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

Vol. IX, No. 2 April 1987 avril

CONTENTS

SUR LES EXTENSIONS RELATIVEMENT PYTHAGORICIENNES

Yoshio NAKAMURA

Présenté par K. Murasugi, F.R.S.C.

Résumé. Nous dirons une extension K d'un corps k (K/k en abrégé) est relativement pythagoricienne (une généralisation de la définition dans [5]), si chaque somme $\sum_{i=1}^{n} a_i^2$ ($a_i \in k, n<\infty$) des carrés dans k est un carré dans K, c'est-à-dire $\sum_{i=1}^{n} a_i^2 = \alpha^2 (\exists\, \alpha \in K)$. Dans cette note nous allons caractériser les extensions des corps relativement pythagoriciennes et montrer quelque propriétés de ces extensions.

1) Notations et définitions.

Dans toute la suite, tous les corps sont supposés de la caractéristique ≠2. On dit un corps commutatif est formellement réel si -1 n'est pas somme des carrés dans ce corps. Une forme quadratique $q=\langle a_1, a_2, \ldots, a_n\rangle$ sur le corps k est une forme diagonale $a_1 x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2$, où $a_1, a_2, \ldots, a_n \in k$. Pour les définitions d'ordre dans un corps k, anneaux de Witt W(k), isotrope etc, on réfère à [3]. $W_t(k)$ désigne la torsion du groupe additif W(k). Généralement nous utilisons le même symbole pour une forme quadratique dans k et cette image dans W(k). Pour tout $q \in W(k)$, q_K désigne la forme q considéré dans K qui est une extension d'un corps k. $\mathrm{Ker}(W(k) \to W(K))$ est l'ensemble de tous les éléments $q \in W(k)$ tels que $q_K = 0$

dans W(K). La plus petite extension k_r/k qui est relativement pythagoricienne, c'est-à-dire $k_r = \bigcap_i k_i$ l'intersection de toutes extensions k_i/k relativement pythagoriciennes dans une clôture algébrique de k, est dit une clôture relativement pythagoricienne du corps k. Il est évident que K/k est relativement pythagoricienne si et seulement si $K \supset k_r$.

2) Le cas des corps non plus formellement réel.

Théorème 1. Si un corps k n'est pas formellement réel, alors k_r est le corps engendré sur k par toutes racines carrées des éléments de k.

Preuve: Par notre supposition, il existe des éléments $a_1, \ldots, a_n \in k$, tels que $-1 = \sum_{i=1}^{n} a_i^2$. On sait que chaque élément $a \in k$ est représenté tel que $x^2 - y^2 = a$, pour des certains éléments x, y de k. Ainsi $a = x^2 + (\sum_{i=1}^{n} a_i^2)y^2$ est une somme des carrés dans k. Alors $\sqrt{a} \in k_r$. Il est bien sûr que le corps engendré sur k par toutes racines carrées des éléments de k est relativement pythagoricien. Donc ce corps-ci est exactement k_r.

3) Le cas des corps formellement réel.

Proposition 1. Soit k un corps formellement réel. Si S est un préordre(preordering [4]) dans k, c'est-à-dire $S \subsetneq k, k^2 \subset S, S+S \subset S, S \cdot S \subset S$, et si $K = k(\{\sqrt{s} \mid s \in S\})$, alors on a

$$\mathrm{Ker}(W(k)\to W(K_p)) = \sum_{s\in S} \langle 1,-s\rangle W(k),$$

où K_p est une clôture pythagoricienne de K ([3]).

Pour la preuve on confère à [1].

Théorème 2. Pour un corps formellement réel, on a

$$\mathrm{Ker}(W(k)\to W(k_r)) = \Sigma\langle 1,-a_i^2\rangle W(k) = W_t(k).$$

Preuve: Un ensemble de toute somme $\sum_{i=1}^{n} a_i^2$ ($a_i \in k, n<\infty$) des carrés dans k est une préordre dans k, et $k_r = k(\{\sqrt{\sum_{i=1}^{n} a_i^2} \mid a_i \in k, n<\infty\})$. Dans proposition 1, remplaçons K par k_r. Alors $K_p = k_p$ et nous avons

$$\mathrm{Ker}(W(k)\to W(k_p)) = \Sigma\langle 1,-\Sigma a_i^2\rangle W(k).$$

Mais $\Sigma\langle 1,-\Sigma a_i^2\rangle W(k) \subset \mathrm{Ker}(W(k)\to W(k_r))$ et $k_r \subset k_p$. On sait $\mathrm{Ker}(W(k)\to W(k_p)) = W_t(k)$ ([3]), donc la preuve est complète.

Lemme 1. Soit K/k une extension formellement réelle. Si tout $q \in W_t(k)$ est la forme isotrope sur K, alors K/k est relativement pythagoricienne.

Preuve: Pour des éléments $a_1,\ldots,a_n$ dans k, $q=\langle 1,-\sum_{i=1}^{n} a_i^2\rangle$ est un élément de $W_t(k)$, aussi bien dans la preuve de theoreme 2. Par la supposition q_K est isotrope, alors $q_K=0$. Donc $\sum_{i=1}^{n} a_i^2$ est un carré d'un élément de K, ceci montre que K/k est relativement pythagoricienne.

Théorème 3. Soit K un corps formellement réel. Une extension K/k est relativement pythagoricienne si et seulement si $\mathrm{Ker}(W(k)\to W(K)) \supset W_t(k)$.

Preuve: Si $\mathrm{Ker}(W(k)\to W(K)) \supset W_t(k)$, alors K/k est relativement pythagoricienne par lemme 1. Au contraire, soit K/k relativement pythagoricienne. Par le théorème 2,

$$\mathrm{Ker}(W(k)\to W(K)) \supset \mathrm{Ker}(W(k)\to W(k_r)) = W_t(k).$$

Dans le théorème 3 il est facile qu'on remplace la condition $\mathrm{Ker}(W(k)\to W(K)) \supset W_t(k)$ par la condition que tout $q \in W_t(k)$ est la forme isotrope sur K ou par la condition $\mathrm{Ker}(W(k)\to W(K)) = W_t(k)$. Et celui-ci peut être caractérisé comme la proposition suivante.

Proposition 2. Soit K un corps formellement réel. Alors $W_t(k) = \mathrm{Ker}(W(k)\to W(K))$ si et seulement si
(1) tous les ordres de k peuvent être prolongé dans K, et
(2) pour tout $q\neq 0\in W(k)$, q_K n'est pas d'ordre fini comme un élément d'un groupe additif W(K).

Preuve: Suppons que $W_t(k) = \mathrm{Ker}(W(k)\to W(K))$. Alors on a (1) par [2] ou [5,p.154]. Or, si $rq_K = 0 \in W(K)$ pour certain nombre naturel r, alors $rq \in \mathrm{Ker}(W(k)\to W(K)) = W_t(k)$. Ainsi $q \in W_t(k) = \mathrm{Ker}(W(k)\to W(K))$, et $q_K = 0$, ce qui montre (2). Au contraire suppons (1) et (2). Alors $W_t(k) \supset$

Ker(W(k)→W(K)) par [2]. D'autre part, pour tout $q \in W_t(k)$, il y a nombre naturel r tel que $rq = 0 \in W(k)$. Donc $rq_K = 0$ et $q_K = 0$ en vertu de (2), ce qui montre $W_t(k) \subset$ Ker(W(k)→W(K)) et achève la démonstration.

Nous allons montrer une autre simple propriété d'une extension formellement réelle.

Proposition 3. Soit K un corps formellement réel et soit K/k une extension relativement pythagoricienne. Alors, si la forme quadratique q non-isotrope représente quelq'un $a \in k$ et -a, q est isotrope sur K.

Preuve: On peut suppons

$$q = \langle a, a_2, \ldots, a_n \rangle, \quad \text{où } a_2, \ldots, a_n \in k.$$

Puisque q représente -a, alors

$$q \perp \langle a \rangle = \langle a, a, a_2, \ldots, a_n \rangle$$

est isotrope sur k, ce qui montre $q = \langle a, a_2, \ldots, a_n \rangle$ est isotrope sur K d'après la supposition de notre proposition.

Références

[1] R.Elman,T.Y.Lam and A.R.Wadsworth, Amenable Fields and Pfister Extensions, Queen's Papers on pure & applied Math.,No.46(1977),p.451-452.

[2] R.Elman,T.Y.Lam and A.R.Wadsworth, Orderings under field extensions, Jour.für reine angew.Math.,306

(1979),p.7-27.

[3] T.Y.Lam, The Algebraic Theory of Quadratic Forms, Benjamin, 1973.

[4] T.Y.Lam, Orderings, Valuations and Quadratic Forms, Amer.Math.Soc.,1984

[5] Y.Nakamura, On relatively formally real fields, Math.Rep.Toyama Univ.,Vol.9(1986).

Département de Mathématiques
Faculté des Sciences
Université Toyama
930 Toyama, Gofuku 3190
Japon

Received December 1, 1986

ALGEBRES HEREDITAIRES ET TUBULAIRES PAR MORCEAUX

Ibrahim Assem et Andrzej Skowroński

Présenté par V. Dlab, F.R.S.C.

RESUME: Nous caractérisons les algèbres dont la catégorie dérivée est équivalente à la catégorie dérivée d'une algèbre héréditaire de type Dynkin ou Euclidien, ou d'une algèbre tubulaire canonique.

1. Soit k un corps algébriquement clos. Toutes nos algèbres sont associatives, unifères et de k-dimension finie. Sans perte de généralité, on peut aussi les supposer sobres et connexes. Tous nos modules sont à droite et de k-dimension finie. Soit A une algèbre, et $D^b(A)$ la catégorie dérivée des complexes bornés sur la catégorie mod A des A-modules [V]. Pour un graphe fini et connexe Δ, on dit que A est héréditaire par morceaux de type Δ [H1] si $D^b(A)$ est équivalente, en tant que catégorie triangulée, à $D^b(C)$, où C est une algèbre héréditaire dont le carquois ordinaire [G] admet Δ comme graphe sous-jacent. On se limitera dans cette note à considérer le cas où Δ est un graphe de Dynkin ou un graphe Euclidien, ce qui correspond au cas où C est de type de représentation classifiable. De même, on dit que A est tubulaire par morceaux si $D^b(A)$ est équivalente, en tant que catégorie triangulée, à $D^b(C)$, où C est une algèbre tubulaire canonique [R]. L'objectif de cette note est de présenter quelques résultats obtenus dans la classification de ces algèbres.

2. On rappelle qu'un module T_A est dit inclinant (respectivement, co-inclinant) [HR] si $\mathrm{Ext}^2_A(T,-) = 0$ (respectivement, $\mathrm{Ext}^2_A(-,T) = 0$), $\mathrm{Ext}^1_A(T,T) = 0$, et le nombre de facteurs directs indécomposables non-isomorphes de T_A est égal au rang du groupe de Grothendieck $K_0(A)$. Deux algèbres A et B sont dites équivalentes pour les inclinaisons et les co-inclinaisons s'il existe une suite d'algèbres $A_0 = A, A_1, \ldots A_{m+1} = B$ et une suite de modules inclinants ou co-inclinants $T^i_{A_i}$ $(i = 0, 1, \ldots m)$ tels que $A_{i+1} = \mathrm{End}\, T^i_{A_i}$. Si B est héréditaire ayant Δ comme graphe sous-jacent de son carquois, et si en outre chaque T^i est un

A_i-module inclinant tel que, pour tout module indécomposable M_{A_i}, on a soit $\mathrm{Hom}_{A_i}(T^i, M) = 0$, soit $\mathrm{Ext}^1_{A_i}(T^i, M) = 0$, on dit que A est une algèbre pré-inclinée de type Δ [AH]^i. Enfin, si $m \neq 1$, A est dite inclinée [HR]. Il suit de [H1][H2] que les conditions suivantes sont équivalentes pour une algèbre A et un graphe Δ, Dynkin ou Euclidien:

(i) A est héréditaire par morceaux de type Δ.

(ii) A est équivalente pour les inclinaisons et les co-inclinaisons à une algèbre héréditaire de type Δ.

(iii) A est pré-inclinée de type Δ.

La caractérisation des algèbres héréditaires par morceaux de type Dynkin ou Euclidien se ramène donc à celle des algèbres pré-inclinées.

3. Soit A une algèbre triangulaire, c'est à dire dont le carquois ordinaire n'a pas de cycles orientés. En particulier, la dimension globale de A est finie et par conséquent, la catégorie dérivée $D^b(A)$ s'identifie à la catégorie d'homotopie des complexes bornés de A-modules projectifs $K^b(\mathrm{proj}\ A)$ [V]. Soit $P^\cdot$ un complexe indécomposable de $K^b(\mathrm{proj}\ A)$. Si $P^i = 0$ pour $i<p$ et $i>q$, alors que $P^p \neq 0$, $P^q \neq 0$, on dit que la largeur de $P^\cdot$ est $q-p+1$. La dimension globale forte de A est le suprémum des largeurs des complexes indécomposables de $K^b(\mathrm{proj}\ A)$. Il est clair que la dimension globale de A est plus petite ou égale à sa dimension globale forte. On dira aussi que $D^b(A)$ est de cycles finis si, pour toute suite de morphismes non-nuls et non-inversibles entre complexes indécomposables de $D^b(A)$ de la forme $M_0^\cdot \to M_1^\cdot \to \ldots \to M_m^\cdot = M_0^\cdot$, les complexes $M_i^\cdot$ ($i = 0, 1, \ldots m-1$) se trouvent dans un tube (au sens de [R]) du carquois de $D^b(A)$ [H1]. On a:

THEOREME (A): Les conditions suivantes sont équivalentes pour une algèbre A:

(i) A est héréditaire par morceaux de type Dynkin ou Euclidien ou tubulaire par morceaux.

