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

Vol. XII, No. 4 August 1990 août

CONTENTS

A NOTE ON THE STEINITZ CONSTANT OF THE EUCLIDEAN PLANE

Wojciech Banaszczyk

Presented by I. Halperin, F.R.S.C.

Abstract. Let R^2 be the two-dimensional euclidean space. The paper contains a relatively simple proof of the following result, announced in [1]: given a finite system of vectors $u_1,\ldots,u_n \in R^2$ with $\|u_1\|,\ldots,\|u_n\| \le 1$ and $u_1 + \ldots + u_n = 0$, one can find a permutation π of indices such that the norms of all partial sums $u_{\pi(1)} + \ldots + u_{\pi(k)}$ are not greater than $\sqrt{5}/2$.

Let R^2 be the two-dimensional euclidean space and B its closed unit ball. Given $p,q \ge 0$, we denote by $K(p,q)$ the infimum of all $\rho > 0$ satisfying the following condition:

for each $a \in pB$ and each system $u_1,\ldots,u_n \in B$ with $a + u_1 + \ldots + u_n \in qB$, there is a permutation π of indices such that $a + u_{\pi(1)} + \ldots + u_{\pi(k)} \in \rho B$ for each $k = 1,\ldots,n$.

The quantity $K(0,0)$ is sometimes called the Steinitz constant of R^2 (see the introductions to [1] and [6]).

The equalities $K(1,0) = K(1,1) = \sqrt{2}$ were proved independently by Gross [7], Bergström [4] and Damsteeg and Halperin [5]. The author proved in [1] that $K(0,0) = \sqrt{5}/2$ (see also [4]).

Let conv A denote the convex hull of a set $A \subset R^2$. The inequality $K(0,0) \le \sqrt{5}/2$ was obtained in [1] as a direct consequence of the following fact:

LEMMA A. *Let* $u_1,\dots,u_n \in B$, $n \geq 3$, *be a system such that*

$$(1) \qquad (B/2) \cap \operatorname{conv}\{-u_j + \sum_{i=1}^{n} u_i\}_{j=1}^{n} \neq \emptyset.$$

Then one can find an index $k = 1,\dots,n$ *such that*

$$(B/2) \cap \operatorname{conv}\{-u_j + \sum_{i\neq k} u_i\}_{j\neq k} \neq \emptyset,$$

$$\| \sum_{i\neq k} u_i \| \leq \sqrt{5}/2.$$

The proof of Lemma A was too involved to be included in [1]. Recently the author has found a simpler proof; presented below. The author is indebted to Prof. Israel Halperin for encouraging suggestions.

A few words on notations. The scalar product of vectors $u,v \in R^2$ is denoted by (u,v). By $[u,v]$ we denote the segment joining u and v. The triangle with vertices u,w,v is denoted by $T(u,w,v)$. We say that vectors $u_1,\dots,u_n \in R^2$ are *positively dependent* if they are linearly dependent with non-negative coefficients.

We shall need the following lemma:

LEMMA B. *Let* $w_1,w_2,w_3 \in B$ *be positively dependent vectors. denote*

$$v_1 = w_2 + w_3, \qquad T_1 = T(w_1,v_2,v_3),$$

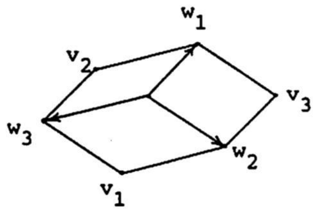
$$v_2 = w_1 + w_3, \qquad T_2 = T(v_1,w_2,v_3),$$

$$v_3 = w_1 + w_2, \qquad T_3 = T(v_1,v_2,w_3).$$

Let $c \in R^2$ *be a point such that* $(c + B/2) \cap T(w_1,w_2,w_3) \neq \emptyset$. *Then there is an index* $i = 1,2,3$ *such that* $(c + B/2) \cap T_i \neq \emptyset$

and $\|w_i - c\| \le \sqrt{5}/2$.

P r o o f. Without loss of generality we may assume that w_1, w_2, w_3 are linearly dependent with strictly positive coefficients; then the points $w_1, v_3, w_2, v_1, w_3, v_2$ are consecutive vertices of a convex hexagon, as shown in the following figure:



Denote this hexagon by H and adopt $D = c + B/2$. Suppose first that D intersects one of the sides of H; we may assume that D intersects $[w_1, v_3]$. If $v_3 \notin D$, then $\|w_1 - c\| \le \sqrt{5}/2$ and we may take $i = 1$. So, let $v_3 \in D$. Since D intersects $T(w_1, w_2, w_3)$, it follows that D intersects $[w_1, w_2]$. But $\|w_1 - w_2\| < \|w_1\| + \|w_2\| \le 2$, which implies that $\|w_j - c\| < \sqrt{5}/2$ for j equal to 1 or 2 . Then we may take $i = j$ because the condition $v_3 \in D$ means that D intersects both T_1 and T_2.

Let us now suppose that D does not intersect any side of H. Since D intersects the triangle $T(w_1, w_2, w_3)$ contained in H, it follows that D is contained in the interior of H. Let S be the triangle $T(v_1, v_2, v_3)$. We shall consider four cases.

1° D intersects all three sides of S. It is not hard to see that $H \subset \bigcup_{j=1}^{3} (w_j + B)$. For instance, $T(0, w_1, v_3) \subset w_1 + B$ etc. So, there is an index $j = 1,2,3$ with $\|w_j - c\| \le 1$ and we may take $i = j$.

2° D intersects precisely two sides of S. Without loss of generality we may assume that D intersects $[v_1, v_2]$ and $[v_1, v_3]$

and is disjoint from $[v_2,v_3]$. Since the segments $[v_2,v_3]$ and $[w_2,w_3]$ are parallel and their distance is less or equal to $\|v_2 - w_3\| = \|w_1\| \le 1$, it follows that D intersects $[w_2,w_3]$. But $\|w_2 - w_3\| < \|w_2\| + \|w_3\| \le 2$, whence $\|w_j - c\| < \sqrt{5}/2$ for j equal to 2 or 3, and we may take $i = j$.

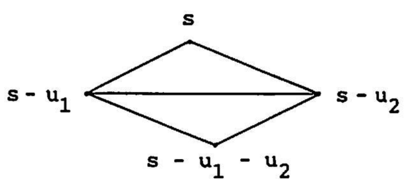
3° D intersects precisely one side of S. We may assume that D intersects $[v_2,v_3]$ and is disjoint from $[v_1,v_2]$ and $[v_1,v_3]$. A direct calculation which we leave to the reader shows that, in this case, we have $\|w_1 - c\| < 1.11\ldots < \sqrt{5}/2$, so that we may take $i = 1$.

4° D does not intersect any side of S. This is impossible. Indeed, it is easy to verify that if the interior of a triangle T contains a circle with radius r, then the area of T is strictly greater that $3^{3/2}\cdot r^2$. On the other hand, it is not hard to see that the area of S is less or equal to $4^{-1}\cdot 3^{3/2}$. The area of each of the triangles T_1,T_2 and T_3 is less or equal to 2^{-1}.

P r o o f of Lemma A. Denote $s = \sum_{i=1}^{n} u_i$. It follows from (1) that there is a pair i,j of distinct indices such that $(B/2) \cap T(s,s - u_i,s - u_j) \neq \emptyset$. We may assume that $i = 1$ and $j = 2$; thus

$$(B/2) \cap T(s,s - u_1,s - u_2) \neq \emptyset. \tag{2}$$

We shall consider several cases. If $s - u_1 - u_2 \in B/2$, then (2) implies that $(B/2) \cap [s - u_1,s - u_2] \neq \emptyset$:



Since $\|(s - u_1) - (s - u_2)\| = \|u_1 - u_2\| \le \|u_1\| + \|u_2\| \le 2$, we have $\|s - u_1\| \le \sqrt{5}/2$ or $\|s - u_2\| \le \sqrt{5}/2$ and we take $k = 1$ or $k= 2$, accordingly. So, suppose that $s - u_1 - u_2 \notin B/2$. If $(B/2) \cap [s - u_1, s - u_1 - u_2] \neq \emptyset$, then $\|s - u_1\| \le \sqrt{5}/2$ and we take $k = 1$. Similarly, if $(B/2) \cap [s - u_2, s - u_1 - u_2] \neq \emptyset$, we take $k = 2$. Therefore we may assume that

(3) $$(B/2) \cap \bigcup_{i=1}^{2} [s - u_i, s - u_1 - u_2] = \emptyset.$$

It follows easily from (2) and (3) that $(B/2) \cap \bigcup_{i=1}^{2} [s, s - u_i] \neq \emptyset$; without loss of generality we may assume that

(4) $$(B/2) \cap [s, s - u_1] \neq \emptyset.$$

Suppose that $u_1, \ldots, u_n$ are positively dependent. Then there is a pair of distinct indices $i, j \neq 1$ such that the vectors u_1, u_i, u_j are positively dependent, too. By (4), we have $(-s + B/2) \cap T(-u_1, -u_i, -u_j) \neq \emptyset$. The existence of an index k with the desired properties follows now from Lemma B.

Finally, suppose that $u_1, \ldots, u_n$ are not positively dependent. Then there is a vector $e \in R^2$ such that

(5) $$(u_i, e) > 0 \quad \text{for} \quad i = 1, \ldots, n.$$

It is not hard to see that there is an index $j \neq 1$ such that $s \in \{\alpha u_1 + \beta u_j : \alpha, \beta \ge 0\}$. We may assume that $j = 2$. Thus

(6) $$s = \alpha u_1 + \beta u_2$$

for certain $\alpha, \beta \ge 0$. In view of (3), (4) and the convexity of $B/2$, we must have $\alpha, \beta < 1$. Then, by (5) and (6),

$$(u_1, e) + (u_2, e) \le \sum_{i=1}^{n} (u_i, e) = (s, e)$$

$$= \alpha(u_1,e) + \beta(u_2,e) < (u_1,e) + (u_2,e)$$

which is impossible. This completes the proof.

REMARK. An easy modification of the above argument allows one to prove that

$$K(p,q) = [1 + \max(p^2,q^2,1/4)]^{1/2}$$

for each pair $p,q \geq 0$.

References

[1] W. Banaszczyk, **The Steinitz constant of the plane**, J. reine. angew. Math. 373 (1987), 218-220.

[2] W. Banaszczyk, **The Steinitz theorem on** rearrangement **of series for nuclear spaces**, to appear in J. reine angew. Math.

[3] F.A. Behrend, **The Steinitz-Gross theorem on sums of vectors**, Canad. J. Math. 6 (1954), 108-124.

[4] V. Berström, **Zwei Sätze über ebene Vektorpolygone**, Abh.Math. Sem. Univ. Hamburg 8 (1931), 206-214.

[5] I. Damsteeg and I. Halperin, **The Steinitz-Gross theorem on** sums of vectors, Trans. Roy. Soc. Canada, Ser. III, 44 (1950), 31-35.

