Wadsworth & Brooks/Cole, Monterey, 1986.

Department of Mathematics
University of Lund

Received April 23, 1991

# LE THEOREME DE ROLLE

# SUR LE CORPS DES SERIES FORMELLES GENERALISEES

*ALI BENHISSI*

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

**RESUME :** Dans cette note on étudie les conditions de validité du théorème de Rolle pour les polynômes sur le corps des séries formelles généralisées .

**INTRODUCTION :** Dans la suite K désigne un corps ordonnable, G un groupe abélien totalement ordonné et $K((T^G))$ le corps des séries formelles généralisées à coefficients dans K et à supports bien ordonnés dans G .

1 . D'après [ 5 ] th . 2 . 1 , si K est réel clos et G est divisible par tous les entiers impairs, alors $K((T^G))$ a la propriété de Rolle .

2 . Dans [ 5 ] p. 69, on signale que le premier exemple de corps ayant la propriété de Rolle sans être réel clos est donné par Pelling dans [ 7 ] . D'ailleurs, dans la littérature on trouve pas d'autre ! Les séries formelles généralisées fournissent une nouvelle famille de tels corps . En effet si K est réel clos quelconque et G est divisible par tous les entiers impairs et non divisible par 2 , par exemple $G = \{ n / 2k+1 \ , \ n \in Z \ , \ k \in IN \}$ , alors $K((T^G))$ a la propriété de Rolle d'après la première remarque et n'est pas réel clos d'après [ 2 ] proposition 1 .

3 . Si $K((T^G))$ a la propriété de Rolle, alors G est divisible par tous les entiers impairs car si $\alpha \in G$ et $n \in IN^*$ est impair, alors la série $T^\alpha$ admet d'après corollaire 2 . 6 du [ 5 ] une racine $n^{eme}$ dans $K((T^G))$ . Donc $\alpha$ est divisible par n dans G .

**LEMME 1 :** Soient K et L deux corps isomorphes et ordonnables . Si l'un des deux corps a la propriété de Rolle , il en est de même pour l'autre .

**DEMONSTRATION** : Supposons que K a la propriété de Rolle . Soient $P \in L[X]$ et $a < b$ dans L tels que $P(a) = P(b) = 0$ . Notons $\bar{P}$ , $\bar{a}$ et $\bar{b}$ les images de P , a et b par l'isomorphisme de L dans K . Alors $\bar{P}(\bar{a}) = \bar{P}(\bar{b}) = 0$ , et d'après cor. 2 . 3 du [ 5 ], il existe $\bar{c} \in K$ tel que $\bar{P}'(c) = 0$ et $(\bar{a}-\bar{c})(\bar{b}-\bar{c}) \in K^{*2}$ . Si c est l'image de $\bar{c}$ par l'isomorphisme, alors $P'(c) = 0$ et $(a-c)(b-c) \in L^{*2}$. Donc $a < c < b$

**EXEMPLE** : Soient K un corps réel clos et $G_1$ et $G_2$ deux groupes abéliens totalement ordonnés . On suppose que $G_1$ est divisible et que $G_2$ est divisible par tous les entiers impairs et non divisible par 2 . Munissons le groupe produit $G_1 \times G_2$ de l'ordre lexicographique . Le corps : $K((T^{G1 \times G2}))$ a la propriété de Rolle . Les corps :$K((T^{G1 \times G2}))$ et $K((T^{G2}))((T^{G1}))$ sont isomorphes ,voir [ 1 ]ch.II,pr. 3 .D'après le lemme le corps ordonnable $K((T^{G2}))((T^{G1}))$ a la propriété de Rolle, pourtant le corps $K((T^{G2}))$ n'est pas réel clos .

**PROPOSITION 1** : Si K est archimédien pour au moins l'un de ses ordres et si $K((T^G))$ a la propriété de Rolle , alors K est réel clos .