(ii) A est pré-inclinée de type Dynkin ou Euclidien ou équivalente pour les inclinaisons et les co-inclinaisons à une algèbre tubulaire canonique.

(iii) A est triangulaire, sa dimension globale forte est finie, et $D^b(A)$ est de cycles finis.

On en déduit que A est tubulaire par morceaux si et seulement si elle est équivalente pour les inclinaisons et les co-inclinaisons à une algèbre tubulaire canonique.

4. On sait que toute algèbre A s'écrit sous la forme $A \simeq kQ/I$, où kQ est l'algèbre des chemins du carquois Q de A et I un idéal de kQ contenu dans $\text{rad}^2 kQ$ [G]. Un tel isomorphisme est une présentation de A. Le groupe fondamental $\pi_1(Q,I)$ de la paire (Q,I) est défini dans [MP]. Une algèbre A sera dite simplement connexe si, pour toute présentation $A \simeq kQ/I$ de A, Q n'a pas de cycles orientés et le groupe fondamental de (Q,I) est trivial.

THEOREME (B): Soit A une algèbre satisfaisant les conditions équivalentes du théorème (A). Alors A n'est pas simplement connexe si et seulement si elle est pré-inclinée de type $\tilde{A}_n$.

5. La classification se scinde donc en deux parties: le cas où A est pré-inclinée de type $\tilde{A}_n$ et le cas simplement connexe. Dans le premier cas, on a:

THEOREME (C): Une algèbre A est pré-inclinée de type $\tilde{A}_n$ si et seulement si on peut trouver une présentation $A \simeq kQ/I$ telle que (Q,I) a exactement n+1 sommets et satisfait les conditions suivantes:

(i) Le nombre de flèches de source ou de but donné est au plus égal à deux.

(ii) I est engendré par un ensemble de chemins de longueur deux (appelés relations).

(iii) Pour chaque flèche α, il existe au plus une flèche β et une flèche γ telles que $\alpha\beta$ et $\gamma\alpha$ n'appartiennent pas à I.

(iv) Pour chaque flèche α, il existe au plus une flèche λ et une flèche μ telles que $\alpha\lambda$ et $\mu\alpha$ appartiennent à I.

(v) Q contient un cycle unique (non-orienté) C sur lequel le nombre de relations dans le sens des aiguilles d'une montre égale le nombre de relations dans le sens contraire.

On voit de suite que le groupe fondamental de (Q,I) est isomorphe à $\mathbb{Z}$. En outre, A est de représentation finie si et seulement si le cycle C est

lié. Dans ce cas, nous obtenons aussi une caractérisation de A par les propriétés de son carquois d'Auslander-Reiten.

6. Dans le cas simplement connexe, on considère deux cas: si A est de représentation infinie, on obtient une description complète (par carquois liés) de l'algèbre A. Si A est de représentation finie, on utilise sa forme quadratique: soit S_1, S_2 ... S_n un ensemble complet des classes d'isomorphisme des A-modules simples. La forme quadratique q_A de A est la forme sur $K_0(A)$ dont la matrice $[q_{ij}]$ est donnée par:

$$q_{ij} = \sum_{t \geq 0} (-1)^t \dim_k \operatorname{Ext}_A^t (S_i, S_j)$$

Happel a démontré que A est pré-inclinée de type Dynkin si et seulement si A est simplement connexe et q_A positive définie. Nos méthodes permettent de donner une démonstration simple de ce résultat. Nous démontrons aussi que:

THEOREME (D): Une algèbre A de représentation finie est pré-inclinée de type Euclidien $\neq A_n$ si et seulement si A est simplement connexe et q_A positive semidéfinie de corang un.

Rappelons que la connexité simple d'une algèbre de représentation finie s'exprime au moyen d'un critère combinatoire simple (la condition (S) de Bautista-Larrión-Salmerón).

7. Les résultats précédents s'appliquent à l'étude des extensions triviales domestiques. L'extension triviale T(A) de A par son cogénérateur injectif minimal ${}_ADA_A = \operatorname{Hom}_k({}_AA_A, k)$ est l'algèbre dont la structure additive est celle du groupe abélien A DA et dont la multiplication est définie par:

$$(a,f)\,(b,g) = (ab,\ ag+fb)$$

pour a,b A et f,g DA. T(A) est une algèbre auto-injective et même symétrique. On rappelle aussi qu'une algèbre B est dite domestique s'il existe un nombre fini de foncteurs (de paramétrisation) F_i: mod k[X] $\to$ mod B, où i = 1, 2, ... t tels que:

(a) Pour chaque i, $F_i = - \otimes_{k[X]} Q_i$ où Q_i est un k[X]-B-bimodule, libre et de type fini en tant que k[X]-module.

(b) Pour chaque dimension d, toutes les classes d'isomorphisme de B-modules indécomposables, sauf au plus un nombre fini, sont de la forme $F_i(M)$

pour un i et un k[X]-module indécomposable M.

Enfin, B est dite t-paramétrique si le nombre minimal de ces foncteurs est t.

On a le résultat suivant, obtenu avec J. Nehring (comparer avec [AHR]):

THEOREME (E): Soit A une algèbre simplement connexe. Les conditions suivantes sont équivalentes:

(i) T(A) est domestique de représentation infinie.

(ii) T(A) est 2-paramétrique.

(iii) A est pré-inclinée de type Euclidien $\neq \tilde{A}_n$.

(iv) Il existe une algèbre inclinée B de représentation infinie et de type $\neq \tilde{A}_n$ telle que T(A) ≅ T(B).

Note: Ces résultats ont été obtenus alors que les auteurs visitaient l'Université de Bielefeld en tant que boursiers Alexandre von Humboldt. Ils voudraient remercier C. M. Ringel pour son hospitalité.

BIBLIOGRAPHIE:

[AH] Assem, I. et Happel, D.: Generalized tilted algebras of type $\tilde{A}_n$, Comm. Algebra 9 (1981) (20), 2101-2125.

[AHR] Assem, I.; Happel, D. et Roldán, O.: Representation-finite trivial extension algebras, J. Pure Appl. Algebra 33 (1984), 235-242.

[G] Gabriel, P.: Auslander-Reiten sequences and representation-finite algebras, Proc. ICRA II (Ottawa 1979), Springer Lecture Notes No. 831 (1980), 1-71.

[H1] Happel, D.: On the derived category of a finite-dimensional algebra, à paraître dans Comment. Math. Helv.

[H2] Happel, D.: Iterated tilted algebras of affine type, à paraître dans Comm. Algebra.

[HR] Happel, D. et Ringel, C. M.: Tilted algebras, Trans. Amer. Math. Soc. 274 (1982), No. 2, 399-443.

[MP] Martínez-Villa, R. et de la Peña, J. A.: The universal cover of a quiver with relations, J. Pure Appl. Algebra 30 (1983), 277-292.

[R] Ringel, C. M.: Tame algebras and integral quadratic forms, Springer Lecture Notes No. 1099 (1984).

[V] Verdier, J.-L.: Catégories dérivées, état 0, dans SGA 4½, Springer Lecture Notes No. 569 (1977), 262-311.

Ibrahim Assem
Faculté de Mathématiques
Université de Bielefeld
4800 Bielefeld 1
République Fédérale Allemande

Andrzej Skowroński
Institut de Mathématiques
Université Nicolas Copernic
87-100, Toruń, Chopina 12/18
Pologne

Received January 6, 1987

HOMOMORPHISMES P-PETITS DE GROUPES ABELIENS P-TORSION P-REDUITS

B. SARR

Présenté par H. Zassenhaus, F.R.S.C.

Sommaire: Dans ce travail, nous donnons une généralisation de certains résultats de R.S. Pierce concernant les homomorphismes petits de groupes abéliens primaires. Nous considérons ici une classe de groupes abéliens mixtes appelés groupes p-torsion dont les sous-groupes de p-base sont de torsion.

1) Notations et définitions :

- Un groupe G est dit p-torsion, s'il possède un sous-groupe de p-base p-primaire. p est un nombre premier fixé.
- Un sous-groupe A d'un groupe p-torsion G est dit p-large dans G s'il est totalement invariant et si pour tout sous-groupe de p-base B de G, on a $G = A + B$.
- La notation est en général celle de [5] .
- Toute suite u de la forme $u = (u_0, u_1, \ldots, u_k, \ldots)$ est une suite croissante d'entiers non négatifs.
- $G(u) = \{ x \in G \mid H_p^G(x) \geq u \}$ où $H_p^G(x)$ désigne la suite d'Ulm de x dans G .
- $U_G = \{u = (u_0, u_1, \ldots, u_k, \ldots) \mid G(u)$ est p-large dans $G\}$.
- G_p désigne la partie p-primaire de G .
- Dans la suite les groupes considérés sont p-torsion et p-réduits.
- Remarque : Si G est p-torsion et p-réduit et si

x élément de G est d'ordre fini, alors son ordre est une puissance de p.

Proposition 1.1 : Soit L un sous-groupe totalement invariant de G. Les conditions suivantes sont équivalentes.

i) L est p-large dans G.

ii) Il existe une suite $v = (v_0, v_1, \ldots, v_k, \ldots)$ croissante telle que $p^{v_k} G[p^k] \subseteq L$ et $G = L + G_p$.

Proposition 1.2 : Soit $u = (u_0, u_1, \ldots, u_k, \ldots)$ strictement croissante. On a l'égalité

$$G_p(u) = \sum_k p^{v_k} G[p^k] \quad \text{où } v_k = u_{k-1} - k + 1 \text{ et } v_0 \leq v_1 .$$

Preuve : On montre par induction sur e(x) avec $x \in G_p(u)$ que $G_p(u) \subseteq \sum_k p^{v_k} G[p^k]$. L'autre inclusion se fait en montrant par induction sur k que $p^{v_k} G[p^k] \subseteq G_p(u)$.

Proposition 1.3 : Soit F un sous-groupe de G. Les conditions suivantes sont équivalentes.

i) F contient un sous-groupe p-large de G.

ii) Il existe une suite $v = (v_0, v_1, \ldots, v_k, \ldots)$ telle que $p^{v_k} G[p^k] \subseteq F$ et $G = (F \cap G(u)) + G_p$ où $u = (u_0, u_1, \ldots, u_k, \ldots)$ avec $u_k = v_{k+1} + k$.

Preuve : i) $\Rightarrow$ ii). Si $F \supseteq G(u)$ qui est p-large dans G, on montre comme dans la proposition 1.1 qu'on a ii). De plus

$G = G(u) + G_p = (F \cap G(u)) + G_p$.

ii) $\Rightarrow$ i). On a $G = (F \cap G(u)) + G_p$ avec $u_k = v_{k+1} + k$. $G(u) = G(u) \cap G = G(u) \cap ((F \cap G(u)) + G_p) = (F \cap G(u)) + G_p(u)$. Donc il suffit de montrer que $G_p(u) \subseteq F$. D'après la proposition 1.2, on a $G_p(u) = \sum_k p^{v_k} G[p^k]$ et $p^{v_k} G[p^k] \subseteq F \ \forall\ k$ par hypothèse, donc $G_p(u) \subseteq F$. Il s'ensuit que $G(u) \subseteq F$ et $G = G(u) + G_p$. Par conséquent $G(u)$ est p-large dans G.

Définition 1.4 : Un homomorphisme $\varphi: G \longrightarrow A$ est dit p-petit si son noyau $\ker\varphi$ contient un sous-groupe p-large de G.

L'ensemble des homomorphismes p-petits de G dans A est noté PHom(G,A).

Exemple : Tout homomorphisme d'un groupe p-borné est p-petit et tout homomorphisme dans un groupe p-borné est p-petit.

Théorème 1.5 : Soit $\varphi \in \mathrm{Hom}(G,A)$. Les conditions suivantes sont équivalentes.

i) φ est p-petit.

ii) Il existe une suite $v = (v_0, v_1, \ldots, v_k, \ldots)$ strictement croissante telle que $e(x) \geq v_k$ implique $e(\varphi(x)) \leq e(x) - k$ et $G = ((\ker\varphi) \cap G(u)) + G_p$ où $u = (u_0, u_1, \ldots, u_k, \ldots)$ avec $u_k = v_{k+1} - 1$.

iii) Il existe une suite $w = (w_0, w_1, \ldots, w_k, \ldots)$ telle que $p^{w_k} G[p^k] \subseteq \ker\varphi$ et $G = ((\ker\varphi) \cap G(z)) + G_p$ où $z = (z_0, z_1, \ldots, z_k, \ldots)$ avec $z_k = w_{k+1} + k$.

Preuve : i) $\Rightarrow$ iii). Déjà prouvé (proposition 1.3) .

ii) ⇒ iii). Posons $w_k = v_k - k$. On remarque que si $u = (u_0,u_1,\ldots,u_k,\ldots)$ avec $u_k = v_{k+1} - 1$ et si $z = (z_0,z_1,\ldots,z_k,\ldots)$ avec $z_k = w_{k+1} + k$, on a $z = u$ et par conséquent $G = ((\ker\varphi) \cap G(u)) + G_p = ((\ker\varphi) \cap G(z)) + G_p$.

Montrons par induction sur k que $p^{w_k}G[p^k] \subseteq \ker\varphi$.

$p^{w_0}G[p^0] = \{0\} \subseteq \ker\varphi$. $p^{w_1}G[p] \subseteq \ker\varphi$. En effet, si $x \in p^{w_1}G[p]$ et $x \neq 0$, on a $e(x) = 1$ et $h_p^G(x) \geq w_1$. Il existe $y \in G$ tel que $x = p^{w_1}y$, $e(y) = w_1 + 1 = v_1$, donc $e(\varphi(y)) \leq v_1 - 1 = w_1$ et par conséquent $\varphi(x) = \varphi(p^{w_1}y) = p^{w_1}\varphi(y) = 0$ et $x \in \ker\varphi$.