[6] V.S. Grinberg and S.V. Sevast´yanov, **Value of the Steinitz constant**, Funktional. Anal. i Prilozh. 14 (1980), 56-57 (in Russian), translated as Functional Anal. Appl. 14 (1980), 125--126.

[7] W. Gross, **Bedingt konvergente Reihen**, Monatsh. Math. Phys. 28 (1917), 221-237.

Institute of Mathematics
University of Łódź
ul. S. Banacha 22
90-238 Łódź, Poland

Received May 14, 1990

A GENERALIZATION OF TERJANIAN'S THEOREM

Yves HELLEGOUARCH

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

In this paper we relate Jacobi's quadratic symbol in $\mathbb{Q}$ to Hecke's quadratic symbol for certain families of numbers in number fields of odd degree (theorem 1). A by-product of this elaboration is a generalization of Terjanian's theorem to odd degree number fields (theorem 2).

1. PRELIMINARIES

Let $\overline{\mathbb{Z}}$ be the ring of algebraic integers and let α and β be given in $\overline{\mathbb{Z}}$. For any polynomial $P(X) \in \overline{\mathbb{Z}}[X]$ we write :

$$(1) \qquad (P)'_{\alpha,\beta} = \begin{cases} \dfrac{P(\alpha) - P(\beta)}{\alpha - \beta} & \text{if } \alpha \neq \beta \\ P'(\alpha) & \text{if } \alpha = \beta \end{cases}$$

Then we have the following elementary facts.

LEMMA 1.-

i) $(P')_{\alpha,\beta} \in \overline{\mathbb{Z}}$

ii) For any $P(X)$ and $Q(X) \in \overline{\mathbb{Z}}[X]$ we have :

$$(2) \qquad (PQ)'_{\alpha,\beta} = (P)'_{\alpha,\beta}\, Q(\beta) + P(\alpha)\, (Q)'_{\alpha,\beta} .$$

DEFINITION 1.- α and $\beta \in \overline{\mathbb{Z}}$ are said to be relatively prime if their common divisors in $\overline{\mathbb{Z}}$ are units (of $\overline{\mathbb{Z}}$).

It is well known that if α and β are relatively prime and if α divides $\beta\gamma$ in $\overline{\mathbb{Z}}$, then α divides γ in $\overline{\mathbb{Z}}$.

LEMMA 2.- If $P(X)$ and $Q(X)$ are in $\overline{\mathbb{Z}}[X]$ then:

$$(3) \qquad (P \circ Q)'_{\alpha,\beta} \equiv 0 \qquad \operatorname{mod}(Q)'_{\alpha,\beta}$$

COROLLARY 1.- If α and β are relatively prime in $\overline{\mathbb{Z}}$ and if $(m,n) = d \in \mathbb{N}$, then $(X^d)'_{\alpha,\beta}$ is a G.C.D. of $(X^m)'_{\alpha,\beta}$ and $(X^n)'_{\alpha,\beta}$ in $\overline{\mathbb{Z}}$.

<u>Outlined proof</u>:

If $m = nq + r$, put $P = X^{nq} = X^q \circ X^n$ and $Q = X^r$ in (2) and remark by (3) that:

$$\begin{cases} (X^m)'_{\alpha,\beta} \equiv \alpha^{nq} (X)'_{\alpha,\beta} \\ \\ (X^m)'_{\alpha,\beta} \equiv \beta^{nq} (X)'_{\alpha,\beta} \end{cases} \qquad \operatorname{mod} (X^n)'_{\alpha,\beta}$$

Then use Euclid's algorithm in $\mathbb{N}$. □

COROLLARY 2.- If α and β are relatively prime, the only common divisors of α-β and $(X^n)'_{\alpha,\beta}$ are divisors of an indeterminate power of n.

Remark: All those properties are related to general properties of σ-derivations, see [1].

From now on we suppose that $\alpha = a^2$, $\beta = b^2$ with a and b relatively prime and lying in a number field K, and we begin by mentioning some elementary facts.

LEMMA 3.-

i) If $m = nq+r$, we have:

$$(4) \qquad (X^m)'_{a^2,b^2} \equiv a^{2nq} (X^r)'_{a^2,b^2} \qquad \operatorname{mod}(X^n)'_{a^2,b^2}$$

ii) If $m+r = nq$, we have:

$$(5) \qquad b^{2r} (X^m)'_{a^2,b^2} \equiv - a^{2m} (X^r)'_{a^2,b^2} \qquad \operatorname{mod}(X^n)'_{a^2,b^2}$$

DEFINITION 2.- We say that $x \in \overline{\mathbb{Z}}$ is odd if x and 2 are relatively prime. We say that $x \in K \cap \overline{\mathbb{Z}}$ is <u>primary in</u> K if x is odd and if x is congruent to a square (of K) modulo 4. Finally we will write for $m \in \mathbb{Z}$:

$$[m] = \mathrm{sgn}(m)\left(X^{|m|}\right)'_{a^2,b^2}$$

LEMMA 4.-

i) If $m > 0$ in $\mathbb{Z}$, $[m] \gg 0$ (i.e. every conjugate of $[m]$ is positive).
If $m < 0$ in $\mathbb{Z}$, $[m] \ll 0$ (i.e. every conjugate of $[m]$ is negative).

ii) If a and b are odd and if $a \equiv b \pmod 2$ then $[m]$ is primary in K when m is primary in $\mathbb{Z}$ (i.e. $m \equiv 1 \bmod 4$).

LEMMA 5.- If n is primary in $\mathbb{Z}$ and if the absolute degree of K is odd, we have :

$$\left(\frac{-1}{n}\right)_J = \left(\frac{-1}{[n]}\right)_H \tag{6}$$

where the index J (resp. H) indicates that we are considering the Jacobi (resp. Hecke) symbol in $\mathbb{Q}$ (resp. K), see [2] p. 136 and 221.

2. KEY RESULT

This result follows from the following particular case of Hecke's quadratic reciprocity law, see [2] p. 221.

If the number of real embeddings of a number field is odd and if x and y are totally positive or negative relatively prime integers in K, one of which is <u>primary</u>, we have :

$$\left(\frac{x}{y}\right)_H \left(\frac{y}{x}\right)_H = (-1)^{\frac{\mathrm{sgn}(x)-1}{2}\,\frac{\mathrm{sgn}(y)-1}{2}} \tag{7}$$

THEOREM 1.- If the degree of the number field K is odd and if a and b are relatively prime odd integers of K congruent modulo 2, then for any relatively prime primary integers m and n in $\mathbb{Z}$, we have :

$$\left(\frac{m}{n}\right)_J = \left(\frac{[m]}{[n]}\right)_H \tag{8}$$

Proof :

1) We remark that we can apply (7) to the numbers [m] and [n] so that (8) is in fact symmetrical in m and n. This follows from corollary 1 and lemma 4.

2) Then we make an induction on $\nu = \sup(|m|,|n|)$ by supposing that (8) is true when $\nu < \mu$. Suppose now that $\sup(|m|,|n|) = |m| = \mu$ and divide $|m|$ by $|n|$.

2.1) If the remainder r is odd, we write

$$(9) \qquad |m| = |n|q+r \qquad 0<r<|n|$$

Then (9) and relation (4) of lemma 3 give :

$$\left(\frac{|m|}{n}\right)_J = \left(\frac{r}{n}\right)_J \quad , \quad \left(\frac{\left(X^{|m|}\right)'_{a^2,b^2}}{\left(X^{|n|}\right)'_{a^2,b^2}}\right)_H = \left(\frac{\left(X^{r}\right)'_{a^2,b^2}}{\left(X^{|n|}\right)'_{a^2,b^2}}\right)_H$$

We now put $|m| = \varepsilon m$ and $r = \varepsilon' r'$ with $\varepsilon, \varepsilon' = \pm 1$ and a primary r', then we get

$$\left(\frac{\varepsilon}{n}\right)_J\left(\frac{m}{n}\right)_J = \left(\frac{\varepsilon'}{n}\right)_J\left(\frac{r'}{n}\right)_J \quad , \quad \left(\frac{\varepsilon}{[n]}\right)_H\left(\frac{[m]}{[n]}\right)_H = \left(\frac{\varepsilon'}{[n]}\right)_H\left(\frac{[r']}{[n]}\right)_H$$

Then lemma 5 and the induction hypothesis give us (8).

2.2) If the remainder r is even, we write :

$$(10) \qquad |m|+r = |n|q \qquad 0<r<|n| \qquad r \text{ odd.}$$

Then (10) and relation (5) of lemma 3 give :

$$\left(\frac{|m|}{n}\right)_J = \left(\frac{-r}{n}\right)_J \quad , \quad \left(\frac{\left(X^{|m|}\right)'_{a^2,b^2}}{\left(X^{|n|}\right)'_{a^2,b^2}}\right)_H = \left(\frac{-\left(X^{r}\right)'_{a^2,b^2}}{\left(X^{|n|}\right)'_{a^2,b^2}}\right)_H$$

and, with the above notations, we get :

$$\left(\frac{\varepsilon}{n}\right)_J\left(\frac{m}{n}\right)_J = \left(\frac{-\varepsilon'}{n}\right)_J\left(\frac{r'}{n}\right)_J \quad , \quad \left(\frac{\varepsilon}{[n]}\right)_H\left(\frac{[m]}{[n]}\right)_H = \left(\frac{-\varepsilon'}{[n]}\right)_H\left(\frac{[r']}{[n]}\right)_H$$

Then lemma 5 and the induction hypothesis give us (8). □

3. CONSEQUENCES

COROLLARY 3.- Let m be an odd non square integer and let a and b be two integers in $\overline{\mathbb{Z}}$, relatively prime, odd and congruent modulo 2.

If K is a number field containing a and b and of odd absolute degree, then the ideal generated by $\dfrac{a^{2m}-b^{2m}}{a^2-b^2}$ in K cannot be a square.

Proof :

As m is not a square, there is a rational primary prime ℓ such that :

$$\left(\frac{(-1)^{\frac{m-1}{2}}m}{\ell}\right)_J = -1$$

Applying theorem 1 to $m^* = (-1)^{\frac{m-1}{2}}m$ and ℓ we get :

$$\left(\frac{[\ell]}{[m^*]}\right)_H = \left(\frac{\ell}{m^*}\right)_J = -1$$

and this implies that the ideal generated by $[m^*]$ cannot be a square. □

THEOREM 2.- Let p be an odd prime and let a and b be two integers in $\overline{\mathbb{Z}}$ which are supposed relatively prime, odd and congruent modulo 2.

If the degree of a number field K containing a and b is odd, and if $a^{2p}-b^{2p}$ generates the square of an ideal in K, then one of the prime factors of this ideal divides p.