**DEMONSTRATION** : Notons v la valuation usuelle de $K((T^G))$ , $K[[T^G]]$ son anneau , M son idéal maximal et < l'ordre pour lequel K est archimédien et son prolongement de Neumann à $K((T^G))$ . D'après [ 5 ] th. 1 . 2 , le corps $K((T^G))$ admet une valuation hensélienne v' pour laquelle le corps des restes R est réel clos et le groupe de valeurs est divisible par tous les entiers impairs . Soit A l'anneau de v' . On va montrer que $K[[T^G]] \subset A$ . On a : $K[[T^G]] = K + M$ . Soit $f = aT^{\alpha} + \ldots\ldots \in M$ , $a \neq 0$ , $\alpha > 0$ .On peut supposer que $a > 0$ . Donc $0 < f < 1$ .D'après th. 8 . 3 du [ 8 ] , la valuation v' est compatible avec < .
Donc $v'(f) \geq v'(1) = 0$ . Donc $M \subset A$ . Soit $a \in K^*$ , $\exists n \in IN^*$ tel que $0 < |a| < n$ .
Donc $v'(a) \geq v'(n) = v'(1+\ldots.+1) \geq v'(1) = 0$ . Donc $K \subset A$ .
D'après [ 9 ] p. 60 , la valuation v définit sur R une valuation quotient v / v' de corps résiduel K , égal à celui de v , qui est ordonnable . D'après th. 8 . 6 du [ 8 ] , comme R est réel clos , alors K est réel clos .

**PROPOSITION 2** : Si $K$ est euclidien et si $K((T^G))$ a la propriété de Rolle, alors $K$ est réel clos.

**DEMONSTRATION** : Tout polynôme de $K[X]$ de degré impair admet d'après cor.2 . 6 du [ 5 ] , une racine dans $K((T^G))$. Cette racine appartient à $K$ .

**REMARQUE** : L'hypothèse $K$ archimédien ( resp. euclidien ) dans la proposition 1 ( resp. 2 ) est impérative . En effet dans l'exemple précédent on a montré que $K((T^{G2}))((T^{G1}))$ a la propriété de Rolle et que $K((T^{G2}))$ n'est pas réel clos . Ceci s'explique par le fait que $K((T^{G2}))$ n'est archimédien pour aucun de ses ordres d'après [3] et n'est pas euclidien car si $\alpha \in G_2$ n'est pas 2 - divisible alors $\pm T^{\alpha}$ ne peut pas être un carré .

**LEMME 2** : Soit $K$ un corps satisfaisant la propriété de Rolle . Alors toute extension finie de $K$ est de degré égal à une puissance de 2 .

**DEMONSTRATION** : D'après [ 6 ] th. 57 , il suffit de montrer que toute extension finie L de $K$ est de degré divisible par 2 . Soit $P$ le polynôme minimal d'un élément primitrif .
D'après [ 5 ] cor. 2 . 6 , $[L:K] = \text{dég } P$ est pair .

**LEMME 3** : Soient $G \subset G'$ deux groupes abéliens tels que le groupe $G' / G$ est fini et $G$ est divisible par tous les entiers impairs. Alors card $(G' / G)$ est une puissance de 2 .

**DEMONSTRATION** : Supposons que card $(G' / G)$ ne soit pas une puissance de 2 . Il admet donc un diviseur premier $p \geq 3$ . D'après le théorème de Cauchy le groupe $G'/G$ contient un élément $\bar{g}$ d'ordre p.
Donc $p\bar{g} = \bar{0}$ , puis $pg \in G$.Comme $G$ est divisible par p ,alors : $pg/p \in G$ . Donc $\bar{g} = \bar{0}$ : absurde .

**PROPOSITION 3** : Soient $G$ un groupe abélien totalement ordonné divisible par tous les entiers impairs et $K$ un corps vérifiant la condition ( * ) : << si $P \in K[X]$ et $a < b \in K$ sont tels que $P(a) = P(b) = 0$ , alors il existe $c \in K$ tel que $a < c < b$ et $c$ est un zéro d'ordre impair

de P'>> . Alors $K((T^G))$ satisfait la propriété de Rolle .