Supposons que $p^{w_{k-1}}G[p^{k-1}] \subseteq \ker\varphi$ et soit $x \in p^{w_k}G[p^k]$. On a $e(x) = k$ ou $e(x) < k$. Si $e(x) < k$, $x \in p^{w_{k-1}}G[p^{k-1}]$ et par hypothèse d'induction $x \in \ker\varphi$. Si $e(x) = k$, $x = p^{w_k}y$ avec $y \in G_p$, $e(y) = w_k + k = v_k$ et $e(\varphi(y)) \leq v_k - k = w_k$ par conséquent $\varphi(x) = p^{w_k}\varphi(y) = 0$ et $x \in \ker\varphi$.

iii) ⇒ ii). Posons $v_k = w_k + k$. Si $z = (z_0,z_1,\ldots,z_k,\ldots)$ avec $z_k = w_{k+1} + k$ et si $u = (u_0,u_1,\ldots,u_k,\ldots)$ avec $u_k = v_{k+1} - 1$ alors $z = u$ et $G = ((\ker\varphi) \cap G(z)) + G_p = ((\ker\varphi) \cap G(u)) + G_p$. Soit maintenant $n = e(x) \geq v_k$, $e(p^{n-k}x) = k$ et $h_p^G(p^{n-k}x) \geq n - k \geq w_k$ donc $\varphi(p^{n-k}x) = 0 = p^{n-k}\varphi(x)$, par conséquent $e(\varphi(x)) \leq e(x) - k$.

2) Quelques théorèmes d'extension

Dans cette partie, nous montrons que sous certaines conditions, les homomorphismes p-petits s'étendent d'un sous-groupe de G à

tout G. B désigne un sous-groupe de p-base de G.

Lemme 2.1 : Soit un homomorphisme $\varphi: B \longrightarrow A$ tel que $\ker\varphi \geq B(u)$ ($B(u)$ est p-large dans B). Si $u \in U_G$, φ s'étend à un homomorphisme p-petit unique de G dans A.

Corollaire 2.2 : Si g_1 et g_2 sont deux homomorphismes p-petits de G dans A tels que $g_1(b) = g_2(b)$ pour tout $b \in B$, alors $g_1 = g_2$.

Théorème 2.3 : B étant un sous-groupe de p-base de G ($B = \bigoplus_{i\in I} \langle b_i \rangle$), si pour tout $i \in I$, $x_i \in A_p$ est donné satisfaisant:

1) $e(x_i) \leq e(b_i)$

2) il existe $v = (v_0, v_1, \ldots, v_k, \ldots)$ strictement croissante telle que $e(b_i) \geq v_k$ implique $e(x_i) \leq e(b_i) - k$,

et si $u \in U_G$ où $u = (u_0, u_1, \ldots, u_k, \ldots)$ avec $u_k = v_{k+1} - 1$, alors il existe un homomorphisme p-petit unique $f: G \longrightarrow A$ tel que $f(b_i) = x_i$ pour tout $i \in I$.

Théorème 2.4 : Soit F un sous-groupe p-pur de G, $g \in \mathrm{Hom}(F,A)$ tel que $\ker g \geq F(u)$ qui est p-large dans F. Si $u \in U_G$, alors g peut être étendu à un homomorphisme p-petit de G dans A.

Théorème 2.5 : Soit L un sous-groupe p-large de G, $g \in \mathrm{Hom}(L,A)$ tel que $\ker g \geq L(u)$ qui est p-large dans L. Si $h_p^A(g(x)) \geq h_p^G(x)$ pour $x \in L$ et si $u \in U_G$, alors g peut être étendu à un homomorphisme p-petit de G dans A.

Corollaire 2.6 : Soit $g \in \mathrm{Hom}(p^kG, p^kA)$ tel que

$\ker g \geq (p^k G)(u)$ qui est p-large dans $p^k G$. Si $u \in U_G$, g peut être étendu à un homomorphisme p-petit de G dans A.

Références

[1] K. Benabdallah, S. Yoshioka : On p-large subgroups of p-torsion groups, Canad. Math. Bull., Vol.27(4), 1984

[2] R.S. Pierce : Homomorphisms of primary abelian groups, Topics in abelian groups, Proceedings New Mexico State University

[3] K. Benabdallah, Kin-Ya Honda : Quasi p-large subgroups of abelian groups, Comment Mathematici Universitatis Sancti Pauli, Vol.31(2), 1982, ed. Rikkyo Univ. Math. Ikebukuro Tokyo, 171, Japan

[4] K. Benabdallah, R. Wilson : Thick groups and essentially finitely indecomposable groups, Canad. Journal of Mathematics, Vol.XXX, No.3, 1978, 650-654.

[5] L. Fuchs, Infinite abelian groups, Vol. I et II, Academic Press, New York, 1970 et 1973.

Ecole Polytechnique de THIES
Boîte Postale 10, Thies
SENEGAL

Received January 6, 1987

C.R. Math. Rep. Acad. Sci. Canada - Vol. XI, No. 2, April 1987 avril

THE GENERALIZED FERMAT-TORRICELLI POINT AND THE GENERALIZED LHUILIER-LEMOINE POINT

D.S.Mitrinović, J.E.Pečarić and V.Volenec

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

ABSTRACT. In this paper we give some comments on the generalized Fermat-Torricelli point and the generalized Lhuilier-Lemoine point. Certain facts which contest some priorities are brought to light. We also give some new results concerning polytopes.

1. Let P be a point inside the triangle $A_1A_2A_3$. Let $R_k = PA_k$ and let r_k be the distance from P to the side A_kA_{k+1} ($k=1,2,3$, $A_4 = A_1$).

P.Fermat had given the suggestion to Torricelli to find the point for which the minimum of ΣR_1 is attained. Torricelli found three solutions and he gave the same problem to Viviani. Viviani published a solution of his own in 1658. This important point, known as the Fermat-Torricelli point, was studied by T.Simpson in 1750, Fuss in 1798, Tédenat and Lhuilier in 1810, Gruson in 1816, Bertrand in 1843, Lehmus in 1854, Grunert in 1867, etc. [17].

S.Lhuilier, in 1809, investigated the point in a triangle (or tetrahedron) having the minimal sum of squares of distances to the sides (or faces). E.W.Grebe rediscovered this point in 1847, and É.Lemoine again in 1873. It bacame generally known as the "Lemoine point" (or occasionally the "Grebe point"), but its discovery by Lhuilier was forgotten.

For a given scalene triangle $A_1A_2A_3$ and a variable point P, let F_t denote the position of P for which ΣR_1^t is extremal, and let L_t denote the position for which Σr_1^t is extremal.

P.Penning [10] shows that the locus of F_t, when t varies over all real values, is a curve (having two branches) which lies entirely

inside the triangle and passes through the midpoints of the sides, two distinct points F_{+o} and F_{-o}, the Fermat-Torricelli point F_1, the centroid F_2, and the circumcentre F_∞. (The letter F is appropriate because it was Fagnano who first observed that F_2 is the centroid.)

H.S.M.Coxeter has noticed that the locus of L_t coincides with the locus of the point whose trilinear coordinates r_ν are proportional to a_ν^u ($\nu = 1,2,3$) when u varies over all real values ($u = 1/(t-1)$). Thus it is a curve passing through the centroid L_0, the vertex $L_1 = A_1$ (if $a_1 > a_2 > a_3$), the Lhuilier-Lemoine point L_2 (hence the use of the letter L), and the incentre L_∞. J.L.Synge has given the following proof:

Since $\Sigma a_1 r_1 = 2F$, $\Sigma a_1 dr_1 = 0$. If Σr_1^t is extremal, $\Sigma r_1^{t-1} dr_1 = 0$. Thus $r_\nu^{t-1} = \lambda a_\nu$ ($\nu = 1,2,3$) and $r_\nu = \mu a_\nu^u$ ($u = 1/(t-1)$).

The point whose trilinear coordinates are proportional to a_ν^u is, of course, the point whose areal coordinates are proportional to a_ν^{u+1}. Its locus was thoroughly investigated by O.Bottema and P.Penning [1].

2. Now, we shall give a generalization of the above result for the generalized Lhuilier-Lemoine point.

Let P be any point inside a convex polytope $\mathcal{A}$ from E^n ($n \geq 2$) with m ($m > n$) facets a_i. Let C_i ($i=1,\ldots,m$) be the (n-1)-dimensional contents of a_i, and let r_i be the distances of the point P to the hyperplanes of a_i. If V is the volume of $\mathcal{A}$, then

$$\sum_{i=1}^{m} C_i r_i = nV. \tag{1}$$

The following result contains the generalization of L_t:

THEOREM 1. Let x_i ($i=1,\ldots,m$) be positive numbers. If either $t > 1$ or $t < 0$, then

$$\sum_{i=1}^{m} x_i r_i^t \geq (nV)^t \Big(\sum_{i=1}^{m} (C_i^t / x_i)^{1/(t-1)} \Big)^{1-t} \tag{2}$$

with equality if and only if

$$x_1 r_1^{t-1}/C_1 = x_2 r_2^{t-1}/C_2 = \dots = x_m r_m^{t-1}/C_m. \tag{3}$$

For $0 < t < 1$, the reverse inequality is valid.

Remarks: 1° The case $m = n+1$, $p < 0$ is given in [6], and $n = 2$, $m = 3$, $p > 1$ in [2,4].

2° For $t > 1$, we have

$$\sum_{i=1}^{m} x_i r_i^t \le (nV)^t \max_{1\le i\le m} (x_i/C_i^t) \qquad (= M).$$

Indeed, since $0 \le C_i r_i/nV \le 1$ $(1 \le i \le m)$ we have

$$\frac{1}{(nV)^p} \sum_{i=1}^{m} x_i r_i^t = \sum_{i=1}^{m} \frac{x_i}{C_i} \left(\frac{C_i r_i}{nV}\right)^t \le M \sum_{i=1}^{m} \left(\frac{C_i r_i}{nV}\right)^t \le M \sum_{i=1}^{m} \frac{C_i r_i}{nV} = M.$$

For $n = 2$, $m = 3$, we infer a result from [4].

3° In [11], S.Reich asked to prove or disprove the triangle inequality

$$\Sigma\, 1/r_1 \ge 3/r. \tag{4}$$

L.Carlitz noted that the inequality is invalid and proved (2) for $m = 3$, $x_1 = x_2 = x_3 = 1$, $t = -1$. Klamkin [6] showed that instead of (4) the following analogous inequality is true:

$$\Sigma\, 1/r_1 \ge 2/r \tag{5}$$

with equality for a degenerate triangle. He also gave generalizations of (5) for a simplex (see [6,7]). Similar generalizations are valid for a circumscribable polytope. For example, we have

$$\sum_{i=1}^{m} 1/r_i^p \ge 2/r^p \qquad (p > 0). \tag{6}$$

Indeed, using (2), we get

$$\sum_{i=1}^{m} \frac{1}{r_i^p} \ge \frac{1}{(nV)^p} \Big(\sum_{i=1}^{m} C_i^{p/(p+1)}\Big)^{p+1} = \Big(\sum_{i=1}^{m} C_i^{p/(p+1)}\Big)^{p+1} / \Big(r \sum_{i=1}^{m} C_i\Big)^p \ge 2/r^p.$$

The last inequality follows from the inequality

$$\frac{1}{2}\sum_{i=1}^{m} c_i^q \geq \left(\frac{1}{2}\sum_{i=1}^{m} c_i\right)^q, \tag{7}$$

where $q = p/(p+1)$ (so, $0 < q < 1$). Note that (7) is a simple consequence of Petrović's inequality: $\Sigma f(x_i) \geq 2f(\frac{1}{2}\Sigma x_i)$, for a concave function $f:[0,a) \to R$, $f(0) = 0$, and $0 \leq x_k \leq \frac{1}{2}\Sigma x_i$ $(k=1,\ldots,m)$.

First, we shall prove the following

LEMMA. Let x_i $(i=1,\ldots,m)$ be positive numbers with $X_m = \sum_{i=1}^{m} x_i$ such that $C_i r_i / x_i \leq d$ $(i=1,\ldots,m)$ and let $f:(0,d] \to R$ be a convex function. Then

$$\sum_{i=1}^{m} x_i f(C_i r_i / x_i) \geq X_m f(nV/X_m). \tag{8}$$

If f is strictly convex, then equality holds in (8) only if

$$C_1 r_1 / x_1 = C_2 r_2 / x_2 = \ldots = C_m r_m / x_m. \tag{9}$$

The inequality is reversed if f is a concave function.

PROOF. Using Jensen's inequality for convex functions and (1), we get

$$X_m f(nV/X_m) = X_m f\left(\frac{1}{X_m}\sum_{i=1}^{m} x_i (C_i r_i / x_i)\right) \leq \sum_{i=1}^{m} x_i f(C_i r_i / x_i).$$

PROOF OF THEOREM 1. For $f(x) = x^t$, $x_i \to (C_i^t / x_i)^{1/(t-1)}$ $(i=1,\ldots,n)$, we get Theorem 1 from the Lemma.

3. Now, we shall give some other consequences of the Lemma.

THEOREM 2. For $x_1 = \ldots = x_m = 1$, (8) becomes $\sum_{i=1}^{m} f(C_i r_i) \geq m f(nV/m)$.