Proof :

Since :

$$a^{2p}-b^{2p} = (a^2-b^2)\,(X^p)'_{a^2,b^2}$$

generates the square of an ideal in K, corollary 3 implies that the two factors on the right have a common (ideal) divisor. Corollary 2 gives the conclusion. □

COROLLARY 4.- Let K be a number field of odd degree and class number, and let $\mathcal{O}_K$ be its maximal order. Then if the odd prime p is greater than a certain constant $C(K)$ the relation :

$$x^{2p} - y^{2p} = \varepsilon\, 2^{2\gamma} z^2$$

with $\gamma \in \mathbb{N}$, $\gamma \geq 1$, $(x,y,z) \in \mathcal{O}_K^3$ and x or y prime to 2, $\varepsilon \in \mathcal{O}^*_K$, implies that z and p have a common (ideal) divisor.

Outlined Proof :

Apply theorem 2 to the Hilbert class field H of K and take p sufficiently big not to divide the cardinal of the group of units of $\mathcal{O}_H/4\mathcal{O}_H$. In order to do this, note that $[H : K]$ is odd and so is the degree of H over $\mathbb{Q}$, and use the Principal Ideal Theorem to replace x and y by relatively prime integers in H. □

The next corollary enables one to get rid of the condition "x or y is prime to 2".

COROLLARY 5.- Let K be a number field of odd degree and class number, and let $\gamma \in \mathbb{N}$, $\gamma \geq 1$. Then if the odd prime p is greater than a certain constant $C(K, \gamma)$ the relation :

$$x^{2p} - y^{2p} = \varepsilon\, 2^{2\gamma} z^{2p}$$

with $(x,y,z) \in \mathcal{O}_K^3$ and $\varepsilon \in \mathcal{O}_K^*$ implies that z and p have a common (ideal) divisor.

REFERENCES :

[1] Y. HELLEGOUARCH.- *"Calcul différentiel galoisien"*, Journées Arithmétiques de Marseille, submitted to Astérisque.

[2] E. HECKE.- *"Lectures on the theory of algebraic numbers"*, Springer 1981.

[3] P. RIBENBOIM.- *"13 lectures on Fermat's last theorem"*, Springer 1979.

Université de Caen
F-1400 Caen, France

Received October 6, 1989
in revised form May 10, 1990

EQUATIONS FOR FAMILIES OF RELATIONS CAN ALSO BE SOLVED

J. Mala and Á. Száz

Presented by G.F.D. Duff, F.R.S.C.

ABSTRACT

To justify the title, we show that if $\mathcal{R}$ is a family of relations on a set X, then there exists a natural enlargement $\hat{\mathcal{R}}$ of $\mathcal{R}$ such that $\hat{\mathcal{R}}^{-1} = \hat{\mathcal{R}}$ if and only if $\hat{\mathcal{R}} = \{S\}^{\wedge}$ for some symmetric relation S on X.

Since Weil's uniformities and their immediate generalizations [2] are families of relations, it is of some importance to solve equations not only for functions or relations, but also for families of those.

The possibility of such kinds of investigations can be most easily demonstrated by proving the following theorem whose subject matter is very similar to that of the theorems of Kenyon [1].

<u>THEOREM</u>. <u>If</u> $\mathcal{R}$ <u>is a family of relations</u> $R \subset X \times X$ <u>and</u>

$$\hat{\mathcal{R}} = \{ S \subset X \times X : \forall x \in X : \exists R \in \mathcal{R} : R(x) \subset S(x) \},$$

<u>then the following assertions are equivalent</u>:

(i) $\hat{\mathcal{R}}^{-1} = \{ S^{-1} : S \in \hat{\mathcal{R}} \} = \hat{\mathcal{R}}$;

(ii) $\bigcap \mathcal{R}$ <u>is symmetric and</u> $\bigcap \mathcal{R} \in \hat{\mathcal{R}}$;

(iii) <u>there exists a symmetric relation</u> $S \subset X \times X$ <u>such that</u> $\hat{\mathcal{R}} = \{S\}^{\wedge}$.

<u>PROOF</u>. If (i) holds, then because of $\mathcal{R} \subset \hat{\mathcal{R}}$, we also have

$$\mathcal{R}^{-1} \subset \hat{\mathcal{R}} .$$

Hence, by noticing that

$$\bigcap \hat{\mathcal{R}} = \bigcap \mathcal{R} \qquad \text{and} \qquad \bigcap \mathcal{R}^{-1} = (\bigcap \mathcal{R})^{-1} ,$$

we can at once derive that

$$\bigcap \mathcal{R} \subset (\bigcap \mathcal{R})^{-1} .$$

Consequently, the relation

$$S = \bigcap \mathcal{R}$$

is symmetric.

To prove that now $S \in \hat{\mathcal{R}}$ is also true, note that if $V_x \subset X \times X$ for all $x \in X$ such that

$$V_x(z) = S(x) \quad \text{if} \quad z=x \quad \text{and} \quad V_x(z) = X \quad \text{if} \quad z \in X \setminus \{x\} ,$$

then the family

$$\mathcal{V} = \{V_x\}_{x \in X}$$

has the property $S \in \hat{\mathcal{V}}$.

Moreover, since

$$V_x^{-1}(w) = X \setminus \{x\} \text{ if } w \in X \setminus S(x) \quad \text{and} \quad V_x^{-1}(w) = X \text{ if } w \in S(x) ,$$

and S is symmetric, it is clear that

$$\mathcal{V}^{-1} \subset \hat{\mathcal{R}}$$

is also true.

Namely, if $x \in X$ and $w \in X \setminus S(x)$, then because of the symmetry of S, we also have $w \notin S^{-1}(x)$, i.e., $x \notin S(w)$. Hence, by the definition of S, it is clear that there exists an $R \in \mathcal{R}$ such that $x \notin R(w)$, i.e., $R(w) \subset X \setminus \{x\}$. Consequently, $V_x^{-1} \in \hat{\mathcal{R}}$.

Now, by combining the above inclusion with (i), we can also state that

$$\mathcal{V}^{-1} \subset \hat{\mathcal{R}}^{-1},$$

i.e., $\mathcal{V} \subset \hat{\mathcal{R}}$. Hence, by noticing that

$$\hat{\hat{\mathcal{R}}} = \hat{\mathcal{R}}$$

we can at once derive that $\hat{\mathcal{V}} \subset \hat{\mathcal{R}}$.

This latter inclusion, together with $S \in \hat{\mathcal{V}}$, shows that $S \in \hat{\mathcal{R}}$. Consequently, (ii) also holds.

Finally, to complete the proof, we note that if (ii) holds, then the relation $S = \bigcap \mathcal{R}$ has the properties stated in (iii).

On the other hand, if (iii) holds, then because of

$$\hat{\mathcal{R}}^{-1} = (\{S\}^{\wedge})^{-1} = \{S^{-1}\}^{\wedge} = \{S\}^{\wedge} = \hat{\mathcal{R}},$$

(i) also holds.

<u>REMARK</u>. Concerning the equations

$$(\mathcal{R}^{-1})^{\wedge} = \hat{\mathcal{R}} \qquad \text{and} \qquad (\mathcal{R}^{-1})^{\wedge} = \hat{\mathcal{R}}^{-1}$$

we could not prove some similar results.

The authors are indebted to Gy. Maksa for his valuable suggestions.

REFERENCES

[1] H. Kenyon, Two theorems about relations, Trans. Amer. Math. Soc. 107 (1963), 1-9.

[2] Á. Száz, Basic tools and mild continuities in relator spaces, Acta Math. Hungar. 50 (1987), 177-201.

József Mala
Department of Mathematics
Teachers' Training College
H-4401 Nyiregyháza, Hungary

Árpád Száz
Institute of Mathematics
Lajos Kossuth University
H-4010 Debrecen, Hungary

Received June 20, 1990

TORSION-FREE NORMAL COMPLEMENTS IN UNIT GROUPS OF INTEGRAL GROUP RINGS

M.M. PARMENTER *

Presented by N.D. Gupta, F.R.S.C.

Let $U(ZG)$ denote the group of units of an integral group ring. In [4], Ritter and Sehgal showed that for many finite nilpotent groups, the Bass cyclic and bicyclic units generate a subgroup of finite index in $U(ZG)$. This result does not hold for all finite nilpotent groups - the problem lies with the Sylow 2 - subgroup of G. Specifically, it is shown in [4] that the Bass cyclic and bicyclic units generate a subgroup of infinite index in $U(ZP)$ for the following group P of order 16:

$$P = \langle a,b \mid a^4 = b^4 = 1,\ [b,a] = a^2\rangle$$

In [1], a further investigation of $U(ZP)$ was carried out, and it was shown that if W is the subgroup of $U(ZP)$ consisting of all units of the form $1 + (1 - a^2)(1 + b^2)\ (\alpha_1 + \alpha_2 a + \alpha_3 b + \alpha_4 ab)$, α_i in Z, then W is a torsion-free normal complement for P in $U(ZP)$, and that a necessary and sufficient condition for such an element to be a unit is that $(1 + 4\alpha_1)^2 + (4\alpha_2)^2 - (4\alpha_3)^2 - (4\alpha_4)^2 = 1$. Using this, the author constructed a finite set of generators for a subgroup of finite index in W (announced at the Canadian Mathematical Society Meetings in June, 1989).

Subsequently, Jespers and Leal [2] investigated the structure of $U(ZG)$ for a wide class of groups using a different approach. When applied to the particular group P mentioned above, their work yields the surprising result that the

* This research was supported in part by the Natural Sciences and Engineering Research Council, Grant No. A8775.

subgroup of finite index we had described is in fact equal to W and that W is isomorphic to a group of 2×2 integer matrices which is free of rank 9. The same approach is also applied to show that the dihedral group of order 8 has a torsion-free normal complement isomorphic to a group of 2×2 integer matrices which is free of rank 3.

It may not be apparent, however, to the reader of [2] that both of the particular results mentioned above can also be established by simple, direct arguments following from [1]. In view of the significance of the group P in work on units, we think that it may be useful to briefly indicate the steps of these elementary arguments.

For general information on terminology and results concerning group rings, the reader is referred to [5].

1. Dihedral Group

Before considering the group P, we must first describe the units of ZD_4, where D_4 is the dihedral group of order 8, i.e.

$$D_4 = \langle a,b \mid a^4 = b^2 = 1,\ [b,a] = a^2\rangle$$

We remark that the units of ZD_4 have also been carefully studied by Polcino Milies [3], but a different formulation is needed for our purposes.