**DEMONSTRATION** : Soient $P(X) \in K((T^G))[X]$ et $a < b \in K((T^G))$ tel que : $P(a) = P(b) = 0$ . Quitte à remplacer $P(X)$ par $P(a+(b-a)X)$ , on peut supposer que $a = 0$ et $b = 1$ . On peut aussi supposer que les valuations des coefficients de $P(X)$ sont toutes positives et pas toutes nulles . Soit $p(X) \in K[X]$ le polynôme dont les coefficients sont les termes constants de ceux de $P(X)$. Alors $p(0) = p(1) = 0$ , $p \neq 0$ , $p'(X)$ est le polynôme dont les coefficients sont les termes constants de ceux de $P'(X)$ . Il existe $0 < c < 1$ un zéro d'ordre m impair de $p'(X)$ dans K . Posons : $p'(X) = (X-c)^m g(X)$ , où $g(X) \in K[X]$ n'est pas annulé par c . Par le lemme de Hensel , il existe $H(X) \in K[[T^G]][X]$ unitaire de degré m et $G(X) \in K[[T^G]][X]$ tels que $P'(X) = H(X)G(X)$ et $(X-c)^m$ ( resp . $g(X)$ ) est le polynôme dont les coefficients sont les termes constants des coefficients de $H(X)$ ( resp. $G(X)$ ). Comme deg $H(X) = m$ est impair , alors $H(X)$ admet au moins un facteur irréductible de degré impair . [ Ce facteur F peut être choisi tel que si $F^k / H$ et $F^{k+1} \nmid H$ , alors k est impair ] . Soient f une racine d'un tel facteur dans une clôture algébrique de $K((T^G))$ et n son degré . Soient G' le groupe et K' le corps résiduel du prolongement de la valuation naturelle de $K((T^G))$ à $K((T^G))(f)$ . Alors : $[K((T^G))(f) : K((T^G))] = n$ $= [K' : K] . [G' : G]$ . Comme n est impair , alors que $[K' : K]$ et $[G' : G]$ sont des puissances de 2 par les lemmes 2 et 3, on doit avoir : $n = [K' : K] = [G' : G] = 1$ .Donc $f \in K((T^G))$ et $H(X) = (X-f)^k R(X) \in K[[T^G]][X]$ . Comme $K[[T^G]]$ est un anneau de valuation , alors $f \in K[[T^G]]$ . Ainsi f est une racine de $P'(X)$ de terme constant c avec $0 < c < 1$ . Donc $0 < f < 1$ . Dans cette notation $<$ désigne un ordre sur K et l'un de ses prolongements à $K((T^G))$ .

**REMARQUE** : L'ordre de f dans $P'(X)$ est égal à l'entier impair k . En effet supposons que $G(f) = 0$ , alors $g(c) = 0$ : absurde .

**PROPOSITION 4** : Tout corps réel clos a la propriété ( * ) de la proposition 3 .

**DEMONSTRATION** : Soient K un corps réel clos, $P \in K[X]$ et $a < b \in K$ tels que $P(a) = P(b) = 0$. Comme P a un nombre fini de racines, on peut se ramener au cas où a et b sont deux racines consécutives. Par le théorème de Rolle 1 . 2 . 5 p. 10 du [4], P' admet au moins une racine dans ]a, b[. Soient $c_1, \ldots\ldots, c_n$ toutes ses racines. Supposons qu'elles soient toutes d'ordres pairs. Alors :

$$P' = \prod_{i=1}^{n} (X - c_i)^{m_i} g(X),$$

où les $m_i \in IN^*$ sont pairs et $g(X)$ n'a pas de racine dans ]a, b[. D'après 1 . 2 . 4 p. 10 du [4], $g(X)$ ne change pas de signe sur ]a, b[. Comme le $m_i$ sont pairs, il sera de même pour P'. Donc d'après 1 . 2 . 7 du [4], le polynôme P est strictement monotone sur l'intervalle [a, b], ce qui contredit $P(a) = P(b) = 0$.