EXAMPLES: 1° For $f(x) = x^p$ we get $\sum_{i=1}^{m} (C_i r_i)^p \geq m^{1-p} n^p V^p$ $(p < 0$ or $p > 1)$ and the reverse inequality for $0 < p < 1$.

The cases $n = 2$ and 3 were considered in [16], and these results were generalizations of results from [8,9,14,15].

2° For $f(x) = \log x$ we get $\prod_{i=1}^{m} (r_i C_i) \leq (nV/m)^m$.

This is a generalization of results from [12] $(n = 2,3,\ m = n+1)$.

THEOREM 3. For $x_i = C_i$ $(i=1,\ldots,m)$, (8) becomes

$$(10)\qquad \sum_{i=1}^{m} C_i f(r_i) \geq C f(nV/C),$$

where $C = \sum_{i=1}^{m} C_i$ is the "surface" of the polytope.

Remark. The cases $f(x) = x^p$, $n = 2$ and $n = 3$ were given in [16].

Let $\mathcal{A}$ be a circumscribable polytope, i.e. let a hypersphere of radius r be inscribed in $\mathcal{A}$. Then (1) gives $nV = \sum_{i=1}^{m} C_i r$, i.e. $r = \frac{nV}{C}$.

In this case (10) becomes $\sum_{i=1}^{m} C_i f(r_i) \geq C f(r)$.

EXAMPLES: 3^0 For $f(x) = x^p$ we get $\sum_{i=1}^{m} C_i r_i^p \geq C r^p$ $(p>1$ or $p<0)$. For $0<p<1$, the reverse inequality is valid.

For $n = 2$, $m = 3$ we have a result from [16], generalizing results from [2,12].

4^0 For $f(x) = \log x$, we get: $\prod_{i=1}^{m} r_i^{C_i} \leq r^C$.

THEOREM 4. (i) $\sum_{1\leq i<j\leq m} C_i C_j r_i r_j \leq \frac{m-1}{2m} n^2 V^2$,

(ii) $\sum_{1\leq i<j\leq m} C_i C_j r_i r_j + \sum_{i=1}^{m} C_i^2 r_i^2 \geq \frac{m+1}{2m} n^2 V^2$.

PROOF. These results are simple consequences of Example 1^0 for $p = 2$ and of identity $\sum_{1\leq i<j\leq m} C_i C_j r_i r_j = \frac{1}{2}(n^2V^2 - \sum_{i=1}^{m} C_i^2 r_i^2)$.

Remark. For $m = 3$, $n = 2$, (i) is given in [13] and (ii) is due to L. Carlitz.

THEOREM 5. For a triangle the following inequalities are valid

$$(11)\qquad (\Sigma \sqrt{r_1})^2 \leq (s^2+r^2+4Rr)/2R$$

with equality only if $P = I$; and

$$(12)\qquad \Sigma \sqrt{r_1} \leq (R+r)\sqrt{2/R} \leq 3\sqrt{R/2}$$

with equalities only if a triangle is equilateral and P is its center.

PROOF. This is a consequence of Theorem 1 ($m = 3$, $t = 1/2$, $x_1 = x_2 = x_3 = 1$), of identity $\Sigma 1/a = (s^2+r^2+4Rr)/(4Rrs)$ and of the well-known

inequality $s^2 \leq 4R^2+4Rr+3r^2$.

Remark. (12) is an interpolation of an inequality of L.Carlitz [3].

ACKNOWLEDGEMENT. The authors are grateful to Professor H.S.M. Coxeter for useful suggestions.

Received January 6, 1987

REFERENCES:

1. O.BOTTEMA and P.PENNING, De verzameling van de punten welker oppervlaktecoordinaten ten oprichte van een driehoek zich verhouden als machten van de zijdelengten. Nieuw Tijdschrift woor Wiskunde 72 (1985), 157-162.
2. L.CARLITZ-M.S.KLAMKIN, Problem 910. Math.Mag. 48 (1975), 242-243.
3. L.CARLITZ-M.S.KLAMKIN, Problem 959. Math.Mag. 50 (1977), 212-213.
4. N.SCHAUMBERGEN-M.S.KLAMKIN, Problem 140. Two-Year Coll.Math.J. 11 (1980), 279-280.
5. H.H.HAMZIN, Problem 749. Mat. v škole 1970, No 2, 88, and No 6, 75.
6. M.S.KLAMKIN, Extensions of a triangle inequality of Carlitz. Univ. Beograd.Publ.Elektrotehn.Fak.Ser.Mat.Fiz. No 602-633 (1978), 147-149.
7. M.S.KLAMKIN, Extensions of a triangle inequality of Carlitz II. Ibid. No 678-715 (1980), 159-160.
8. I.LIVIU, Problem 17055. Gaz.Mat.(Bucharest) 83 (1978), 82.
9. D.MIHEŢ, Problem 13668. Ibid. B 24 (1973), 740.
10. P.PENNING, Expoints. Nieuw Archief voor Wiskunde (3), 4 (1986), 19-31.
11. S.REICH-L.CARLITZ, Problem 801. Math.Mag. 44 (1971), 166 and 45 (1972), 107-109.
12. D.O.ŠKLARSKIJ-N.N.ČENCOV-I.M.JAGLOM, Geometriceskie neravenstva i zadaci na maksimum i minimum. Moskva, 1970.
13. I.I.TOMESCU, Problem 9290. Gaz.Mat.(Bucharest) B 20 (1969), 335-336
14. I.TOMESCU, Problem 13027. Ibid. B 24 (1973), 307.
15. I.TOMESCU, Problem 13248. Ibid. B 24 (1973), 372.
16. I.TOMESCU, Generalizări ale Problemei 13027. Ibid. B 24 (1973), 583-586.
17. É.VIGARIÉ, Esquisse historique sur la marche du développement de la géométrie du triangle. Association française pour l'avancement des sciences. Congrès de Paris 1889, pp. 1-25.

Tehn. fak., p.p. 177, Zagreb 41000, Yugoslavia

A Moment Method for Primes in Short Intervals

A. Y. Cheer and D. A. Goldston
Presented by P. Ribenboim, F.R.S.C.

Abstract. We present a method for showing that there is a positive proportion of intervals which contain no primes and are longer than the average distance between consecutive primes. This method uses the first three moments for the distribution of intervals with a given number of primes. Better results are obtained conditionally by assuming the first n moments are Poisson.

Introduction. In this paper we examine the occurrence of long intervals containing no prime numbers from a statistical point of view. Previous work on this subject (see[5], chapter 5) has been directed towards constructing very long sequences of consecutive composite numbers. However, these sequences occur so infrequently that they have no statistical significance. We introduce in this paper a moment method for finding a positive proportion of intervals which are longer than the average and which contain no primes.

Let $\pi(x)$ denote the number of primes less than or equal to x. We define the kth moment for the number of primes in an interval of length $\lambda \log x$ by

$$(1)\quad M_k(\lambda,X) = \frac{1}{X}\int_X^{2X} \left(\pi(x+\lambda\log x) - \pi(x)\right)^k dx \quad .$$

We also define, for $n = 0, 1, 2, \ldots$,

$$(2)\quad a_n(\lambda,X) = (1/X)(\text{ measure } \{ x \in [X, 2X] : [x, x + \lambda\log x] \text{ contains exactly n primes}\}) .$$

Since the integrand in (1) is a step function, we have,

$$(3)\quad M_k(\lambda,X) = \sum_{n=1}^{\infty} n^k a_n(\lambda,X) \quad , \quad \text{for } k = 1,2,3,\ldots \quad .$$

The sum above is actually a finite sum since $a_n(\lambda,X) = 0$ for $n \geq X$. We also have the obvious relations

$$(4)\quad a_0(\lambda,X) + \sum_{n=1}^{\infty} a_n(\lambda,X) = 1$$

and

(5) $a_n(\lambda,X) \geq 0$, for n = 0,1,2,. . . .

The quantities $a_n(\lambda,X)$ represent the percentage of intervals of length λlogx which contain exactly n primes. Since the average spacing between consecutive primes is logx, our goal is to show that $a_0(\lambda,X)$ is non-zero for some $\lambda > 1$ and all sufficiently large X. To accomplish this, let us suppose we are given $M_k(\lambda,X)$ for k=1, 2, . . . N, and let us assume $a_0(\lambda,X) = 0$. Then (3) and (4) form a system of N+1 linear equations in the non-negative unknowns $a_1(\lambda,X)$, $a_2(\lambda,X)$, ... , and it becomes a linear programming problem to solve this system for a given λ. If however there is no solution for a given λ, then we conclude that the assumption that $a_0(\lambda,X) = 0$ is untenable.

We cannot carry out the above approach as described because our knowledge of the moments $M_k(\lambda,X)$ is limited to crude upper and lower bounds for $k \geq 2$, but it is possible to use these bounds for $M_2(\lambda,X)$ and $M_3(\lambda,X)$ in equations (3), (4), and (5) to prove a weak result of the desired type:

Theorem 1. We have $a_0(1.004,X) \geq c > 0$ for all sufficiently large X, where c is an absolute constant.

It is easy to see that, for p_n the nth prime number, and $d_n = p_{n+1} - p_n$ the length of the nth gap between consecutive primes,

$$(6)\quad a_0(\lambda,X) \sim \frac{1}{X} \sum_{\substack{X \leq p_n \leq 2X \\ d_n \geq \lambda \log p_n}} \left(d_n - \lambda \log p_n \right) \quad , \quad \text{as } X \to \infty .$$

In another paper[1], we have shown that by using a method of Erdös for small gaps between primes, it is possible to find a lower bound for the above sum for any $\lambda < 9/8$, and therefore this value also holds for Theorem 1. However, that method cannot be made to hold for $\lambda > 3/2$, while the method presented here has no such limitations.

It has been conjectured that the primes are distributed around their average in a Poisson distribution. Gallagher[2] has shown that this conjecture is true if the Hardy-Littlewood r-tuple conjecture holds uniformly over tuples of primes of lengths λlogx. In the case of the Poisson distribution, we have

$$(7)\quad M_k(\lambda,X) \sim m_k(\lambda) = \sum_{r=1}^{k} \sigma(k,r) \frac{\lambda^r}{r!} \quad , \quad \text{as } X \to \infty ,$$

and

(8) $a_n(\lambda,X) \sim \frac{\lambda^n}{n!} e^{-\lambda}$, as $X \to \infty$.

Here $\sigma(k,r)$ are the Stirling numbers of the second type, and $m_k(\lambda)$ is the kth moment of a Poisson distribution. In particular we have $a_0(\lambda,X) \sim e^{-\lambda} > 0$ for all λ. This result requires all the moments to be Poisson, but if we assume that only the second and third moments are Poisson, we can substantially improve on Theorem 1 and the results in [1] :

Theorem 2. Assume (7) holds for k=2 and k=3. Then, for $\varepsilon > 0$ and all sufficiently large X, we have

(9) $a_0(\lambda,X) > 1 - \lambda + \frac{5}{12}\lambda^2 - \frac{1}{12}\lambda^3 - \varepsilon$, for $0 \le \lambda \le 2$,

and

(10) $$\sum_{X \le p_n \le 2X} d_n^2 \ge \left(\frac{14}{9} - \varepsilon\right) X\log X \quad .$$

By assuming further moments are Poisson, it is possible to prove better results than the above; we mention some of these in the last section.

2.Proof of Theorem 1. The following is known about the first three moments $M_k(\lambda,X)$: for fixed λ, $\varepsilon > 0$, and X sufficiently large,

(11) $M_1(\lambda,X) \sim \lambda$, as $X \to \infty$,

(12) $\lambda/2 + \lambda^2 - \varepsilon \le M_2(\lambda,X) \le \lambda + C\lambda^2 + \varepsilon$,

(13) $M_3(\lambda,X) \le \lambda + 3C\lambda^2 + D\lambda^3 + \varepsilon$.

Equation (11) is the prime number theorem, the lower bound in equation (12) is from [3], and the upper bound in equation (12) and equation (13) follow from sieve upper bounds applied to the argument on page 5 of [2]. The number C is the sieve constant in the bound for prime twins, and D is the corresponding constant in the 3-dimensional sieve for prime triples. The value C = 4 and D = 48 may be found in [4].

We now prove Theorem 1. We may ignore all ε's and X dependences, since these have no effect on the proof. We fix λ, and write $a_n(\lambda,X)$ as a_n . By combining (3), (4), (11), (12), and (13), with C = 4 and D = 48, we have

(14) $$\sum_{n=1}^{\infty} a_n = 1, \quad \sum_{n=1}^{\infty} n a_n = \lambda, \quad \sum_{n=1}^{\infty} n^2 a_n \ge \frac{\lambda}{2} + \lambda^2, \quad \sum_{n=1}^{\infty} n^3 a_n \le \lambda + 12\lambda^2 + 48\lambda^3 .$$

By recombining we obtain

$$(15)\quad \sum_{n=1}^{\infty}(n-1)a_n=\lambda-1\,,\quad \sum_{n=1}^{\infty}(n-1)^2a_n\ge\lambda^2-\frac{3}{2}\lambda+1\,,\quad \sum_{n=1}^{\infty}(n-1)^3a_n\le 48\lambda^3+9\lambda^2+\frac{5}{2}\lambda-1\,.$$

By Cauchy's inequality

$$(16)\quad \Big(\sum_{n=1}^{\infty}(n-1)^2a_n\Big)^2\le\Big(\sum_{n=1}^{\infty}(n-1)a_n\Big)\Big(\sum_{n=1}^{\infty}(n-1)^3a_n\Big)$$

By substituting (15) into (16) we obtain $0\le 47\lambda^3-36\lambda^2-(43/4)\lambda-(1/2)$. This is false unless λ is larger than the root $\lambda_0=1.004259085\ldots$, which proves Theorem 1. The above argument is very close to optimal. Using a linear programming computation we find (15) is unsolvable for $\lambda=1.0042591123$, while for $\lambda=1.0042591124$ we have the (rounded) solution $a_1=.99996$, $a_{117}=1.3041\text{x}10^{-9}$, $a_{118}=3.6518\text{x}10^{-6}$, and $a_{119}=3.2472\text{x}10^{-5}$.