It was shown in [1] that, up to multiplication by $\pm D_4$, all units in ZD_4 are of the form $1 + (1 - a^2)(\alpha_1 + \alpha_2 a + \alpha_3 b + \alpha_4 ab)$, α_i in Z, and that a necessary and sufficient condition for such an element to be a unit is that

$$(*)\qquad (1 + 2\alpha_1)^2 + (2\alpha_2)^2 - (2\alpha_3)^2 - (2\alpha_4)^2 = 1\ .$$

Let U_2 be the subgroup of $U(ZD_4)$ consisting of all such units

Consider the set of 2×2 matrices

$$R = \begin{bmatrix} 1 + 2Z & 2Z \\ 2Z & 1 + 2Z \end{bmatrix}.$$

If we define a map $f\colon U_2 \to R$ by

$$f(1 + (1 - a^2)(\alpha_1 + \alpha_2 a + \alpha_3 b + \alpha_4 ab)) = \begin{bmatrix} 1 + 2(\alpha_1 + \alpha_4) & 2(\alpha_3 + \alpha_2) \\ 2(\alpha_3 - \alpha_2) & 1 + 2(\alpha_1 - \alpha_4) \end{bmatrix}$$

then, using property (*), it is easily checked by direct calculation that f is an injective homomorphism. Moreover, the image of f is precisely the set of all

determinant 1 matrices $\begin{bmatrix} 1 + 2a & 2b \\ 2c & 1 + 2d \end{bmatrix}$ where $b + c$ is even.

The above description of these units now allows us to determine the structure of U_2. Since this is done in exactly the same way as in [2], we will just sketch the procedure. First note that the subgroup V of U_2 consisting of those elements for which $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$ is even is a torsion-free normal complement for D_4 in $U(ZD_4)$, and that $\alpha(V)$ is a subgroup of index 2 in a matrix group which is known to be free of rank 2. Hence $\alpha(V)$ is free of rank 3, and a set of generators can be calculated. One such set turns out to be exactly the images of the bicyclic units in V.

In summary, we have

<u>Theorem 1</u>:

In $U(ZD_4)$, D_4 has a torsion-free normal complement which is a free group of rank 3 generated by bicyclic units.

2. Group of Order 16

Now we are ready to consider the interesting group P defined earlier, namely

$$P = \langle a,b \mid a^4 = b^4 = 1,\ [b,a] = a^2 \rangle$$

It was mentioned before that, up to multiplication by $\pm P$, all units in $U(ZP)$ are of the form $1 + (1 - a^2)(1 + b^2)(\alpha_1 + \alpha_2 a + \alpha_3 b + \alpha_4 ab)$, α_i in Z, and that a necessary and sufficient condition for such an element to be a unit is that

$$(**) \qquad (1 + 4\alpha_1)^2 + (4\alpha_2)^2 - (4\alpha_3)^2 - (4\alpha_4)^2 = 1.$$

Let W be the subgroup of $U(ZP)$ consisting of all such units.

Define $g\colon ZP \to ZD_4$ to be the Z - linear extension of the natural epimorphism from P to D_4 obtained by setting $b^2 = 1$. Then $g(W)$ is contained in the set of units of V of the form $1 + 2(1 - a^2)(\alpha_1 + \alpha_2 a + \alpha_3 b + \alpha_4 ab)$.

Surprisingly, perhaps, it is also true that any such unit in V is, in fact, in $g(W)$. To see this, note that if 2 is replaced by $1 + b^2$ in such a unit, we obtain an element of ZP, and this element satisfies equation (**) because the original unit satisfied (*) in ZD_4.

In addition, it is clear that g is injective when applied to W. It follows that W is isomorphic to the group of units in V of the form $1 + 2(1 - a^2)(\alpha_1 + \alpha_2 a + \alpha_3 b + \alpha_4 ab)$. Using the fact proved earlier that the bicyclic units generate V, we conclude that $g(W)$ is of index 4 in V. It follows that W is a free group of rank 9, and a set of generators can be constructed from those of V (also a nice matrix interpretation of the group W is obtained since W is isomorphic to $f(g(W))$.

In summary, we have

<u>Theorem 2</u>:

In $U(ZP)$, P has a torsion-free normal complement which is a free group of rank 9.

The following set of generators for W is obtained by slightly modifying the above procedure:

$$v_1 = 1 + (1 - a^2)\ (1 + b^2)\ (a + b)$$
$$v_2 = 1 + (1 - a^2)\ (1 + b^2)\ (-a + ab)$$
$$v_3 = 1 + (1 - a^2)\ (1 + b^2)\ (13a + 5b - 12ab)$$
$$v_4 = 1 + (1 - a^2)\ (1 + b^2)\ (17a + 15b - 8ab)$$
$$v_5 = 1 + (1 - a^2)\ (1 + b^2)\ (-125a - 44b + 117ab)$$
$$v_6 = 1 + (1 - a^2)\ (1 + b^2)\ (149a + 51b - 140ab)$$
$$v_7 = 1 + (1 - a^2)\ (1 + b^2)\ (-2 + a - 2ab)$$
$$v_8 = 1 + (1 - a^2)\ (1 + b^2)\ (-8 - 19a - 14b + 15ab)$$
$$v_9 = 1 + (1 - a^2)\ (1 + b^2)\ (-2 - 7a - 4b + 6ab)$$

This presentation is perhaps interesting because generators v_3, v_4, v_5, v_6 share with the bicyclic generators v_1, v_2 the property that they are all of the form $1 + n$ where n is nilpotent. We will close by showing that it is impossible to find a complete set of generators of this type.

Since a nilpotent element in an integral group ring has identity coefficient equal to 0 ([5], p. 167, or an easy direct argument for the special case where the group is P), it follows that if $1 + n_1, \ldots\ldots 1 + n_t$ are units in W, with $n_1, \ldots\ldots n_t$ nilpotent, and $(1 + n_1)\ (1 + n_2)\ \ldots\ (1 + n_t) = 1 + (1 - a^2)\ (1 + b^2)$ $(\alpha_1 + \alpha_2 a + \alpha_3 ab + \alpha_4 ab)$, then $\alpha_1 \equiv 0 \pmod 4$. Thus generators v_7 and v_9 are not contained in the subgroup of W generated by all units of the form $1 + n$, where n is nilpotent.

REFERENCES

1. E.G. Goodaire, E. Jespers, M.M. Parmenter, Determining units in some integral group rings, Canad. Math. Bull., to appear.

2. Eric Jespers, Guilherme Leal, Describing units of integral group rings of some 2-groups, to appear.

3. C. Polcino Milies, The units of the integral group ring ZD_4, Bol. Soc. Brasil. Mat 4 (1972), 85-92.

4. J. Ritter, S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, to appear.

5. S.K. Sehgal, Topics in group rings , Marcel Dekker, New York, 1978.

Memorial University of Newfoundland
St. John's, Canada

Received May 30, 1990

Class Numbers Bounded Below by the Divisor Function

By R.A. Mollin

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

Abstract

The main result of this paper is to provide lower bounds in terms of the divisor function τ for the class numbers of a collection of real quadratic fields. These results generalize the very special case found in Halter-Koch [2]. Moreover it generalizes and extends work in Mollin [4] – [11] as well as in Azuhata [1], Hasse [3] and Yokai [15] – [17].

§1. Notation and Preliminaries.

Throughout $K = Q(\sqrt{d})$ where $d > 0$ is square-free and K has class number h(d). $\tau(x)$ denotes the number of positive divisors of an integer x. We let

$$\sigma = \left\{ \begin{array}{l} 2 \text{ if } d \equiv 1 \pmod 4 \\ 1 \text{ if } d \equiv 2,3 \pmod 4 \end{array} \right\} \text{ and}$$

$$w_d = (\sigma - 1 + \sqrt{d})/\sigma.$$

The continued fraction expansion of $w_d = \langle a_0, \overline{a_1, a_2, \ldots, a_k} \rangle$, with period length k, satisfies: $a_i = \lfloor (P_i + \sqrt{d})/Q_i \rfloor$ for $i \geq 0$ where: $(P_0, Q_0) = (\sigma - 1, \sigma)$, and $\lfloor\ \rfloor$ denotes the greatest integer function.

Finally, $P_{i+1} = a_i Q_i - P_i$, and $Q_{i+1} Q_i = d - P^2_{i+1}$ for $i \geq 0$.

§2. Results

Since the proofs are too long and detailed to provide herein we state, without proof, the results; and provide applications thereof. The proofs will appear elsewhere.

Theorem 2.1

Let $d = a^2 + r \not\equiv 1 \pmod 4$ be square-free with $|r| < 2a$, and set $g = \gcd(2a - |r - 1|, d)$. Assume that no divisor m of $2a - |r - 1|$ with $1 < m < 2a - |r - 1|$ equals Q_i for any i in the continued fraction expansion of $\sqrt{d}$. Then: $h(d) \geq \tau(2a - |r - 1|) - 2^n$ where n is the number of distinct prime divisors of g if $2a - |r - 1|$ is odd or g is even, and n is the number of distinct prime divisors of 2g otherwise.

Applications I

(1) If $r = 1$ and a is odd then we have the result of the Halter-Koch [2]; viz.; $h(d) \geq 2\tau(a) - 2$. This is a very special case of Theorem 2.1, however since here $k = 1$. The only other possibility where $k = 1$ will be completed in Theorem 2.2.

(2) $|r| = 2$, (Note that in [9] we showed that if $h(d) = 1$ and $d = \ell^2 + r$ (>7) with $d \not\equiv 1 \pmod 4$ then $|r| = 2$). By Theorem 2.1:

$$(d) \geq \begin{cases} \tau(2a - 1) - 1 \text{ if } g = 1 \text{ and } r = 2 \\ \tau(2a - 1) - 2 \text{ if } g = 3 \text{ and } r = 2 \\ \tau(2a - 3) - 1 \text{ if } r = -2 \end{cases}$$

This leads to the conjecture: If $d = a^2 \pm 2$ then $h(d) = 1$ if and only if $d \in \{2,3,6,7,11,14,23,38,47,62,83,167,227,398\}$. A more general result than this conjecture was proved under a suitable Riemann hypothesis in [12] – [13]; and without the Riemann hypothesis in [14] to the extent that there is possibly only one more value, (which would turn out to be a counterexample to the Riemann hypothesis if it existed). Also see [9, Theorem 1, p.162] for further restrictions on d when $h(d) = 1$, and compare those restrictions forced by the above.

(3) $d = a^2 + r$ where $|r|\,|4a$ and $d \not\equiv 1 \pmod 4$. It is easily checked that the hypothesis of Theorem 2.1 holds in this case. In fact (1) – (2) above are special cases thereof.

Theorem 2.2. Let $d = \ell^2 + r \equiv 1 \pmod 4$ be square-free with $|r| < 2\ell$.

(a) If $2\ell - |r - 1| \equiv 0 \pmod 4$ then $h(d) \geq \tau((2\ell - |r - 1|)/4) - 2^m$ where m is the number of distinct prime divisors of gcd $(2\ell - |r - 1|, d)$; and no divisor t of $(2\ell - |r - 1|)/4$ appears as a $Q_i/2$ in the continued fraction expansion of $(1 + \sqrt{d})/2$ with $1 < t < (2\ell - |r - 1|)/4$.

(b) If $2\ell - |r - 1| \equiv 0 \pmod 4$ and no divisor t, with $1 < t < 2\ell - |r - 1|$ equals $Q_i/2$ for any i in the continued fraction expansion of $(1 + \sqrt{d})/2$ then:

$$h(d) \geq \tau(\ell - |r/4 - 1|) - 2^m$$

where m is the number of distinct prime divisors of gcd $(\ell - |r/4 - 1|, d)$.