**REMARQUES** :

1) Il existe des corps qui ne sont pas réel clos et qui satisfont le théorème de Rolle et la propriété (*). En effet si K est réel clos et G est divisible par tous les entiers impairs et non par 2, alors on a montré précédemment que le corps $K((T^G))$ a la propriété de Rolle mais il n'est pas réel clos. D'après la remarque de la proposition 3, il vérifie aussi la propriété (*).

2) D'après le théorème 3 . 1 du [5] et la proposition 1 du [2], le corps $K((T^G))$ a la propriété de Rolle pour les fractions rationnelles si et seulement si K est réel clos et G est divisible.

## REFERENCES

[ 1 ] A . BENHISSI , Les corps de séries formelles généralisées , Thèse , Marseille 1988 . Atelier national de reproduction des thèses de Grenoble II .

[ 2 ] A . BENHISSI , Séries formelles généralisées sur un corps pythagoricien , C . R . Math . Rep. Acad . Sci . Canada , vol . XII , n° 5 , 1990, pp 193 - 198 .

[ 3 ] A . BENHISSI , Quelques propriétés des séries formelles généralisées , accepté dans les comptes rendus du Canada .

[ 4 ] J . BOCHNAK , M . COSTE , M . F . ROY , Géométrie algébrique réelle , Springer - Verlag , 1987 .

[ 5 ] R . BROWN , T . C . CRAVEN , M . J . PELLING , Ordered fields satisfying Rolle's theorem , Illinois J . Math . vol . 30 , n° 1 , 1986 , pp . 66 - 78 .

[ 6 ] I . KAPLANSKY , Fields and rings , The University of Chicago Press , 1972 .

[ 7 ] M . J . PELLING , Solution of advanced problem n° 5861 , Amer . Math . Monthly , vol . 88 ( 1981 ) , pp 150 - 152 .

[ 8 ] A . PRESTEL , Lectures on formally real fields , lecture notes in math . 1093 .

[ 9 ] P . RIBENBOIM , Théorie des valuations , les presses de l'université de Montréal 1968 .

Faculté des Sciences de Monastir

Département de Mathématiques

5000 - MONASTIR - TUNISIE .

Received April 21, 1991

# On Solvable Lie Ideals of a Ring

R.K.Sharma and J.B.Srivastava

*Presented by H. Zassenhaus, F.R.S.C.*

**Abstract:** Let R be an associative , unitary ring in which 2 is invertible. It is proved that if a Lie ideal U of R is solvable then $\gamma_2(U)R$ is a two sided nil ideal of R.

Let R be an associative ring with identity and $\mathcal{L}(R)$ be the associated Lie ring of R under the Lie multiplication

$[x,y] = xy-yx$ ; $x,y \in R$.

An ideal U of $\mathcal{L}(R)$ is called a Lie ideal of R. The identity $ur = [u,r] + ru$ ; $u \in U, r \in R$ implies that $UR = RU = RUR$ = the two sided ideal of R generated by U. For any two Lie ideals U and V of R, [U,V] denotes the Lie ideal of R generated by all [u,v]; $u \in U$, $v \in V$.

The Commutators are defined left normed, i.e. $[x_1,x_2,\ldots,x_n]=[[x_1,x_2,\ldots,x_{n-1}],x_n]$, for $n\geq 3$ and $[x_1,x_2]=x_1x_2-x_2x_1$ for all $x_1,x_2,\ldots,x_n \in R$. The derived chain and the lower central chain of a Lie ideal U of R are defined by

$\delta^{(0)}(U)=U$, $\delta^{(m)}(U)=[\delta^{(m-1)}(U), \delta^{(m-1)}(U)]$ for $m \geq 1$,

and $\gamma_1(U)=U$, $\gamma_n(U)=[\gamma_{n-1}(U),U]$ for $n \geq 2$, respectively.

U is said to be solvable(nilpotent) if for some positive integer C, $\delta^{(c)}(U)=0$ $(\gamma_{c+1}(U)=0)$. R is said to be Lie solvable (Lie nilpotent) if there exists a positive integer n such that $\delta^{(n)}(\mathcal{L}(R)) = 0$ , $(\gamma_{n+1}(\mathcal{L}(R)) = 0)$.