3. Proof of Theorem 2. We now assume the second and third moments $M_k(\lambda,X)$ are Poisson, which together with (11) give

$$(17)\quad M_1(\lambda,X)\sim\lambda\,,\quad M_2(\lambda,X)\sim\lambda+\lambda^2\,,\quad M_3(\lambda,X)\sim\lambda+3\lambda^2+\lambda^3\,.$$

Once again we ignore ε and X dependences, since they have no effect on the argument. Before proving Theorem 2, we show that the previous argument now gives that $a_0(\lambda,X)>0$ for any $\lambda<2$. By (17) we have that equation (14) may be replaced by

$$(18)\quad \sum_{n=1}^{\infty}a_n=1,\quad \sum_{n=1}^{\infty}n\,a_n=\lambda,\quad \sum_{n=1}^{\infty}n^2a_n=\lambda+\lambda^2,\quad \sum_{n=1}^{\infty}n^3a_n=\lambda+3\lambda^2+\lambda^3\,;$$

which on recombining gives

$$(19)\quad \sum_{n=1}^{\infty}(n-1)a_n=\lambda-1,\quad \sum_{n=1}^{\infty}(n-1)^2a_n=\lambda^2-\lambda+1,\quad \sum_{n=1}^{\infty}(n-1)^3a_n=\lambda^3+\lambda-1\,.$$

On substituting into (16) we obtain $0\le\lambda^2(\lambda-2)$, whence $\lambda\ge 2$. This argument is sharp since $a_1=2/3$, $a_4=1/3$, and the other $a_n=0$ satisfy equation (18) when $\lambda=2$.

We now prove Theorem 2. It is well known that for the Poisson distribution

$$(20)\quad \sum_{n=0}^{\infty}n(n-1)(n-2)\ldots(n-k+1)\,a_n(\lambda)=\lambda^k,\qquad \text{for } k\ge 1\,.$$

This may be easily verified for k=1, 2, and 3 by (18). By (4) we have

$$(21)\quad a_0(\lambda)=1-\sum_{n=1}^{\infty}a_n(\lambda)\ \ge\ 1-\sum_{n=1}^{\infty}p(n)\,a_n(\lambda)\,,$$

where p(n) is any function such that $p(n) \geq 1$ for n = 1, 2, 3, ... Suppose p(n) is a polynomial of the form

$$(22)\quad p(n) = \sum_{k=1}^{N} B_k\, n(n-1)(n-2)\ldots(n-k+1) \quad , \; p(n) \geq 1 \text{ for } n=1,2,3,\ldots .$$

By (20) and (21) we conclude that

$$(23)\quad a_0(\lambda) \geq 1 - \sum_{k=1}^{N} B_k \lambda^k$$

Now take $p(n) = (1/12)(n-1)(n-3)(n-4) + 1$. Clearly $p(n) \geq 1$ for n = 1, 2, 3,... . Putting p(n) into the form of (22) gives $p(n) = n - (5/12)n(n-1) + (1/12)n(n-1)(n-2)$,which proves the first part of Theorem 2. The second part follows from the relation (see [1])

$$(24)\quad \sum_{X \leq p_n \leq 2X} d_n^2 \quad \sim \quad 2X\log X \int_0^{\infty} a_0(\lambda,X)\, d\lambda$$

4. N Poisson Moments. The methods used above can be applied to N moments which are assumed to be Poisson. For N=5 the polynomial $p(n) = (n-1)(n-3)(n-6)(n-7)/504 + 1$ shows that $a_0(\lambda,X) > 0$ for any $\lambda<3$, and gives the constant 1.782. . . in (10). For N = 2k+1, the polynomial $p(n) = (n-1)(n-2)\ldots(n-2k-1)/(2k+1)! + 1$ shows that

$$(25)\quad a_0(\lambda,X) \geq \sum_{n=0}^{2k+1} \frac{(-\lambda)^n}{n!}$$

This may also be seen in an easier fashion by differentiating the power series generating function for the $a_n(\lambda,X)$'s and using (20). However, none of these estimates are optimal. Suppose the first N moments are Poisson, and let Λ_N be the supremum of the set of all λ's for which the the N+1 equations (3) and (4) have no solutions $a_n(\lambda,X) \geq 0$ with $a_0(\lambda,X) = 0$. By using a linear programming calculation, we computed the first few Λ_N . We found that in general $\Lambda_{2N} = \Lambda_{2N-1}$, and $\Lambda_3 = 2$, $\Lambda_5 = 3.11713...$, $\Lambda_7 = 4.143770...$, $\Lambda_9 = 5.238078...$, and $\Lambda_{11} = 6.291643...$.

5. Acknowledgement. Theorem 1 was obtained jointly with D. R. Heath-Brown, who we would like to thank. We would also like to thank A. Odlyzko and C. Pomerance for helpful suggestions. This work was completed while A. Cheer was on sabbatical at NASA/Ames Research Center, Moffett Field, Calif. .

References

[1] A. Y. Cheer and D. A. Goldston,"Larger than average gaps between consecutive prime numbers" to appear

[2] P. X. Gallagher,"On the distribution of primes in short intervals", Mathematika 23 (1976), 4-9.

[3] D. A. Goldston,"The second moment for prime numbers", Quarterly J. Math. Oxford (2), 35 (1984), 153-163.

[4] H. Halberstam and H.-E. Richert, Sieve Methods, Academic Press, London 1974.

[5] K. Prachar, Primzahlverteilung, Springer-Verlag, Berlin, 1957.

Department of Mathematics
University of California
Davis, California 95616

Department of Mathematics and Computer Science
San Jose State University
San Jose, California 95192

Received January 13, 1987

DOUBLE COVERINGS OF HYPERELLIPTIC KLEIN SURFACES

E. Bujalance*, J.J. Etayo* and J.M. Gamboa*

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

Abstract. Totally real (in particular unramified) coverings of Klein surfaces were studied in [6]. They obtain the topological features of the covering as a function of the ones of the base. Here we restrict ourselves to elliptic-hyperelliptic normal unramified double coverings of hyperelliptic bordered surfaces, obtaining of course additional information. Besides we present a conjecture on the classification of all double coverings of hyperelliptic surfaces. The details of the proofs will appear in [4]. The corresponding questions on Riemann surfaces have been studied in [2,5].

Klein surfaces are compact surfaces with a dianalytic structure [1]. A Klein surface X is said q-hyperelliptic if it has an involution ϕ such that X/ϕ has algebraic genus q. 0-hyperelliptic surfaces are called hyperelliptic. 1-hyperelliptic surfaces are elliptic-hyperelliptic. A covering of a surface X is a couple (X',π), X' being a Klein surface and π a surjective morphism from X' onto X. The covering is normal and unramified if the group of automorphisms of X' commuting with π acts transitively over the fibers and without fixed points on X'.

We will say that a surface X has type $(g,+,k)$ (resp., $(g,-,k)$) if it has topological genus g and k boundary components, and is orientable (resp., non-orientable).

The result we obtain is the following:

Theorem. Let X be a hyperelliptic Klein surface with boundary of algebraic genus $p = \alpha g+k-1 > 3$ ($\alpha=2$ in orientable case, $\alpha=1$ otherwise) and let $\pi : X' \to X$ be an unramified elliptic-hyperelliptic double covering of X.

a) If X has type $(g,+,k)$ with $g \neq 0$ (and so $k < 3$ by [7]) then X' has type $(2g-1,-,2k)$ and the number of such coverings is $\binom{2g+k}{2}$.

b) If X has type $(0,+,k)$ then X' has type $(0,+,2k-2)$ or $(1,+,2k-4)$ and the number of such coverings is k of the first kind, $\binom{k}{2}-k$ of the second one.

c) If X has type $(g,-,k)$ then X' has type

i) if $k = 1$, $(2g-2,-,2)$ and the number of such coverings is $\binom{g+1}{2}$.

ii) if $k = 2$, $(2g,-,2)$, $(2g-2,-,4)$ or $(g-1,+,4)$, in respective numbers $2g$, $\binom{g}{2}$ and 1.

iii) if $k > 2$, $(2g-2,-,2k-4)$, $(2g,-,2k-2)$ and $(2g-2,-,2k)$, in respective numbers $\binom{k}{2}-k$, $kg+k$ and $\binom{g}{2}$.

The tool we use to prove the theorem, and which reduces the problem to a combinatorial question, is the theory of NEC groups. An NEC group Γ is a discrete subgroup of the group of isometries of the hyperbolic plane D, and it has associated a signature $(g,\pm,[m_1,\dots,m_r],\{(n_{i1},\dots,n_{is_i})_{i=1,\dots,k}\})$ which gives a presentation of the group (see [9,12]) and reflects the topological properties of the projection $D \to D/\Gamma$. We use in what follows this presentation of the group. Each bordered surface X of algebraic genus $p > 2$ may be expressed as D/Γ; when X has type $(g,\pm,k)$, Γ has signature $(g,\pm,[-],\{(-)^k\})$ [10]. In [7] it is proved that the surface D/Γ is hyperelliptic (resp., elliptic-

hyperelliptic) if and only if there exists an NEC group Γ_1 of algebraic genus 0 (resp., 1) such that $[\Gamma_1:\Gamma] = 2$. This group is unique when D/Γ has genus greater than or equal to 2 (resp., 6) (a particular case of Castelnuovo's inequality [11]).

Proof of the theorem. We sketch the proof of part a) of the theorem. The other parts are dealt in a similar way.

The signature of the group Γ_1 of the hyperellipticity of $X = D/\Gamma$ is $(0,+,[2,\overset{2g+k}{\ldots},2],\{(--)\})$ [3]. Since D/Γ' is an unramified covering of D/Γ the signature of Γ' has neither proper periods nor non-empty period-cycles. Applying the relation of areas of NEC groups and [8], the signature of Γ' is thus $(g',+,[--],\{(--),\overset{4g+2k-2-2g'}{\ldots},(--)\})$. Since the covering is unramified, we have besides $2 \leq 4g+2k-2-2g' \leq 4$. Calling now Γ_1' the group of the elliptic-hyperelliptic character of D/Γ', by [4] and from the fact that Γ_1' has no non-empty period-cycle (since Γ_1' is a normal subgroup of Γ, D/Γ' having genus greater than 5), one can reduce to the case that Γ_1' has signature $(0,+,[2,\overset{4g+2k-4}{\ldots},2],\{(--)(--)\})$, with $4g+2k = 6$ if $g'=0$. Since the signature of Γ is $(g,+,[--],\{(--),\overset{k}{\ldots},(--)\})$, there exists an epimorphism θ_1 from Γ_1 onto C_2 with kernel Γ, defined by $\theta_1(x_1) = \ldots = \theta_1(x_{2g+k}) = \bar{1}$, $\theta_1(c_{10}) = \bar{0}$, $\theta_1(e_1) = \bar{k}$. For each group Γ_1 we now define an epimorphism θ from Γ_1 onto C_2 with kernel Γ_1'. This epimorphism is given by $\theta(x_i) = \theta(x_j) = \bar{1}$, for two values $i,j \leq 2g+k$, $\theta(x_m) = \bar{0}$ for $i \neq m \neq j$. $\theta(c_{10}) = \theta(e_1) = \bar{0}$. The number of epimorphisms defined in this way is $\binom{2g+k}{2}$. We prove now that for each epimorphism θ there exists an associated subgroup Γ' of Γ_1' with signature $(g',+,[--],\{(--),\overset{4g+2k-2-2g'}{\ldots},(--)\})$. If we suppose, for simpli-

city. $i=1$, $j-2$, a set of generators of Γ_1' is $x_1' = x_2x_3x_2$, $x_2' = x_2x_4x_2$, $\cdots$, $x_{2g+k-2}' = x_2x_{2g+k}x_2$, $x_{2g+k-1}' = x_3$, $\cdots$, $x_{4g+2k-4}' = x_{2g+k}$, $c_{10}' = c_{10}$, $c_{20}' = x_1c_{10}x_1$, $e_1' = e_1$, $e_2' = x_1e_1x_1$. We define now θ' from Γ_1' onto C_2 by $\theta'(x_1') = \ldots = \theta'(x_{4g+2k-4}') = \bar{1}$. $\theta'(c_{10}') = \theta'(c_{20}') = \bar{0}$, $\theta'(e_1') = \theta'(e_2') = \bar{k}$. We call $\Gamma' = \ker\theta'$ and this is the subgroup of Γ_1' and of Γ we were looking for.

Each group Γ' provides us a distinct covering D/Γ' and we have so all coverings with signature $(2g-1,+,[-],\{(-),\overset{2k}{\ldots},(--)\})$. (Notice that the number of period-cycles in Γ' is $2k$, and so $4g+2k-2-2g' = 2k$, which implies $g' = 2g-1$).

By addition of the number of coverings of the different topological types we deduce:

Corollary. If X is a hyperelliptic Klein surface of algebraic genus $p > 3$ the number of elliptic-hyperelliptic unramified double coverings of X is $\binom{p+1}{2}$.

Remark. According with [6], if X is an arbitrary bordered Klein surface of type $(g,+,k)$ and X' is an arbitrary unramified double covering of X, then X' has type $(2g+t+1,+,2k-2t)$ and for each t, $0 < t \leq [\frac{k}{2}]$, there are $2^{p+1-k}\binom{k}{2t}$ such coverings. for $t = 0$ there are $2^{p+1-k}-1$. Observe that from part a) of our theorem. when X is hyperelliptic and X' is elliptic-hyperelliptic, $t = 0$ and there are only $\binom{p+1}{2}$ coverings.