Applications II:

(1) If $r = 1$ then we get Halter-Koch's [2] special case $h(d) \geq \tau(\ell/2) - 1$.

(2) If $r = 4$ then we get Halter-Koch's only other result along these lines in [2]; viz. $h(d) \geq \tau(\ell) - 1$.

(3) If $d \equiv 1 \pmod 4$, $r > 1$ is odd and $r|\ell$ then $h(d) \geq \tau((2\ell - r + 1)/4) - 1$. Here we can easily check that the hypothesis of Theorem 2.2 holds.

(4) If $r > 4, d \equiv 1 \pmod 4$, r even and $r|4\ell$ then again the hypothesis of Theorem 2.2 holds and we get:

$h(d) \geq \tau(\ell - r/4 + 1) - 2^m$ where m is the number of distinct prime divisors of gcd $(\ell - r/4 + 1, d)$.

(5) If $d \equiv 1 \pmod 4$, $r < -1$, ℓ even and $r|\ell$ then $h(d) \geq \tau((2\ell + r - 1)/4) - 2^m$ where m is the number of distinct prime divisors of gcd $(2\ell + r - 1, d)$.

(6) $d \equiv 1 \pmod 4$, $r < 0$, $r \neq -4$, r even and $r|4\ell$. Then: $h(d) \geq \tau(\ell + (r/4) - 1) - 2^m$ where m is the number of distinct prime divisors of $\gcd(\ell + (r/4) - 1, d)$.

Remark 2.1 All of the examples in Applications (I) – (II) are instances of ERD–types, i.e., extended Richaud–Degert types $d = \ell^2 + r$ with $r|4\ell$ which have been extensively studied in [1] – [17]. In point of fact the aforementioned applications yield all ERD–types thus extending and completing the special cases $r = 1$ and $r = 4$ done by Halter–Koch [2].

Remark 2.2 The above applies not only to ERD–types but more general types as well. For example $d = 10^2 - 6 = 94$ is not an ERD–type and the bound in Theorem 2.2 is precise; i.e., $h(d) = 1 = \tau(2a + r - 1) - 1 = \tau(13) - 1 = 1$. Many more such examples abound, and it can be shown that there are in fact infinitely many such non–ERD types.

Remark 2.3 To illustrate the sharpness of the bounds we give some explicit examples for Applications (II).

(1) $d = 65 = 8^2 + 1$; $h(d) = 2 = \tau(4) - 1$

(2) $d = 85 = 9^2 + 4$; $h(d) = 2 = \tau(9) - 1$

(3) $d = 105 = 10^2 + 5$; $h(d) = 2 = \tau(4) - 1$

$d = 689 = 26^2 + 13$; $h(d) = 4 > \tau(10) - 1 = 3$

(4) $d = 21 = 3^2 + 12$; $h(d) = 1 = \tau(7) - 1$

$d = 2669 = 51^2 + 68$; $h(d) = 4 > \tau(35) - 1 = 3$

(5) $d = 12^2 - 3$; $h(d) = 1 = \tau(5) - 1$

$d = 777 = 28^2 - 7$; $h(d) = 4 = \tau(12) - 2$

(6) $d = 1509 = 39^2 - 12$; $h(d) = 3 = \tau(35) - 1$

Acknowledgement: The author's research is supported by an NSERC grant. Moreover this current research was supported by a Killam research award held at the University of Calgary in 1990.

References

[1] T. Azuhata, On the Fundamental Units and the Class Numbers of Real Quadratic Fields, Nagoya Math. J. 95 (1984), 125–135.

[2] F. Halter–Koch, Quadratische Ordnungen mit grosser Klassenzahl, J. Number Theory 34, (1990), 82–94.

[3] H. Hasse, Über mehrklassige aber eingeschlechtige reell–quadratische Zahlkörper, Elem. Math 20 (1965), 49–59.

[4] R. A. Mollin, Necessary and sufficient conditions for the class number of a real quadratic field to be one, and a conjecture of S. Chowla, Proc. Amer. Math. Soc. 102 (1988), 17–21.

[5] R. A. Mollin, On the insolubility of a class of diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud–Degert type, Nagoya Math. J. 105 (1987), 39–47.

[6] R. A. Mollin, Diophantine Equations and Class Numbers, J. Number Theory 24 (1986) 7–19.

[7] R. A. Mollin, Generalized Fibonacci primitive roots, and Class Numbers of real quadratic fields, Fib. Quarterly 26 (1988), 46–53.

[8] R. A. Mollin, Class Number One criteria for real quadratic fields I, Proc. Japan Acad., Ser. A, 63 (1987), 121–125.

[9] R. A. Mollin, Class Number One criteria for real quadratic fields II, Proc. Japan Acad., Ser A. 63 (1987), 162–164.

[10] R. A. Mollin, Lower bounds for class numbers of real quadratic and biquadratic fields, Proc. Amer. Math. Soc. 101 (1987), 439–444.

[11] R. A. Mollin, Lower bounds for class numbers of real quadratic fields, Proc. Amer., Math Soc. 96 (1986), 545–550.

[12] R. A. Mollin, and H. C. Williams, On prime-valued polynomials and class numbers of real quadratic fields, Nagoya Math J. 112 (1988), 143–151.

[13] R. A. Mollin and H. C. Williams, Prime producing quadratic polynomials and real quadratic fields of class number one, in Number Theory (J. M. DeKoninck and C. Levesque (ed)), Walter de Gruyter, Berlin, New York (1989), 654–663.

[14] R. A. Mollin and H. C. Williams, Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception), in Number Theory (R. A. Mollin (ed.)), Walter de Gruyter, Berlin, New York (1990), 417–425.

[15] H. Yokoi, On the diphantine equation $x^2 - py^2 = \pm 4q$ and the class number of real subfields of a cyclotomic field, Nagoya Math. J. 91 (1983), 151–161.

[16] H. Yokoi, On real quadratic fields containing units with norm–1, Nagoya math. J. 33 (1968), 139–152.

[17] H. Yokoi, On the fundamental unit of real quadratic fields with norm 1, J. Number Theory 2, (1970), 106–115.

Department of Mathematics & Statistics

University of Calgary

Received July 4, 1990

ZEROS FOR SET-VALUED MAPS WITH NON-COMPACT DOMAINS

by

H. Ben-El-Mechaiekh

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

ABSTRACT. The main purpose of this note is to prove a result on the existence of a zero for certain set-valued maps with non-compact domains which extends well known theorems of Browder [5], Fan [10], Cornet [8] and Lasry-Robert [12].

BASIC DEFINITIONS

Let's first formulate some basic definitions and properties. (Our notations and terminology on set-valued maps are those of [4]). By a <u>space</u> E we shall always understand a Hausdorff topological vector space. If Y is a space, a point $x_0 \in X$ is a <u>zero</u> for the map $A : X \to Y$ if $0 \in A(x_0)$

If X and Y are two sets and if **A** is a class of (set-valued) maps, we write

$$\mathbf{A}(X,Y) = \{A : X \to Y \mid A \in \mathbf{A}\}, \ \mathbf{A}(X) = \mathbf{A}(X,X).$$

The basic class of **H**-maps is defined by:

$A \in \mathbf{H} \iff$ (i) A has non-empty closed convex values, (ii) A is uhc $^{(1)}$;

The class $\mathbf{K} = \{A \mid A$ is usc and has non-empty compact convex values$\}$ first considered by Kakutani, satisfies $\mathbf{K} \subseteq \mathbf{H}$. In fact, if E is a locally convex space, $\mathbf{K}(X,E) = \{A \in \mathbf{H}(X,E) \mid A$ has compact values$\}$ (cf Castaing-Valadier [6]). Also, if f is a locally lipschitzian (resp. convex and continuous on the interior of its domain) real function, then the Clarke generalized gradient map ∂f (resp. gradient) is an **H**-map (cf Aubin [1]).

Definition 0. Let E and F be two spaces, $l \in L(E,F)$ a bounded linear operator, X a non-empty subset of E and $U, V \subseteq X$. A map $S : X \to F$ is said to satisfy the <u>condition of Fan on U with respect to V and l</u> if and only if for any $x \in U$, $\inf_{l^*\psi \in M_V(x)} \sigma_S(x,\psi) \geq 0$

$$\text{where } M_V(x) = \{\varphi \in E' \mid \varphi(x) \geq \max_{z \in V} \varphi(z)\}.$$

In the case where $V = U = X$, a similar condition was considered by Aubin [1].

THE MAIN THEOREM

The purpose of this note is to prove the following:

Theorem 1. Let X be a non-empty convex paracompact subset of a space E, F a locally convex space, $\iota \in L(E,F)$ and $S \in H(X,F)$. Suppose that there exist a compact $K \subseteq X$ and a compact convex $C \subseteq X$ such that:

(i) S satisfies the condition of Fan on $X \setminus K$ with respect to C and ι;

(ii) S satisfies the condition of Fan on $K \cap \partial X$ with respect to X and ι.

Then S has a zero and $\iota + S$ is surjective.

PRELIMINARY RESULTS AND PROOF

The following non-linear alternative will be useful in the sequel:

Lemma 2 [(2)]. Let X be a non-empty convex subset of a space E and $f, g : X \times X \to R$ two functions satisfying the following conditions:
(i) for any $(x,y) \in X \times Y$, $f(x,y) \leq g(x,y)$; (ii) for any $y \in X$, $x \to f(x,y)$ is lsc on X;
(iii) for any $x \in X$, $y \to g(x,y)$ is quasi-concave on X; (iv) for some $\lambda \in R$, there exist a compact $K \subseteq X$ and a compact convex $C \subseteq X$ such that for each $x \in X \setminus K$ there exists $y \in C$ with $f(x,y) > \lambda$.

Then, one of the following properties holds:

(1) there exists $x_0 \in X$ such that $f(x_0,y) \leq \lambda$ for all $y \in X$, or

(2) there exists $y_0 \in X$ such that $g(y_0,y_0) > \lambda$.

Let's introduce at this point a convenient abstract class of set-valued maps, namely the class of S-maps defined by:

$A \in S(X,Y) \iff$ For every paracompact $K \subseteq X$, $A|_K$ has selection $s \in c(K,Y)$;

where $c(K,Y)$ is the class of all continuous functions from K into Y.

Examples of S-maps were first considered by E. Michael [14]. The inclusions $F(X,Y) \subseteq \Phi(X,Y) \subseteq S(X,Y)$ where $A \in F(X,Y) \iff$ A has open fibers and non-empty convex values; $A \in \Phi(X,Y) \iff$ (i) A has convex values, (ii) A has a selection B with open fibers and non-empty values are proved in [3]. For other examples of S-maps the reader is referred to E. Michael [14], [15].

The starting point is the following existence theorem for quasi-concave functions.