Jennings [1] proved that if a ring R is Lie nilpotent then $\gamma_2(\mathcal{L}(R))R$ is a nil ideal of R. Sharma and Srivastava [3] proved that if a ring R in which both 2 and 3 are invertible is Lie solvable, then $\gamma_2(\mathcal{L}(R))R$ is a nil ideal of R. In case of Lie nilpotent grouprings , we refer to Levin and Sehgal [2] and Sharma and Srivastava [4]. In this paper we take up the case of a solvable Lie ideal U of a ring R in which 2 is invertible and prove (Theorem 5) that $\gamma_2(U)R$ is a two sided nil ideal of R. It is shown that the condition of invertibility of 2 cannot be dropped. Some other related results are also obtained.

We begin with

Lemma 1. For any Lie ideal U of a ring R,

$$(\gamma_3(U)R)^3 \subseteq \delta^{(2)}(U)R$$

Proof. follows from Lemma 2.4(ii) and Theorem 2.7 of [4].

Lemma 2. For any Lie ideal U of a ring R,

$$[\delta^{(1)}(U), \mathcal{L}(R)]\ R)^6 \subseteq \delta^{(2)}(U)R.$$

Proof. follows from Lemma 1 and Corollary (1.6(i), [3] ).

Lemma 3. Let U be a Lie ideal of a ring R, then

for $x, y \in U$, $4[x, y]^3 \in \gamma_3(U)R$.

Proof. We observe that

$$2\,[x,y]^2 = [x^2,y,y] + x[y,x,y] + [y,x,y]x$$
$$\equiv [x^2,y,y] \pmod{\gamma_3(U)R}.$$

And,

$$2\,[x^2,y,y][x,y] = [y^2,x^2,y,x] + [[x^2,y,y],[x,y]]$$
$$+ [x^2,y,y,x]y + y[x^2,y,y,x]$$
$$\equiv [y^2,x^2,y,x] \pmod{\gamma_3(U)R}$$

But $[y^2,x^2,y,x] \in [[U^2,\mathcal{L}(R)],U,U] \subseteq [[U,\mathcal{L}(R)],U,U]$

$\subseteq \gamma_3(U)$ By Lemma (1.2(1) (3)).

Hence, $4[x,y]^3 \in \gamma_3(U)R$

**Lemma 4.** Let $U$ be a Lie ideal of a ring $R$ in which 2 is invertible. Then for every $\alpha \in \delta^{(1)}(U)R$ there exists a positive integer $M$ such that $\alpha^M \in \delta^{(2)}(U)R$.

**Proof.** Let $x_i, y_i \in U$ and $r_i \in R$ for $i = 1,2,\ldots,n$.

If $\alpha = \sum_{i=1}^{n} [x_i,y_i]r_i \in \delta^{(1)}(U)R$, then $\alpha^{2n+1}$ will be a finite sum consisting of (2n+1)-fold products of the elements of the type $[x_i,y_i]r_i$, $i=1,2,\ldots,n$, and in each such (2n+1)-fold product at least one $[x_j,y_j]r_j$ for some $j=1,2,\ldots,n$ will be repeated at least 3-times. Hence $\alpha^{2n+1}$ is a finite sum of the elements of the type $r[x_j,y_j]s[x_j,y_j]t[x_j,y_j]w$ for some $r,s,t,w \in R$.

The proof of the lemma follows from the following observation and Lemma 2

$r[x_j,y_j]s[x_j,y_j]t[x_j,y_j]w$

$= r[x_j,y_j]s[x_j,y_j]^2tw - r[x_j,y_j]s[x_j,y_j][x_j,y_j,t]w$

$\equiv r[x_j,y_j]s[x_j,y_j]^2tw \pmod{[\delta^{(1)}(U),\mathcal{L}(R)]R}$

$= rs[x_j,y_j]^3tw + r[x_j,y_j,s][x_j,y_j]^2tw$

$\equiv rs[x_j,y_j]^3tw \pmod{[\delta^{(1)}(U),\mathcal{L}(R)]R}$

$\equiv 0 \pmod{[\delta^{(1)}(U),\mathcal{L}(R)]R}$ by Lemma 3

M can be taken as any positive integer greater or equal to $\delta(2n+1)$.