A similar situation appears in cases b) and c).

We now formulate a conjecture. If X is a hyperelliptic Klein surface whose algebraic genus is $p \geq 2$, we prove in [3] that the

number of hyperelliptic unramified double coverings of X is $p+1 = \binom{p+1}{1}$. When $p > 3$ the number of elliptic-hyperelliptic unramified double coverings of X is $\binom{p+1}{2}$, as we proved above. Since the number of unramified double coverings of X is 2^p-1, we conjecture that the unramified double coverings of a hyperelliptic surface of genus $p > 2$ may be classified in $[\frac{p+1}{2}]$ classes C_q. $0 \leq q \leq [\frac{p-1}{2}]$, each of them formed by $\binom{p+1}{q+1}$ q-hyperelliptic elements, excepting $C_{(p-1)/2}$, formed by $\frac{1}{2}\binom{p+1}{(p+1)/2}$ elements, all of them $(p-1)/2$-hyperelliptic (holding just if p is odd).

The results of this note may be translated into the language of real algebraic curves using the well-known functorial equivalence established by Alling and Greenleaf [1].

We thank the referee for the very instructive comments on the paper.

* The authors were partially supported by "Comisión Asesora de Investigación Científica y Técnica" (2280/83).

REFERENCES

[1] Alling, N.L. and Greenleaf, N. "Foundations of the theory of Klein surfaces". Lecture Notes in Math., vol. 219, Springer-Verlag: Berlin, etc. (1971).

[2] Bujalance, E. "A classification of unramified double coverings of hyperelliptic Riemann surfaces". Archiv der Math. 47 (1986) 93-96.

[3] Bujalance, E., Etayo, J.J. and Gamboa, J.M. "Hyperelliptic Klein surfaces". Quart. J. Math. Oxford (2) 36 (1985) 141-157.

[4] Bujalance, E., Etayo, J.J. and Gamboa, J.M. "Superficies de Klein elípticas-hiperelípticas". Mem. R. Acad. Ci. Madrid. (to appear).

[5] Farkas, H.M. "Unramified coverings of hyperelliptic Riemann surfaces". Preprint.

[6] Geyer, W.D. and Martens, G. "Überlagerungen berandeter Kleinscher Flächen". Math. Ann. 228 (1977) 101-111.

[7] Gross. B.H. and Harris, J. "Real algebraic curves". Ann. Scient. Ec. Norm. Sup. 14 (1981) 157-182.

[8] Hoare, A.H.M. and Singerman, D. "The orientability of subgroups of plane groups". London Math. Soc. Lect. Note Series 71 (1982) 221-227.

[9] Macbeath. A.M. "The classification of non-euclidean plane crystallographic groups". Can. J. Math. 19 (1967) 1192-1205

[10] Preston. R. "Projective structures and fundamental domains on compact Klein surfaces". Ph. D. thesis. Univ. of Texas (1975).

[11] Stichtenoth, H. "Die Ungleichung von Castelnuovo". J. reine angew. Math. 348 (1984) 197-202.

[12] Wilkie. M.C. "On non-euclidean crystallographic groups". Math. Zeit. 91 (1966) 87-102.

Emilio Bujalance
Departamento de Matemáticas Fundamentales
Facultad de Ciencias
U.N.E.D.
28040 Madrid (Spain)

J.J. Etayo Gordejuela
Departamento de Geometría y Topología
Facultad de C. Matemáticas
Universidad Complutense
28040 Madrid (Spain)

José Manuel Gamboa
Departamento de Algebra y Fundamentos
Facultad de C. Matemáticas
Universidad Complutense
28040 Madrid (Spain)

Received January 19, 1987

Sur la structure réelle des idéaux de $C[X_1, \ldots, X_n]$

Felipe Cucker.

ABSTRACT. We give in this note a left adjoint functor of the complexification which is the algebraic counterpart of considering the euclidean topology on complex algebraic varieties. Some geometrical properties are deduced.

Présenté par P. Ribenboim, F.R.S.C.

Etant donné un corps réel clos $\mathbf{R}$, $\mathbf{C}$ sa clôture algébrique et V une $\mathbf{C}$-variété algébrique affine, l'isomorphisme $\mathbf{C}^n \simeq \mathbf{R}^{2n}$ nous permet regarder l'image de $V(\mathbf{C})$ comme un sous-ensemble algébrique de $\mathbf{R}^{2n}$.

En effet, si $P \in \mathbf{C}[X_1, \ldots, X_n]$ alors $P(a_1+ib_1, \ldots, a_n+ib_n)=0$ ssi les parties réelle et imaginaire du polynôme $P(Z_1+iT_1, \ldots, Z_n+iT_n)$, qui appartiennent à $\mathbf{R}[Z_1, \ldots, Z_n, T_1, \ldots, T_n]$, s'annulent au point $(a_1, \ldots, a_n, b_1, \ldots, b_n)$. Ainsi, si V est l'ensemble des zéros de $P_1, \ldots, P_r$ dans $\mathbf{C}^n$, regardé comme sous-ensemble de $\mathbf{R}^{2n}$ il sera l'ensemble des zéros de $\mathrm{Re}P_1, \ldots, \mathrm{Re}P_r, \mathrm{Im}P_1, \ldots, \mathrm{Im}P_r$.

Cette "réelification" ensembliste possède une contrepartie algébrique (qui à une $\mathbf{C}$-algèbre de type fini associe une $\mathbf{R}$-algèbre de type fini) dont les propriétés de base et les rapports avec la réelification ensembliste sont l'objet de cette note.

Soit $\mathfrak{R}$ et $\mathfrak{C}$ les catégories des $\mathbf{R}$ et $\mathbf{C}$ algèbres de type fini respectivement. On connait bien le foncteur complexification $.[i]: \mathfrak{R} \to \mathfrak{C}$, qui envoie A sur $A[i]=A\otimes_{\mathbf{R}}\mathbf{C}$.

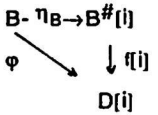
Théorème 1.

Il existe un foncteur $.^{\#}\mathfrak{C} \to \mathfrak{R}$ adjoint à gauche de $.[i]$.

démonstration.

Soit $B=\mathbf{C}[X_1, \ldots, X_n]/(P_1, \ldots, P_r)$ une $\mathbf{C}$-algèbre de type fini quelconque. Appellons $B^{\#}= \mathbf{R}[Z_1, \ldots, Z_n, T_1, \ldots, T_n]/(\mathrm{Re}P_j, \mathrm{Im}P_j)$ $j=1, \ldots, r$ et $\eta_B: B \to B^{\#}[i]$ le morphisme défini par $\eta_B(X_k) = Z_k+iT_k$. Nous allons voir qu'il s'agit d'une flèche universelle (voir [4] III,§1) de B vers $B^{\#}[i]$.

Si D est une $\mathbf{R}$-algèbre de type fini et $\varphi: B \to D[i]$ un morphisme de $\mathbf{R}$-algèbres, il faut voir que $\exists!\ f: B^{\#} \to D$ tel que le triangle suivant commute



Si $\varphi(X_k) = Q_k+iS_k$, $Q_k,S_k \in D$, soit $f(Z_k)=Q_k$ et $f(T_k)=S_k$. Pour que f soit bien définie il faut que $\forall j \leq r$ $f(ReP_j)=f(ImP_j)=0$, ce qui résulte de $f(ReP_j(Z_k,T_k))=ReP_j(Q_k,S_k)$ et $f(ImP_j(Z_k,T_k))=ImP_j(Q_k,S_k)$ puisque $0=\varphi(P_j(X_k))=P_j(Q_k+iS_k)=ReP_j(Q_k,S_k)+iImP_j(Q_k,S_k)$.

En appliquant [4] IV, 1,th.2,ii, nous obtenons que $.^{\#}$ est un foncteur adjoint à gauche de . [i] •

Définition.

Nous appellerons réelification le foncteur $^{\#}$.

Remarques 2.

i) Du théorème mentionné plus haut peut aussi se déduire que si $f:B \to B'$ est un morphisme de C-algèbres, $f^{\#}$est défini comme le morphisme correspondant par l'adjonction à $\eta_{B'}\circ f$; c'est-à-dire si $B'=C[X'_1, \ldots ,X'_m]/(R_1, \ldots ,R_s)$ et $f(X_k)=Q_k(X'_h)$, alors $f^{\#}(Z_k)=ReQ_k(Z'_h,T'_h)$ et $f^{\#}(T_k)=ImQ_k(Z'_h,T'_h)$.

ii) Si V est une C-variété donnée par les polynômes $P_1, \ldots ,P_r$, nous noterons $V^{\#}$ la R-variété donnée par $ReP_1, \ldots ,ReP_r,ImP_1, \ldots ,ImP_r$ et nous noterons φ la bijection $V(C) \simeq V^{\#}(R)$.

Si V est une C-variété et $A=\wp_C(V(C))$, l'anneau des fonctions polynomiales définies sur V(C) à valeurs dans C, on peut se demander si $A^{\#}= \wp_R(V^{\#}(R))$. Prenons $A=C[X]/1+X^2$; on a que $A^{\#}=R[Z,T]/(Z^2-T^2+1, ZT)$. Il est évident que $A^{\#}$ ne coïncide pas avec l'anneau de fonctions polynomiales sur $V^{\#}(R)=\{(0,1),(0,-1)\}$. Donc, la réponse est négative. Nous pouvons prendre une hypothèse plus forte, par exemple V irréductible et nous demander si A intègre entraîne $A^{\#}$ intègre et réel.

Nous verrons bientôt que la réponse à cette question est affirmative. Commençons par un lemme dont l'astuce vient de Ephraim [2].

Lemme 3.

Soit A une C-algèbre de type fini. On a $A^{\#}[i] \simeq A \otimes_C A$.

démonstration.

Soit $A=C[X_1, \ldots, X_n]/(P_1, \ldots, P_r)$, on a bien

$A^{\#}[i] = C[Z_1, \ldots, Z_n, T_1, \ldots, T_n]/(ReP_k, ImP_k)$ $k=1, \ldots, r$.

Considérons le changement linéaire de coordonnées dans C^{2n} $V_j = Z_j + iT_j$ et $W_j = Z_j - iT_j$, $1 \leq j \leq n$. D'autre part considérons l'idéal $(ReP_1, \ldots, ReP_r, ImP_1, \ldots, ImP_r)$ comme étant engendré par les éléments $Q_k = ReP_k + iImP_k$ et $R_k = ReP_k - iImP_k$, $1 \leq k \leq r$. Dans les nouvelles coordonnées on a que $Q_k(V_j, W_j) = P_k(V_j)$ et $R_k(V_j, W_j) = \overline{P_k}(W_j)$, $1 \leq k \leq r$, $1 \leq j \leq n$.

Donc, $A^{\#}[i] \simeq C[V_j, W_j]/(Q_k, R_k) \simeq C[V_j]/P_k \otimes_C C[W_j]/\overline{P_k} \simeq A \otimes_C A$. •

Proposition 4.

Si A est une C-algèbre de type fini intègre (resp. réduite), alors $A^{\#}$ est une R-algébre intègre (resp. réduite).

démonstration.

A intègre (resp. réduite) entraîne $A \otimes_C A$ intègre (resp. réduite) ([5] ch.I,§6, prop.1) ce qui à son tour entraîne $A^{\#}$ intègre (resp. réduite). •

Corollaire 5.

Si A est une C-algèbre de type fini réduite, alors $\dim A^{\#} = 2 \dim A$. •

Ces résultats nous donnent une partie de ce que nous voulions voir. Pour ce qui reste il nous faut examiner ce qui se passe aux points réguliers.

Proposition 6.

Soient $A=C[X_1, \ldots, X_n]/(P_1, \ldots, P_r)$ intègre, V la C-variété donnée par

$(P_1, \ldots, P_r)$ et $x \in V(\mathbf{C})$.

Si x est un point régulier de $V(\mathbf{C})$, alors $\varphi(x)$ est un point régulier de $V^{\#}(\mathbf{R})$.

démonstration.

Soit d la dimension de A; puisque x est un point régulier de $V(\mathbf{C})$ on a que $rg(J(P_j)(x))=n-d$ où J designe la matrice jacobienne. Si l'on fait les changements du lemme, on trouve dans $A^{\#}[i]$ que $rg(J(ReP_j, ImP_j)(x))=rg(J(Q_j, R_j)(x,\bar{x}))$. Mais cette dernière matrice a la forme

$$\left(\begin{array}{c|c} J(P_j)(x) & 0 \\ \hline 0 & \overline{J(P_j)(x)} \end{array}\right)$$

donc, son rang est bien 2(n-d), ce qui entraîne que $\varphi(x)$ est un point régulier de $V^{\#}(\mathbf{R})$. •

Proposition 7.

Si A est une **C**-algèbre de type fini intègre, alors $A^{\#}$ est une **R**-algèbre intègre et réelle.

démonstration.

Soit $A=\mathbf{C}[X_1, \ldots, X_n]/(P_1, \ldots, P_r)$ et V comme ci-dessus. On sait que $Reg(V(\mathbf{C}))\neq\emptyset$; soit donc $x \in Reg(V(\mathbf{C}))$. Nous venons de voir que x est un zéro non singulier de $J=(ReP_j, ImP_j)$ au sens de [1] 3.3.15. Cette même proposition nous assure donc que J est l'idéal des fonctions polynomiales qui s'annulent sur l'ensemble des zéros de J dans $\mathbf{R}^{2n}$, c'est-à-dire que J est réel. •

Corollaire 8.