Proposition 3. Let X be a non-empty convex paracompact subset of a space E, Y a non-empty convex subset of $\mathfrak{X} = \{ \varphi: X \to R \mid \varphi$ is usc and quasi-concave $\}$, and $A \in S(X,Y)$. Suppose that there exist a compact $K \subseteq X$ and a compact convex $C \subseteq X$ such that

$$\text{for any } x \in X \setminus K \text{ and any } \varphi \in A(x),\ \varphi(x) < \max_{z \in C} \varphi(z).$$

Then there exists $x_0 \in X$ and $\varphi_0 \in A(x_0)$ such that $\varphi_0(x_0) = \max_{z \in X} \varphi_0(z)$

PROOF. Since $A \in S(X,Y)$, there exists $s \in c(X,Y)$ with $s(x) \in A(x)$ for all $x \in X$. Clearly, the function $f : X \times X \to R$ defined by $f(x,y) = [s(x)](y) - [s(x)](x)$ for $(x,y) \in X \times X$ satisfies (ii) and (iii) of lemma 2. Moreover, if $x \in X \setminus K$ and $\tilde{y} \in C$ verifies $[s(x)](\tilde{y}) = \max_{z \in C} [s(x)](z)$ then $[s(x)](x)] < [s(x)](\tilde{y})$ i.e. $f(x,\tilde{y}) > 0$ and (iv) is therefore satisfied for $\lambda = 0$. Since $f(y,y) = 0$ for all $y \in X$, (2) is impossible i.e. there exists $x_0 \in X$ such that $f(x_0,y) \leq 0$ for every $y \in X$. The proof is complete with $\varphi_0 = s(x_0)$.♦

In the case where $S = F$, this result was proven by to J.C. Bellenger [2]. If X is compact and $S = \Phi$, the preceding result is due to S. Simons [16]; if $X = \{ \varphi: X \to R \mid \varphi$ is usc and concave$\}$ and $S = F$, the result is due to K. Fan [10].

Let now $l \in L(E,F)$ a bounded linear operator where F is a space and $\hat{Y}$ a convex subset of $\{\psi : F \to R \mid \psi$ is usc and quasi-concave$\}$. Putting $P = F$ in proposition 3 leads to the following analytical formulation:

Proposition 4. Let X be a non-empty convex paracompact subset of a space E and $f, g : X \times \hat{Y} \to R$ be two functions satisfying the conditions:
(i) for any $\psi \in \hat{Y}$, $x \to f(x,\psi)$ is lsc on X; (ii) for any $x \in X$, $\psi \to f(x,\psi)$ is concave on $\hat{Y}$;
(iii) for any $\psi \in \hat{Y}$, $x \to g(x,\psi)$ is usc on X; (iv) for any $x \in X$, $\psi \to g(x,\psi)$ is convex on $\hat{Y}$;
(v) there exist a compact $K \subseteq X$ and a compact convex $C \subseteq X$ such that:

$$\text{for any } x \in X \setminus K, \text{ if } \psi \in \hat{Y} \text{ satisfies } \psi l(x) \geq \max_{z \in C} \psi l(z) \text{ then } f(x,\psi) \leq g(x,\psi).$$

Then one of the following properties holds:
(1) there exists $\hat{x} \in X$ such that $f(\hat{x},\psi) \leq g(\hat{x},\psi)$ for all $\psi \in \hat{Y}$, or
(2) there exists $x_0 \in K$ and $\psi_0 \in \hat{Y}$ such that

$$\psi_0 l(x_0) = \max_{z \in X} \psi_0 l(z) \text{ and } f(x_0,\psi_0) > g(x_0,\psi_0).$$

Now, let $S,T \in H(X,F)$ where X, E and F are as before. The previous proposition applied to $\hat{Y} = F'$, $f(x,\psi) = \inf_{z \in T(x)} \langle\psi,z\rangle$ and $g(x,\psi) = \sigma_S(x,\psi)$ for all $(x,\psi) \in X \times F'$, gives:

Proposition 5. Suppose that there exist a compact $K \subseteq X$ and a compact convex $C \subseteq X$ such that for all $x \in X \setminus K$, for all $\psi \in F'$

$$\langle 1^*\psi, x\rangle \geq \max_{z \in C} \langle 1^*\psi, z\rangle \Rightarrow \inf_{z \in T(x)} \langle\psi,z\rangle \leq \sigma_S(x,\psi).$$

Then one of the following properties holds:

(1) there exists $\hat{x} \in X$ such that $\inf_{z \in T(\hat{x})} \langle\psi, z\rangle \leq \sigma_S(\hat{x},\psi)$ for all $\psi \in F'$, or

(2) there exists $x_0 \in K$ and $\psi_0 \in F'$ such that

$$1^*\psi_0 \in N_X(x_0) \text{ and } \inf_{z \in T(x_0)} \langle\psi_0,z\rangle > \sigma_S(x_0,\psi_0)$$

where $N_X(x_0) = \{\varphi \in E' \mid \varphi(x_0) = \max_{z \in X} \varphi(z)\}$ is the normal cone to X at x_0.

Putting $T \equiv 0$ in Proposition 5 enables us to give the

PROOF OF THEOREM 1. Notice first that (ii) is equivalent to

(ii)' S satisfies the condition of Fan on K with respect to X and 1.

For, if $x \in K \cap \mathrm{int}(X)$, there exists an open neighborhood U of the origin in E such that $x + U \subseteq X$ and, if $1^*\psi \in N_X(x)$, then $1^*\psi(x) \geq 1^*\psi(x + u)$ i.e. $1^*\psi(u) \leq 0$ for any $u \in U$ i.e. $1^*\psi \equiv 0 \equiv \psi$ and therefore $\sigma_S(x,\psi) = 0$. Since the condition (2) of proposition 5 cannot be verified, there exists $\hat{x} \in X$ such that $0 \leq \sigma_S(\hat{x},\psi)$ for all $\psi \in F'$. Suppose, for a contradiction, that $0 \notin S(\hat{x})$. There exists a convex open neighborhood U of the origin in F such that $U \cap S(\hat{x}) = \emptyset$. By The Hahn-Banach theorem, there exists $\hat{\psi} \in F'$ and $\alpha \in \mathbb{R}$ such that $\hat{\psi}(y) \leq \alpha < \hat{\psi}(x)$ for all $x \in U$ and $y \in S(\hat{x})$. Hence, $\hat{\psi}(y) \leq \alpha < 0$ for all $y \in S(\hat{x})$ and $\sigma_S(\hat{x},\hat{\psi}) < 0$ which is impossible. To prove the second part of the theorem, for arbitrary $v \in 1(X)$, say $v = 1(x_0)$, consider the map $R(x) = S(x) + 1(x) - v$. Clearly, $R \in H(X,F)$, and since $\sigma_R(x,\psi) = \sigma_S(x,\psi) + \langle 1^*\psi,x-x_0\rangle$ then R satisfies the condition of Fan on $X \setminus K$ with respect to $\hat{C} = \mathrm{conv}(C,x_0)$ and the condition of Fan on $K \cap \partial X$ with respect to X and 1. The conclusion follows from the first part of the proof.♦

REMARK: in the case where X is compact, then (i) and (ii) are satisfied and we obtain results of Browder [5], Cornet [8], Fan [10] and Lasry-Robert [12].

SOME CONNECTED RESULTS

Putting $S \equiv 0$, $E = F$ and $l = Id$ in Proposition 5 leads to:

Proposition 6. Let E be a locally convex space, $X \subseteq E$ be non-empty convex paracompact, $T \in H(X,E)$, $K \subseteq X$ compact and $C \subseteq X$ convex compact such that:

(i) for any $x \in X \setminus K$, $\langle\varphi, x\rangle \geq \max_{z \in C} \langle\varphi, z\rangle \Rightarrow \inf_{z \in T(x)} \langle\varphi,z\rangle \leq 0$;

(ii) for any $x \in K \cap \partial X$ and any $\varphi \in N_X(x)$, there exists $\hat{y} \in T(x)$ with $\varphi(\hat{y}) \leq 0$.

Then T has a zero.

REMARKS: (1) The previous results contains several extensions of the Fan-Glicksberg-Kakutani fixed point theorem. Indeed, given a a locally convex space E and a convex compact $X \subseteq E$, a map $T : X \to E$ is said to satisfy: (1) the <u>condition of Kakutani</u> if $T(x) \cap (X-x) \neq \emptyset$ for all $x \in X$; (2) the <u>condition of Halpern</u> if $T(x) \cap \bigcup_{\lambda \geq 0} \lambda(X-x) \neq \emptyset$ for all $x \in X$; (3) the <u>weak condition of Halpern</u> if $T(x) \cap \overline{\bigcup_{\lambda \geq 0} \lambda(X-x)} \neq \emptyset$ for all $x \in X$; (4) <u>the condition of Fan</u> if for $x \in X$, and $\varphi \in N_X(x)$ there exists $z \in T(x)$ such that $\varphi(z) \leq 0$; one easily verifies the implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ [(i) and (ii)].

(2) Under the hypothesis of 4 and assuming that for each $x \in X$, $S(x)$ or $T(x)$ is compact for a suitable topology on E, one can formulate a coincidence theorem for H-maps.

The following matching theorem is a slight modification of a result of K. Fan [10] and follows directly from the previous proposition:

Proposition 7. (K. Fan). Let E be a locally convex space, $X \subseteq E$ be non-empty convex paracompact, $K \subseteq X$ compact, $C \subseteq X$ convex compact, $\{F_i \mid i \in I\}$ be a locally finite closed (in X) covering of X and $\{C_i \mid i \in I\}$ a collection of subsets of X indexed by the same set I satisfying: (i) for any $x \in X \setminus K$, $\overline{\text{conv}}\{C_i \mid i \in I(x)\} \cap C \neq \emptyset$; (ii) for any $x \in K \cap \partial X$, $\overline{\text{conv}}\{C_i \mid i \in I(x)\} \cap X \neq \emptyset$ where $I(x) = \{i \in I \mid x \in F_i\}$.

Then there exists a finite subset $I_0 \subseteq I$ such that $\bigcap_{i \in I_0} F_i \cap \overline{\text{conv}}\{C_i \mid i \in I_0\} \neq \emptyset$.

(For the proof, take $T(x) = \overline{\text{conv}}\{C_i \mid i \in I(x)\}$ in proposition 6).

Using Proposition 7, we derive a non-linear alternative of the Leray-Schauder type for the class F.

Theorem 8. Let E be a locally convex space, $X \subseteq E$ closed, $K \subseteq X$ compact, $C \subseteq X$ compact convex, $0 \in \mathrm{int}(X) \cap K$, $A \in F(X,E)$ such that for any $x \in X \setminus K$, $A(x) \cap C \neq \emptyset$.

Then one of the following properties holds:

(1) A has a fixed point, or

(2) there exist $\hat{x} \in \partial X$ and $\lambda \in]0,1[$ such that $\hat{x} \in \lambda A(\hat{x})$.