We can now easily conclude

**Theorem 5.** Let $R$ be a ring in which 2 is invertible. If a Lie ideal $U$ of $R$ is solvable, then $\gamma_2(U)R$ is a two sided nil ideal of $R$.

Proof. follows by repeated applications of Lemma 4.

We can improve upon the Theorem 2.4 of [3] as

Theorem 6. Let R be a ring in which 2 is invertible. If R is Lie solvable then $\gamma_2(\mathcal{L}(R))R$ is a two sided nil ideal of R.

Proof. follows from Theorem 5, for $U=\mathcal{L}(R)$.

Theorem 7. Let R be a ring in which 2 is invertible. If a Lie ideal U of R is nilpotent, then $\gamma_2(U)R$ is a two sided nil ideal of R.

Proof follows from Theorem 5.

Remark 8. The condition of invertibility of 2 in Theorems 5,6 and 7 can not be dropped, for example, if $R=Z_2[S_3]$, the group algebra of characteristic 2 of the group of permutations $S_3$ on three symbols over $Z_2=(0,1)$, and $U=\gamma_2(\mathcal{L}(R))$, then it is easy to see that $\delta^{(2)}(U) \subseteq \gamma_3(U)=0$, $(\sigma+\sigma^2) \in \gamma_2(U)$ and $(\sigma+\sigma^2)^k=(\sigma+\sigma^2)\neq 0$ for every positive integer k, where $\sigma=(1,2,3)$.

References.

[1] S.A.Jennings, On rings whose associated Lie rings are nilpotent, Bull.Amer.Math.Soc. 53(1947),593-597

[2] F.Levin and S.K.Sehgal, On Lie nilpotent grouprings, J.Pure and Appl.Algebra,37(1985),33-39.

[3] R.K.Sharma and J.B.Srivastava, Lie Solvable rings, Proc.Amer.Math.Soc.94(1985),1-8.

[4] R.K.Sharma and J.B.Srivastava, Lie ideals in group rings, J.Pure and Appl.Algebra 63(1990),67-80.

Indian Institute of Technology,Kharagpur(West-Bengal)-721302,INDIA.

Indian Institute of Technology,Hauz Khas,New Delhi-110016,INDIA.

Received May 14, 1991

## Mailing Addresses


1. G. Almqvist
   Department of Mathematics
   University of Lund, Box 118
   S-22100 Lund, Sweden

2. A. Benhissi
   Faculté des Sciences de Monastir
   Département de Mathématiques
   5019 Monastir, Tunisie

3. M. El Azhari
   Ecole Normale Supérieure
   Avenue Ould Akreuch, Takkadoum, Rabat
   B.P. 5118, Maroc

4. C. Farsi
   Department of Mathematics
   University of Toronto
   Toronto, Canada, M5S 1A1

5. I. Fleischer
   Department of Mathematics
   University of Windsor
   Windsor, Canada, N9B 3P4

6. P. Fuchs
   Department of Mathematics
   Masaryk University, Janáckovo nám. 2a
   662 95 Brno, Czechoslovakia

7. J. Gutiérrez
   Depto. de Matemáticas, Estadística y Computación
   Universidad de Cantabria
   39071 Santander, Spain

8. A. Meurman
   Department of Mathematics
   University of Lund, Box 118
   S-22100 Lund, Sweden

9. D. Nour El Abidine
   Département de Mathématiques
   Université Claude Bernard Lyon 1
   69622 Villeurbanne, France

10. R.K. Sharma
    Indian Institute of Technology
    Kharagpur, West Bengal
    721302, India

11. J.B. Srivastava
    Indian Institute of Technology
    Haus Khaz, New Delhi
    110016, India

12. N. Watling
    Department of Mathematics
    SUNY at Buffalo
    Buffalo, NY, 14214, U.S.A.

13. M. Yamada
    Faculty of Engineering
    Ibaraki University
    Hitachi, Japan 316