Si V est une **C**-variété irréductible, alors $V^{\#}$ est une **R**-variété irréductible. •

On peut maintenant améliorer la prop.6.

Théorème 9.

Soit V une C-variété affine irréductible de dim d, $A=\wp_C(V(C))$, $x\in V(C)$. Alors, $x\in Reg(V(C))$ si et seulement si $\varphi(x)\in Reg(V^{\#}(R))$.

démonstration.

La nécéssité c'est la prop. 6.

Pour la suffisance, si $A=C[X_1, \ldots, X_n]/(P_1, \ldots, P_r)$ est un domaine de dimension d, alors

$A^{\#}= R[Z_1, \ldots, Z_n, T_1, \ldots, T_n]/(ReP_1, \ldots, ReP_r, ImP_1, \ldots, ImP_r)$ est un domaine réel de dim 2d . Comme $\varphi(x)$ est régulier dans $V^{\#}(R)$ on doit avoir $rg(J(ReP_j, ImP_j)(x))=2(n-d)$. Donc:

$$rg\left(\begin{array}{c|c} (J(P_j)(x)) & 0 \\ \hline 0 & (J(P_j)(x)) \end{array}\right) = 2(n-d)$$

ce qui est seulement possible si $rg(J(P_j)(x))=n-d$. En conséquence x est régulier dans V(C). •

On peut également améliorer la prop.7.

Théorème 10.

Soit A une C-algèbre de type fini réduite. On a que $A^{\#}$est réelle si et seulement si A est intègre.

démonstration.

La suffisance c'est la prop.7.

Pour la nécéssité, si $A=C[X_1, \ldots, X_n]/(P_1, \ldots, P_r)$ et V est comme toujours, soient $V_1(C), \ldots, V_q(C)$ les composantes irréductibles de V(C).

Puisque $V(C) = V_1(C) \cup \ldots \cup V_q(C)$ on a que $V^{\#}(R) = V_1^{\#}(R) \cup \ldots \cup V_q^{\#}(R)$ et puisque les $V_j(C)$ sont irréductibles pour j=1, ... ,q, les $V_j^{\#}(R)$ doivent l'être aussi d'après le corollaire 8. Ainsi, les $V_j^{\#}(R)$ sont les composantes irréductibles de $V^{\#}(R)$. Puisque $A^{\#}$ est réelle, $A^{\#}=\wp_R(V^{\#}(R))$; donc, $A^{\#}[i]=\wp_C(V^{\#}(C))$ et les composantes irréductibles de $V^{\#}(C)$ sont $V_1^{\#}(C), \ldots, V_q^{\#}(C)$ ([3] ch.I, ex.2.7.).

Mais $V^{\#}(C)=V(C)xV(C)$, et en conséquence elle possède q^2

composantes irréductibles. Ainsi $q^2=q$ ce qui entraîne bien $q=1$. A étant réduite on a bien le résultat chérché. •

Remarque 11.

Le corollaire 8 est un resultat connu quand $\mathbf{R}=\mathbb{R}$ et $\mathbf{C}=\mathbb{C}$ car il resulte du fait que si V est une $\mathbb{C}$-variété irréductible, alors $V(\mathbb{C})$ est connexe. Mais la preuve de ce dernier fait s'appuie sur des arguments analytiques (voir [6] ch.VIII, §2).

Références.

[1] Bochnak, J.; Coste, M.; Roy, M.-F.; Géometrie algébrique réelle , a paraitre chez Springer Verlag.

[2] Ephraim, R.; "C^∞ and analytic equivalence of singularities", Rice Univ. Studies 59,1, 1973.

[3] Kunz, E.; Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, 1985.

[4] Mac Lane, S.; Categories for the Working Mathematician , Springer Verlag G.T.M., 1971.

[5] Mumford, D.; Introduction to algebraic geometry , polycopié, Harvard University.

[6] Shafarevich, I. R.; Basic algebraic geometry , Springer Verlag, 1977.

Note. L'auteur a été partiellement subventioné par C.A.I.C. y T. 2280/83.

Depto. de Algebra.
Facultad de Ciencias.
Univ. de Santander.
SPAIN.

Received January 22, 1987

C.R. Math. Rep. Acad. Sci. Canada - Vol. XI, No. 2, April 1987 avril

A LOWER BOUND FOR LINEAR FORMS IN THE LOGARITHMS OF ALGEBRAIC NUMBERS

J.H. LOXTON, M. MIGNOTTE, A.J. VAN DER POORTEN AND M. WALDSCHMIDT

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

Abstract: We provide an effective lower bound for a homogeneous linear combination with rational coefficients in the logarithms of algebraic numbers. This result implies a lower bound for:

$$|1 - \alpha_1^{b_1}\alpha_2^{b_2} \ldots \alpha_n^{b_n}| ,$$

with nonzero algebraic $\alpha_1, \ldots, \alpha_n$ and rational integers $b_1, \ldots, b_n$.

1. The lower bound. Let $\alpha_1, \ldots, \alpha_n$ be nonzero algebraic numbers and $b_1, \ldots, b_n$ rational integers. For $i = 1, 2, \ldots, n$ let $\mathrm{Log}\alpha_i$ be a (henceforth fixed) determination of the logarithm of α_i. Setting

$$\Lambda = b_1 \mathrm{Log}\alpha_1 + \ldots + b_n \mathrm{Log}\alpha_n ,$$

we provide a lower bound for $|\Lambda|$, presuming of course that $\Lambda \neq 0$. For historical and bibliographical references concerning the significance of the result see [B1].

Denote by $h(\alpha)$ the absolute logarithmic height of the algebraic number α, see [W], and let $D, V_1, \ldots, V_n, B, B_n, E$ and W be positive real numbers respectively satisfying:

$$\mathbb{K}=\mathbb{Q}(\alpha_1,\alpha_2,\ldots,\alpha_n)\,,\qquad D\geq[\mathbb{K}:\mathbb{Q}]$$

$$V_i\geq\max\left(h(\alpha_i)\,,\ \frac{1}{D}|\mathrm{Log}\alpha_i|\,,\ \frac{1}{D}\right),\qquad i=1,\ \ldots,n\,;$$

$$B\geq\max_{j=1,\ \ldots,\ n-1}|b_j|\,,\qquad B_n\geq|b_n|\,;$$

$$e\leq E\leq\min\left(e^{DV_1}\,,\ eDn\left\{\sum_{j=1}^{n}|\mathrm{Log}\alpha_j|\,/\,V_j\right\}^{-1}\right)\,;$$

$$W\geq\mathrm{Log}\left(\frac{B_n}{V_1}+\frac{B}{V_n}+1\right)+\mathrm{Log}E\,.$$

Suppose that

$$V_1\leq V_2\leq\ldots\leq V_n\,,$$

and set: $X^+=\max(1,X)$ for all real numbers X.

THEOREM 1 *Given the strong independence condition*

$$[\mathbb{K}(\alpha_1^{\frac{1}{2}},\alpha_2^{\frac{1}{2}},\ldots,\alpha_n^{\frac{1}{2}}):\mathbb{K}]=2^n\,,$$

there is an effectively computable absolute constant $c_1>0$, *such that*

$$|\Lambda|>\exp\left\{-c_1^{n}n^{n}D^{n+2}(\mathrm{Log}EDV_{n-1}^{+})V_1V_2\ldots V_nW(\mathrm{Log}E)^{-(n+1)}\right\}$$

or $\Lambda=0$.

This bound is sharper than that in [W] (which, however, deals with the more general case of nonhomogeneous linear forms with algebraic coefficients) in that, there, W is in effect defined as

$$\mathrm{Log}(B_n+B)+\mathrm{Log}(EDV_n^{+})\,.$$

It is well known that, in the present 'rational case', the use of so-called Fel'dman polynomials in the auxiliary function permits the omission of the term $\mathrm{Log}DV_n^{+}$; again see [B1]. The useful improvement from B_n+B to $B_n/V_1+B/V_n+1$ is achieved by sharpening the upper bound for the Fel'dman polynomials; see below and compare [B2].

Comparison of our bound with previously published results in the rational case, see [D1],[L-vdP],[S], shows a much better dependence on D as well as the presence of the parameter E: which can be important in certain applications; see [S].

In explicit applications the strong independence assumption presents little difficulty; for example the arithmetical work necessary to close the gap between small values and our bound will reveal any linear relations on the $\log\alpha_i$ - suggesting a preliminary elimination decreasing n. In principle the 'final descent', see [W] pp.276 ff provides an algorithm whereby the α_i and b_i are rearranged to provide strong independence. Finally, in Theorem 2, the 'working version', we quote a result without the strong independence assumption.

Applying [W] it is safe to take $c_1^n = 2^{9n+26}n^4$; however it is clear that the method yields better numerical values. Note for example the allegations of [A-C-H-vdP], while [M] appears to claim that c_1^n may be replaced by $c_2 \cdot n^5 e^6 (2e^3)^n$ with $c_2 > 0$ a small absolute constant.

Quite similar bounds can be obtained in the p-adic case; see [vdP]. An update similar to the present note is in preparation.

2. We explain only the differences from the proof in [W]: The functions $\phi_{J,\tau}(z)$ appearing at [W], p.268 become $\phi^*_{J,\tau}(z)$, differing in that the quantity

$$\prod_{r=1}^{n-1} (\lambda_r + \lambda_n\beta_r)^{\tau_r},$$

occurring in the definition of $\Lambda_J(z;\tau)$ at p.266, is replaced by

$$\prod_{r=1}^{n-1} \Delta(b_n\lambda_r - b_r\lambda_n;\tau).$$

Recalling that

$$\Delta(z\,;\,\tau) := (z+1)\ldots(z+\tau)/\tau!\;\;;\;\;\Delta(z\,;\,0)=1,$$

it is not hard to see that for each pair J,τ and given s:

$$\phi_{J,\tau}(s)=0 \quad \text{for all} \quad |\tau| \le q^{-J}T \quad \text{if and only if}$$

$$\phi^{\wedge}_{J,\tau}(s)=0 \quad \text{for all} \quad |\tau| \le q^{-J}T\,.$$

But for integers $\lambda_1, \ldots, \lambda_n$ with $0 \le \lambda_r \le L_r$, $r=1,\ldots,n$, and $\tau_r > 0$:

$$|\Delta(b_n\lambda_r - b_r\lambda_n\,;\,\tau_r)| \le \left(2e\left(1+\frac{B_nL_r+BL_n+1}{\tau_r}\right)\right)^{\tau_r}.$$

Now notice the convexity inequality:

For positive integers $a,\tau_1,\ldots,\tau_{n-1}$ with $\tau_1+\ldots+\tau_{n-1}\le T$:

$$\left(1+\frac{a}{\tau_1}\right)^{\tau_1} \ldots\ldots \left(1+\frac{a}{\tau_{n-1}}\right)^{\tau_{n-1}} \le \left(1+\frac{(n-1)a}{T}\right)^{T}$$

It follows that

$$\prod_{r=1}^{n-1} |\Delta(b_n\lambda_r - b_r\lambda_n\,;\,\tau_r)| \le \left(2e\left(1+(n-1)\frac{B_nL+BL_n+1}{T}\right)\right)^{T},$$

with L denoting $L=\max L_r$.

For the rest the proof is as in [W].

3. A useful corollary. The following results sharpen that of [B2]. It will be convenient to set

$$X = c_1^n n^n D^{n+2}(\operatorname{Log} EDV_{n-1}^{+})\,V_1V_2\ldots V_n\,(\operatorname{Log} E)^{-(n+1)}$$

and then to introduce additional positive absolute constants c_3, c_4 and c_5 by writing:

$$Y = X\left(\text{Log } \frac{EDX}{V_n}\right) \le c_3^n n^n D^{n+2} \left(\text{Log } EDV_{n-1}^+\right)^2 V_1 V_2 \dots V_n (\text{Log } E)^{-(n+1)}$$

and

$$Z = c_4^n n!\, X(\text{Log } EDX) \le$$

$$\le c_5^n n^{2n} D^{n+2} (\text{Log } EDV_{n-1}^+)(\text{Log } EDV_n^+)\, V_1 V_2 \dots V_n (\text{Log } E)^{-(n+1)}$$

THEOREM 2 *Assuming the strong independence condition we have*

(i) *$\Lambda = 0$ or for all δ with $0 < \delta < \frac{1}{2}$:*

$$|\Lambda| > \left(\frac{\delta}{B_n}\right)^Y e^{-\delta B}$$

(ii) *Hence if $B_n = 1$ then for ε with $0 < \varepsilon < 1$:*

$$0 < |\Lambda| < e^{-\varepsilon B} \quad \textit{implies} \quad B < \left(\frac{2}{\varepsilon} \text{Log } \frac{2}{\varepsilon}\right) Y .$$

Moreover in general:

(iii) *Setting $B \ge B_n$, for ε with $0 < \varepsilon < 1$:*

$$0 < |\Lambda| < e^{-\varepsilon B} \quad \textit{implies} \quad B < \left(\frac{2}{\varepsilon} \text{Log } \frac{2}{\varepsilon}\right) Z .$$

To see (i) notice firstly that the function $x^a e^{-bx}$ takes its maximum at $x = a/b$. Thus it suffices to verify the easy consequences of Theorem 1: $\Lambda = 0$ or

$$|\Lambda| > (2B_n)^{-Y} e^{-B/2} \quad \text{if} \quad 0 < B \le 2Y$$

and

$$|\Lambda| > \exp -Y \text{ Log}\left(\frac{eBB_0}{Y}\right) \cdot \quad \text{if} \quad B \ge 2Y .$$

Then (ii) follows readily from (i) on setting $\delta = \varepsilon/2$. Finally, for (iii) we invoke the 'final descent' as detailed in [W] pp.276 ff.