Notes

(1) A closed convex valued map $A : X \to F$ is upper-hemicontinuous (uhc in short) if the function $x \to \sigma_A(x,\varphi) = \sup_{z \in A(x)} \langle \varphi, z \rangle$ is usc on X for all $\varphi \in F'$. A map $A : X \to Y$ is upper-semicontinuous (usc) in X if $\{x \in X \mid A(x) \subseteq V\}$ is open in X for any open $V \subseteq Y$. If A is usc then it is uhc.

(2) Lemma 2 is the analytic formulation of a fixed point theorem for Φ-maps without compactness on the domain. The reader is referred to [3]. Conditions similar or equivalent to (iv) were considered by various authors (cf [3], [4], [10], [13]).

References

[1] AUBIN, J.P., Analyse fonctionnelle non-linéaire et applications à l'équilibre économique, Ann. Sc. Math. Québec, II, 1, (1978), 5-47.8c

[2] BELLENGER, J.C., Existence of maximizable quasiconcave functions on paracompact Convex spaces, J. Math. Anal. Appl., 123, (1987), 333-338.

[3] BEN-EL-MECHAIEKH, H., DEGUIRE, P., GRANAS, A., Points fixes et coïncidences pour les fonctions multivoques II (Applications de type Φ et Φ^*) C.R. Acad. Sc. Paris, 295, Série I, (1982), 381-384.

[4] BEN-EL-MECHAIEKH, H., DEGUIRE, P., GRANAS, A., Points fixes et coïncidences pour les fonctions multivoques III (Applications de type M et M*) C. R. Acad. Sc. Paris, 305, Série I, (1987), 381-384.

[5] BROWDER, F., The fixed point theory of multi-valued mappings in topological vector spaces, Math. Ann., 177, (1968), 283-301.

[6] CASTAING, C., VALADIER, M., Convex analysis and measurable multifunctions, Lecture Notes in Math., 580, Springer-Verlag, Berlin-Heidelberg-New York, 1977.

[7] CLARKE, F.H., Generalized gradients and applications, Trans. Amer. Math. Soc., 205, (1975), 247-262.

[8] CORNET, B., Paris avec handicaps et théorème de surjectivité de correspondances, C. R. Acad. Sc. Paris, 281, (1975), 479-482.

[9] FAN, K., Sur un théorème minimax, C.R. Acad. Sc. Paris, Groupe I, 259, (1962), 3925-3928.

[10] FAN, K., Some properties of convex sets related to fixed point theorems, Math. Ann., 266, (1984), 519-537.

[11] HALPERN, B.R., BERGMAN, G.M., A fixed-point theorem for inward and outward maps, Trans. Amer. Math. Soc., 130, (1968), 353-358.

[12] LASRY, J.M., ROBERT, R., Analyse Non-Linéaire Multivoque, Cahiers de Math. de la Décision 7611, (1976), Université de Paris-Dauphine.

[13] LASSONDE, M., On the use of KKM multifonctions in fixed point theory and related topics, J. Math. Anal. Appl., 97, (1983), 151-201.

[14] MICHAEL, E., Continuous selections, Ann. Math., 63, N-Z, (1956), 361-382.

[15] MICHAEL, E., Continuous selections and countable sets, Fund. Math., 111, (1981), 1-10.

[16] SIMONS, S., An existence theorem for quasiconcave functions and applications, Nonlinear Anal., TMA, in press.

Department of Mathematics, Brock University, St Catharines, Ontario, L2S 3A1, Canada

Received May 3, 1990
in revised form July 16, 1990

A NOTE ON SPECIAL UNITS OF RUBIN

Trajano Nóbrega

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

1. Introduction:

The group $C_{cycl}(K)$ of cyclotomic units of an abelian number field K plays an important role in the study of annihiators of the ideals class group of K. In a recent paper, Rubin [1], defined a group of Special units $S(K)$ of an abelian number field K and showed that when $K = K_m^+$, the maximal real subfield of the cyclotomic field $Q(e^{\frac{2\pi i}{m}})$, then $S(K)$ contains $C_{cycl}(K)$. He expresses interest in the question whether this inclusion is an equality, when $K = K_m^+$ for some positive integer m.

In this note we show that this inclusion is strict: Let $K_m = Q(e^{\frac{2\pi i}{m}})$, $C_I = C_{cycl}(K_m) \cap K_m^+$ the group of cyclotomic units of K_m^+ defined by intersection and C_N the image by norm from K_m to K_m^+ of $C_{cycl}(K_m)$, where $C_{cycl}K_m) = \{\delta = \Pi_{i=1}^{m-1}(i-\xi_m^i)^{a_i} : a_i \in \mathbb{Z}$ and δ is a unit in $\mathbb{Z}[\xi_m]\}$. We show that $C_N \subseteq C_I \subseteq S(K_m^+)$. In the presence of this it is natural to extend Rubin's question and ask whether the second inclusion above is an equality.

Through this paper we will denote $\xi = e^{\frac{2\pi i}{m}}$, $\xi_n = e^{\frac{2\pi i}{n}}$, for $n \neq m$, $K_n = Q(\xi_n)$, $K_n^+ = K_n \cap \mathbb{R}$ and O_K the ring of integers of a number field K.

Since $K_n = K_{2n}$ when n is odd, for cyclotomic fields K_n we may take $n \not\equiv 2 \pmod 4$.

2. The main results

We begin showing that $C_I \subseteq S(K_m^+)$. For this, we need some notation. Let p be a rational prime that splits completely in K_m^+, $L = K_m^+ \cdot K_p^+$, $L_1 = K_m \cdot L$, $\tilde{p}$ the product of all prime ideals of L that lie over p and $\tilde{p}_1 = \tilde{p}O_{L_1}$. It is easy to see that $\tilde{p} = (1-\xi_p)(1-\xi_p^{-1})O_L$ and $\tilde{p}_1 = (1-\xi_p)(1-\xi_p^{-1})O_{L_1}$.

Theorem 1: If $\varepsilon = \pm\xi^t\Pi_{i=1}^{m-1}(1-\xi^i)^{a_i} \in K_m^+$ then $u = \xi^{2t}\Pi_{i=1}^{m-1}[(1-\xi^i\xi_p)(1-\xi^i\xi_p^{-1})]^{a_i} \in L$, $\varepsilon^2 \equiv u \pmod{\tilde{p}}$ and $N_{L/K_m^+}(u) = 1$. In particular $C_I \subseteq S(K_m^+)$.

Proof: Since $(1-\xi^i)^2 \equiv (1-\xi^i\xi_p)(1-\xi^i\xi_p^{-1}) \pmod{\tilde{p}_1}$ then $\varepsilon^2 \equiv u \pmod{\tilde{p}_1}$. If $\varepsilon \in K_m^+$ then $\varepsilon = \bar{\varepsilon}$, where bar means complex conjugation, and this implies that $\xi^{2t+\Sigma_{i=1}^{m-1}ia_i} = (-1)^{\Sigma_{i=1}^{m-1}a_i}$ and so $4t + 2\Sigma_{i=1}^{m-1}ia_i \equiv 0 \pmod{m}$. But this is sufficient condition for $u \in L$, because $Gal(L_1/L) = \{1, \sigma\}$, where σ is the complex conjugation restricted to L_1. Now, $N_{L/K_m^+}(u) = N_{L_1/K_m}(u) = \xi^{t(p-1)}\Pi_{i=1}^{m-1}N_{L_1|K_m}[(1-\xi^i\xi_p)(1-\xi^i\xi_p^{-1})]^{a_i} = \xi^{t(p-1)}\Pi_{i=1}^{m-1}\left(\frac{1-\xi^{pi}}{1-\xi^i}\right)^{a_i} = \epsilon^{\sigma_p - 1}$, where σ_p is the Frobenius map for p in the Galois group of K_m^+/Q. Since p splits completely in K_m^+ we must have $\sigma_p|_{K_m^+} = Id_{K_m^+}$ and so $N_{L/K_m^+}(u) = 1$. But u is integral and $N_{L/Q}(u) = 1$, then u is a unit of L. Finally, if $\varepsilon \in C_I$ and p is a rational prime that splits completely in K_m^+ then there is a unit of L with norm 1 from L to K_m^+ such that $\varepsilon^2 \equiv u \pmod{\tilde{p}}$, so that ε is a special unit in sense of Rubin; thus $C_I \subseteq S(K_m^+)$.

We now proceed to show that C_I contain C_N properly. First we need two lemmas.

Lemma 1: If m is a prime power, $m = p^a$ say, then $\alpha = \Pi_{i=1}^{m-1}(1-\xi^i)^{a_i}$ is a unit in K_m if and only if $\Sigma_{i=1}^{m-1}p^{r_i}a_i = 0$, where $p^{r_i}//i$.

Proof: Let $i = p^r t$ with $0 \leq r < a$ and $(t,p) = 1$. Then $1 - \xi^i = 1 - (\xi^t)^{p^r} = \Pi_{j=1}^{p^r}(1-\xi^t\xi_{p^r}^j) = \Pi_{j=1}^{p^r}(1-\xi^{t+j\,p^{a-r}})$. But each factor $1-\xi^\ell$, with $(\ell,p) = 1$, is associated to $1-\xi$, hence $1-\xi^i = \varepsilon_i(1-\xi)^{p^r}$ for some unit ε_i of K_m. Now $\alpha = \varepsilon(1-\xi)^{\Sigma_{i=1}^{m-1}p^{r_i}a_i}$ and the principal ideal $(1-\xi)$ is prime, then α is a unit in K_m if and only if $\Sigma_{i=1}^{m-1}p^{r_i}a_i = 0$.

Lemma 2: If $m = p^a$ (with $a > 1$ if $p = 2$) then $C_N = C_I^2$.

Proof: It is clear that $C_I^2 \subseteq C_N$. If $\alpha = \Pi_{i=1}^{m-1}[(1-\xi^i)(1-\xi^{-i})]^{a_i}$, we can write $\alpha = (-1)^{\Sigma_{i=1}^{m-1} a_i} \cdot \xi^{-\Sigma_{i=1}^{m-1} i a_i} \Pi_{i=1}^{m-1}(1-\xi^i)^{2a_i}$. If $m = 2^a$ then $\Sigma_{i=1}^{m-1} i a_i = \Sigma_{i=1}^{m-1} 2^{r_i} t_i a_i \equiv \Sigma_{i=1}^{m-1} 2^{r_i} a_i = 0 \pmod 2$ (lemma 1) and $\alpha = (-1)^{\Sigma_{i=1}^{m-1} a_i} \beta^2$ where $\beta = \xi^{-\Sigma_{i=1}^{m-1} \frac{i a_i}{2}} \cdot \Pi_{i=1}^{m-1}(1-\xi^i)^{a_i} \in K_m$. If $\Sigma_{i=1}^{m-1} a_i \equiv 0 \pmod 2$ then $\beta \in C_I$ and $\alpha = \beta^2 \in C_I^2$. If $\Sigma_{i=1}^{m-1} a_i \equiv 1 \pmod 2$ then $\beta = \xi^{\frac{m}{4}} \gamma$ where $\gamma \in C_I$ and $\alpha = \gamma^2 \in C_I^2$. Now we suppose $p \neq 2$ and $\beta = \xi^{-\Sigma_{i=1}^{m-1} \frac{i a_i}{2}} \cdot \Pi_{i=1}^{m-1}(1-\xi^i)^{a_i}$ where $\Sigma_{i=1}^{m-1} \frac{i a_i}{2}$ is considered mod p^a. Since $\Sigma_{i=1}^{m-1} a_i \equiv \Sigma_{i=1}^{m-1} p^{r_i} a_i = 0 \pmod 2$ (lemma 1) then $\beta \in C_I$ and $\alpha = \beta^2 \in C_I^2$.