In applications the user will often choose to take $E = e$. The quantity Y is probably most conveniently computed directly from its definition in terms of X,

REFERENCES

[A-C-H-vdP] M.K. Agrawal, J. Coates, D.C. Hunt and A.J. van der Poorten, Elliptic curves of conductor 11 *Math. Comp.* 35 (1980) 991-1002.

[B1] A. Baker, The theory of linear forms in logarithms, in [B-M] 1-27.

[B2] A. Baker, A sharpening of the bounds for linear forms in logarithms II, *Acta Arith.* 24 (1973) 33-36.

[B-M] A. Baker and D.W. Masser eds., *Transcendence theory: Advances and Applications* (Academic Press, 1977).

[L-vdP] J.H. Loxton and A.J. van der Poorten, Computing the effectively computable bound in Baker's inequality for linear forms in logarithms *Bull. Austral. Math. Soc.* 15 (1976) 33-57 and 17 (1977) 151-155.

[M] A.A. Matveev, A lower bound for linear forms in logarithms, in *Transcendental Number Theory and its Applications*, Proc. Conf. Moscow Univ., 2-4 Feb. 1983 (Izd. Mosk. Univ. 1983).

[S] T.N. Shorey, Perfect powers in values of certain polynomials at integer points *Math. Proc. Camb. Phil. Soc.* (to appear).

[vdP] A.J. van der Poorten, Linear forms in logarithms in the p-adic case, in [B-M], 29-57

[W] M. Waldschmidt, A lower bound for linear forms in logarithms *Acta Arith.* 37 (1980) 257-283.

Received January 26, 1987

J.H. Loxton
Macquarie University,
School of Mathematics and Physics,
N.S.W. 2109
AUSTRALIA.

M. Mignotte
Université Louis Pasteur
7 rue René Descartes
67084 Strasbourg
FRANCE.

A.J. van der Poorten
Macquarie University
School of Mathematics and Physics
N.S.W. 2109
AUSTRALIA.

M. Waldschmidt
IAS, Princeton NJ 08540
and
Institut Henri Poincaré
75231 Paris Cedex 05
FRANCE.

REMARK ABOUT THE SETS O(n)

In the Theory of Ordered Fields

JÁN MINÁČ

PRESENTED BY PAULO RIBENBOIM, F.R.S.C.

Abstract. In [2], L. Bröcker recursively defined an important sequence of sets O(n), $n > 0$. Bröcker showed that if T is a preordering on a formally real field F with $|\dot{F}/\dot{T}| = 2^n$, $\dot{F} = F \setminus \{0\}$, and if m is the number of orderings on F containing T then $m \in O(n)$. Conversely, he showed that if $m \in O(n)$ then there exists a pythagorean field F having 2^n square classes and m orderings. Bröcker also observed that if $2 \leq n$ and $m \in O(n)$ with $2^{n-2} < m \leq 2^{n-1}$ then $m = 2^{n-2} + 2^i$ for some i, $0 \leq i \leq n-2$. Subsequently, L. Berman [1] discovered the simplified formula $O(1) = \{1\}$ and $O(n) = 2\ O(n-1) \cup (O(n-1)+1)$, $n > 1$.

In the second chapter (and its appendix) of J. Merzel's paper [4] there are several beautiful results about O(n) which are due to B. Reznick. Among these is the following useful result [4, Prop. 2.8 and Prop. 2.A.4]:

THEOREM. *Let $n \leq 2^{a_1} + 2^{a_2} \cdots + 2^{a_s} = a$, where $0 \leq a_1 < \cdots < a_s$. Then $a \in O(n)$ iff $a_s + s \leq n$.*

In this note we give a different proof of this theorem and show some of its consequences.

PROOF OF THEOREM: We shall use induction on n. One can check easily that the theorem is true for $n \leq 8$.

Suppose that the assertion is true for n, $n \geq 8$.

Let $a = 2^{a_1} + \cdots + 2^{a_s} \in O(n)$, $0 \leq a_1 < \cdots < a_s$. By the induction hypothesis we have $n \leq a$ and $a_s + s \leq n$. Hence $2a = 2^{a_1+1} + \cdots + 2^{a_s+1}$, $a_s + 1 + s \leq n + 1$, $n + 1 \leq 2a$.

Furthermore $a + 1 = 2^{b_1} + \cdots + 2^{b_t}$ where $t \leq s + 1$ and $b_t \leq a_s + 1$. However $t = s + 1$ and $b_t = a_s + 1$ cannot happen simultaneously. Therefore $b_t + t \leq a_s + s + 1 \leq n + 1$.

This proves that if $a \in O(n+1)$ then $a_s + s \leq n+1$.

Suppose now that $n+1 \leq a = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_s}$, $0 \leq a_1 < \cdots < a_s$, $a_s + s \leq n+1$:

1) Let a be an odd number. Then

$$a - 1 = 2^{a_2} + \cdots + 2^{a_s}$$
$$a_s + (s-1) \leq n,$$

so by the induction hypothesis $a - 1 \in O(n)$ and hence $a \in O(n+1)$.

2) Let a be an even number such that $2n \leq a$. Then

$$a/2 = 2^{a_1 - 1} + \cdots + 2^{a_s - 1}$$
$$(a_s - 1) + s \leq n,$$

hence by the induction hypothesis $a/2 \in O(n)$ and from 1) we get $a \in O(n+1)$.

3) Finally suppose that $n+1 \leq a < 2n$. Then $n \leq a - 1 \leq 2(n-1)$. Put

$$a - 1 = 2^{c_1} + \cdots + 2^{c_k}, \quad 0 \leq c_1 < \cdots < c_k$$
$$n = 2^{b_1} + \cdots + 2^{b_t}, \quad 0 \leq b_1 < \cdots < b_t.$$

If $t \neq 1$, then

$$2(n-1) = 2 + 2^2 + \cdots + 2^{b_1} + 2^{b_2+1} + \cdots + 2^{b_t+1}.$$

Since $a - 1 \leq 2(n-1)$ we get for $1 \leq t$

$$c_k \leq b_t + 1, \quad k \leq b_t + 1.$$

Since $8 \leq n$, we have $3 \leq b_t$ and

$$c_k + k \leq 2b_t + 2 \leq 2^{b_t} \leq n,$$

hence $a-1 \in O(n)$ and $a \in O(n+1)$. Our proof is complete.

In the following we shall freely use the notions in [3].

Let F be a formally real field. $\dot{T}_F$ is the group of non-zero sums of squares of the field F; $\dot{F}$ is the multiplicative group of F. We shall say that F has type $(k, 2^n)$ if $[\dot{F} : \dot{T}_F] = 2^n$ and k is a number of orderings of the field F.

In [5, I] it was shown that if F has type $(j, 2^n)$, $3 \leq n$, and $j-1 \notin O(n-1)$ then there exists a valuation V on F fully compatible with all orderings of F such that $\dot{F} \neq \dot{F}^2 U_V$. ($U_V$ is the group of units of the valuation ring corresponding to the valuation V).

Following [4] we shall call an element $j \in O(n)$, $2 \leq n$ indecomposable iff $j-1 \notin O(n-1)$. From the theorem and remark above we get the following corollaries:

COROLLARY 1. *If $a = 2^{n-k} \in O(n)$, $1 \leq k < n$, then a is an indecomposable element of $O(n)$ iff $n > 2k$. If $a = 2^{n-k} + 2^{i_1} + \cdots + 2^{i_l} \in O(n)$, $0 \leq i_l < i_{l-1} < \cdots < i_1 < n-k$, then a is an indecomposable element of $O(n)$ iff $k - l - 1 < i_l$.*

COROLLARY 2. *All even elements a of the form $a = 2^{n-k} + 2^{i_1} + \cdots + 2^{i_{k-1}} \in O(n)$, $n > 2, 1 \leq i_{k-1} < \cdots < i_1 < n-k$, are indecomposable elements of the set $O(n)$.*

COROLLARY 3. *If $a \in O(n)$, $n > 2$, $2^{n-2} + 2 \leq a$, then a is an indecomposable element of $O(n)$.*

COROLLARY 4. *Let F be a field of the type $(a, 2^n)$ where: (i) $a = 2^{n-k} + 2^{i_1} + \cdots + 2^{i_l}$, $1 \leq l$, $0 \leq i_l < \cdots < i_1 < n-k$ ((ii) $a = 2^{n-k}$). If (i) $k - l - 1 < i_l$ ((ii) $n > 2k$), then there exists a non-trivial valuation V fully compatible with T_F such that $2^h \leq |\dot{F}/\dot{F}^2 U_V|$, where (i) $i_l - k + l + 1 = h$ ((ii) $n - 2k = h$).*

REMARK: Corollary 4 is equivalent to theorems 1 and 2 in [5, I]. Corollary 2 can also be obtained from the observation 2.A.2. in [4] or from [5, I or III]. In [5, III] the structure of space of orderings of a field F of type $(a, 2^n)$, with

$a = 2^{n-k} + 2^{i_1} + \cdots + 2^{i_{k-1}}$, $0 \leq i_{k-1} < \cdots < n-k$ is determined. As a consequence we get that if F has type $(a, 2^n)$ with $2^{n-2} < a < 2^{n-1}$ then the reduced stability index, $\mathrm{st}(F)$, is $n-2$. Since if $\mathrm{st}(F) = n-2$, then $a \geq 2^{n-2}$ and since a field F of type $(2^{n-2}, 2^n)$, $n \geq 4$, has $\mathrm{st}(F) = n-3$ [5, II] we get:

PROPOSITION. *Let F be a field of type $(a, 2^n)$, $2 \leq n$. Then $\mathrm{st}(F) = n-2$ iff $2^{n-2} < a < 2^{n-1}$.*

Finally, let us remark that more detailed results about relations between $\mathrm{st}(F)$ and the type of F can be found in [6]. They form an improvement of the results in [4, Chapter 5].

NOTE ADDED IN THE PROOF: The theorem above was also mentioned in the paper: M. Marshall, *A Reduced Theory of Quadratic Forms*, pp. 563–579, Conference on Quadratic Forms 1976, Queen's Papers in Pure and Applied Math., No. 46, 1977, (Footnote on the page 578).

I would like to thank the referee for his comments and improvement of the exposition.

ACKNOWLEDGEMENT: This paper has been written whilst pursuing a doctoral degree at Queen's University in Kingston. I am very grateful to Prof. Paulo Ribenboim, Prof. T. M. Viswanathan and Amar Sodhi for their encouragement, suggestions and much more.

REFERENCES

1. L. Berman, *The Kaplansky radical and values of binary quadratic forms over fields*, Thesis, University of California, Berkeley (1978).
2. L. Brōcker, *Über die Anzahl der Anordnungen eines kommutativen Körpers*, Archiv der Mathematik **29** (1977), 458–464.
3. T. Y. Lam, *Ordering, Valuations and Quadratic forms*, CBMS **52** (1983).
4. J. Merzel, *Quadratic forms over fields with finitely many orderings*, Contemporary Math **8** (1982), 185–229.
5. J. Mináč, *On fields for which the number of orderings is divisible by a high power of 2, I, II, III*, C. R. Math. Rep. Acad. Sci. Canada **VII(3)** (1985), 183–188;, **VII(4)**, 221–226;, **VII(5)**, 297–301.

6. J. Mináč, *About reduced stability indices of fields with finite number of orderings*, (in preparation).

Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley CA 94720.

Received February 10, 1987

Mailing Addresses

1. I. Assem — Faculté de Mathématiques, Université de Bielefeld, 4800 Bielefeld 1, Republique Fédérale, Allemande

2. E. Bujalance — Departamento de Matemáticas Fundamentales, Facultad de Ciencias, U.N.E.D., 28040 Madrid, Spain

3. A.Y. Cheer — Department of Mathematics, University of California, Davis, California 95616, U.S.A.

4. F. Cucker — Depto. de Algebra, Facultad de Ciencias, Univ. de Santander, Spain

5. J.J. Etayo — J.J. Etayo Gordejuela, Departamento de Geometría y Topología, Facultad de C. Matemáticas, Universidad Complutense, 28040 Madrid, Spain

6. J.M. Gamboa — Departamento de Algebra y Fundamentos, Facultad de C. Matemáticas, Universidad Complutense, 28040 Madrid, Spain

7. D.A. Goldston — Department of Mathematics and Computer Science, San Jose State University, San Jose, California 95192, U.S.A.

8. J.H. Loxton — Macquarie University, School of Mathematics and Physics, N.S.W. 2109, Australia

9. M. Mignotte — Université Louis Pasteur, 7 rue René Descartes, 67084 Strasbourg, France

10. J. Mináč — Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley, California 94720, U.S.A.

11. D.S. Mitrinović — Tehn. Fak, p.p. 177, Zagreb 41000, Yugoslavia

12. Y. Nakamura — Département de Mathématiques, Faculté des Sciences, Université Toyama, 930 Toyama, Gofuku 3190, Japon

13. J.E. Pécarić — Tehn. fak, p.p. 177, Zagreb 41000, Yugoslavia

14. B. Sarr — Ecole Polytechnique de Thies, Boîte Postale 10, Thies, Senegal

15. A. Skowroński — Institut de Mathématiques, Université Nicolas Copernic, 87-100, Toruń, Chopina 12/18, Pologne

16. A.J. van der Poorten — Macquarie University, School of Mathematics and Physics, N.S.W. 2109, Australia

17. V. Volenec — Tehn. fak, p.p. 177, Zagreb 41000, Yugoslavia

18. M. Waldschmidt — Institut Henri Poincaré, 75231 Paris Cedex 05, France