Remark: Since C_I is of rank $\frac{\phi(m)}{2} - 1$, the torsion part of $C_I = \{\pm 1\}$ and C_I^2 is torsion free, we have $[C_I : C_I^2] = 2^{\frac{\phi(m)}{2}}$, ϕ being Euler's function.

Theorem 2: If we denote by $\theta(m)$ the index $[C_I : C_N]$, then

$$\theta(m) = \begin{cases} 2^{\frac{\phi(m)}{2}} & \text{if } m \text{ is a prime power} \\ 2^{\frac{\phi(m)}{2}-1} & \text{otherwise.} \end{cases}$$

Proof: By lemma 2 and the remark above, we only must show that $[C_N : C_I^2] = 2$ when m is not a prime power. Let $\alpha = \Pi_{i=1}^{m-1}[(1-\xi^i)(1-\xi^{-i})]^{a_i} \in C_N$. If m is odd then $\beta = \xi^{-\Sigma_{i=1}^{m-1} \frac{i a_i}{2}} \cdot \Pi_{i=1}^{m-1}(1-\xi^i)^{a_i} \in K_m$. Moreover, if $\Sigma_{i=1}^{m-1} a_i \equiv 0$ (mod 2), then $\beta \in C_I$ and $\alpha = \beta^2 \in C_I^2$. But if $\Sigma_{i=1}^{m-1} a_i \equiv 1 \pmod 2$. Then we take $\alpha = (1-\xi)(1-\xi^{-1}) \cdot \alpha'$, where $\alpha' = \Pi_{i=1}^{m-1}[(1-\xi^i)(1-\xi^{-i})]^{b_i}$, with $\Sigma_{i=1}^{m-1} b_i \equiv 0$ (mod 2) and $\alpha' \in C_N$ because α and $(1-\xi)(1-\xi^{-1})$ do. So $\alpha \in (1-\xi)(1-\xi^{-1})C_I^2$. Now we suppose m even. If $\Sigma_{i=1}^{m-1} i a_i \equiv 0 \pmod 2$ then $\beta = \xi^{-\Sigma_{i=1}^{m-1} \frac{i a_i}{2}} \cdot \Pi_{i=1}^{m-1}(1-\xi^i)^{a_i} \in K_m$. If further $\Sigma_{i=1}^{m-1} a_i \equiv 0 \pmod 2$ then $\beta \in C_I$ and $\alpha \in C_I^2$. But if $\Sigma_{i=1}^{m-1} a_i \equiv 1 \pmod 2$ then $\beta = \xi^{\frac{m}{4}} \gamma$ with $\gamma \in C_I$, and $\alpha = \gamma^2 \in C_I^2$. If, on the other hand, $\Sigma_{i=1}^{m-1} i a_i \equiv 1$ (mod 2) we take $\alpha = (1-\xi)(1-\xi^{-1})\alpha'$; as before $\alpha \in (1-\xi)(1-\xi^{-1})C_I^2$. In both cases, m even or odd, we showed that $C_N \subseteq C_I^2 \cup (1-\xi)(1-\xi^{-1})C_I^2$. So, to complete the proof, we need only to show that $(1-\xi)(1-\xi^{-1}) \notin C_I^2$. Since $(1-\xi)(1-\xi^{-1}) = -\xi^{-1}(1-\xi)^2$, if $(1-\xi)(1-\xi^{-1}) \in C_I^2$ then $-\xi^{-1} \in \dot{K}_m^2$, that is,

$-\xi^{-1} = (\pm\xi^t)^2$, for some t, and so $-1 = \xi^{2t+1}$. This implies that m is even and m divides $2(2t+1)$, which is a contradiction, because $m \not\equiv 2 \pmod 4$.

Corollary: The group C_N is a proper subgroup of $S(K_m^+)$.

References

[1] K. Rubin, Global Units and Ideal Class Groups, Invent. Math. 89, 511–526 (1987).

[2] P. Samuel, Théorie Algebrique des Nonbres, Hermann Paris (1967).

[3] L. C. Washington, Intoduction to Cyclotomic Fields Graduate Texts in Mathematics, Springer–Verlag, New York (1982).

Trajano Nóbrega
Departamento de Matemática / UNESP
15055 - São José do Rio Preto – SP
Brazil.

Received February 8, 1990
in revised form July 16, 1990

THE MEAN VALUE OF $|\zeta(\frac{1}{2}+it)|^2$ AT THE ZEROS OF $Z^{(k)}(t)$

C. Yalcin Yildirim

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

Introduction. The functional equation of the Riemann zeta-function may be expressed in the asymmetric form

$$(1) \qquad \zeta(1-s) = \chi(1-s)\zeta(s)\,; \qquad \chi(1-s) = \pi^{\frac{1}{2}-s}\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}, \qquad s \in \mathbb{C}\,.$$

The real function $Z(t)$ is defined as

$$(2) \qquad Z(t) = \{\chi(\frac{1}{2}+it)\}^{-\frac{1}{2}}\zeta(\frac{1}{2}+it)$$

and we put

$$(3) \qquad Z_k(s) = \big(\chi(s)\big)^{\frac{1}{2}}\frac{d^k}{ds^k}\big(\chi(s)\zeta(s)\big)$$

so that $|Z_k(\frac{1}{2}+it)| = |Z^{(k)}(t)|$.

In [1] Conrey and Ghosh proved on the Riemann Hypothesis (RH) that $\sum_{0<\gamma_1\le T}|\zeta(\frac{1}{2}+i\gamma_1)|^2 \sim \frac{e^2-5}{2}\frac{TL^2}{2\pi}$. Here $\frac{1}{2}+i\gamma_1$ runs through the zeros of $Z_1(s)$ ($|\zeta(\frac{1}{2}+i\gamma_1)|$ is a maximum on $\operatorname{Re} s = \frac{1}{2}$) and $L = \log\frac{T}{2\pi}$. They also stated on RH $\sum_{0<\gamma_1\le T}|\zeta(\frac{1}{2}+i\gamma_1+i\frac{2\pi\alpha}{L})|^2 \sim C(\alpha)\frac{TL^2}{2\pi}$ giving $C(\alpha)$ explicitly and deduced that the gaps between the maxima of $\zeta(s)$ can be 1.4 times the expected average. In this paper we prove the following extension of this result.

Theorem. *Assume RH and let k be a fixed natural number. Let γ_k run through the zeros of $Z^{(k)}(t)$ (i.e. $Z_k(\frac{1}{2}+i\gamma_k)=0$). Then as $T\to\infty$:*

$$\sum_{0<\gamma_k<T}|\zeta(\frac{1}{2}+i\gamma_k+i\frac{2\pi\alpha}{L})|^2 = \frac{TL^2}{2\pi}\Big\{1+2(k+1)\frac{\cos 2\pi\alpha-1}{(2\pi\alpha)^2} + 2\operatorname{Re}\sum_{j=1}^{k}\frac{e^{-u_j}-u_j-1}{u_j^2}\Big\} + O_k(TL)$$

$$\sim \frac{TL^2}{2\pi}c_k(\alpha)\,, \quad \text{say,}$$

where $u_j = -2\nu_j + 2\pi\alpha i$ and ν_j is a zero of the k-th partial sum for the exponential function, i.e.: $1+\nu_j+\frac{\nu_j^2}{2!}+\cdots+\frac{\nu_j^k}{k!}=0 \qquad (j=1,2,\ldots,k)$.

Assuming RH, $Z(t)$ has asymptotically $\frac{T}{2\pi}\log T$ zeros in $[0,T]$ as $T \to \infty$. By repeated application of Rolle's theorem the same is true of $Z^{(k)}(t)$. Comparison with the classical result $\int_0^T |\zeta(\frac{1}{2}+it)|^2 dt \sim T\log T$ (see [4], Ch. 7) makes it clear that the average of $|\zeta(\frac{1}{2}+i\gamma_k)|^2$ over the zeros, $\gamma_k \in [0,T]$, of $Z^k(t)$ is $c_k(0)$ times the average of $|\zeta(\frac{1}{2}+it)|^2$ over all $t \in [0,T]$. The sum over the zeros of partial sums of e^z has been evaluated in [6] as

$$\sum_{j=1}^{k} \frac{e^{-2\nu_j}+2\nu_j-1}{\nu_j} = \begin{cases} 2k+2+\frac{2}{k}+O(\frac{\log k}{k^2}) & (k \text{ odd and } k>1) \\ 2k+2-\frac{6}{k}+O(\frac{\log k}{k^2}) & (k \text{ even}). \end{cases} \tag{4}$$

Using (4) in the Theorem we have

Corollary. $$\sum_{0<\gamma_k<T} |\zeta(\tfrac{1}{2}+i\gamma_k)|^2 \sim \begin{cases} \frac{TL^2}{2\pi}(1+\frac{1}{k}+O(\frac{\log k}{k^2})) & (k \text{ odd and } k>1) \\ \frac{TL^2}{2\pi}(1-\frac{3}{k}+O(\frac{\log k}{k^2})) & (k \text{ even}) \end{cases}$$

From the Theorem we may compute values for β_k such that for all sufficiently large T there exists γ_k and γ_k^+, consecutive zeros of $Z^{(k)}(t)$ with $T<\gamma_k<\gamma_k^+ \le 2T$ and $\gamma_k^+-\gamma_k>\beta_k\frac{2\pi}{L}$. The computation is based on determining β_k such that $\int_{-\beta_k/2}^{\beta_k/2} c_k(\alpha)d\alpha = 1$.

A table of the values of $c_k(0)$ and β_k for $1 \le k \le 28$ has been given in [5]. As k increases β_k decreases monotonically. Some sample values are $\beta_1 = 1.4$, $\beta_2 = 1.295$, $\beta_3 = 1.224$, $\beta_{28} = 1.035$.

Preliminaries. In this section we present the lemmas that will be used in the proof. The constants implied by $\ll$ or O symbols may, in general, depend on k but we suppress this in our notation as k is a fixed integer and $T \to \infty$.

Lemma 1. *The function $\chi(s)$ defined in (1) satisfies in $|\text{Im } s| = |t| \ge 1$*
$\frac{\chi'}{\chi}(s) = -\log\frac{|t|}{2\pi} + O\left(\frac{1}{1+|t|}\right)$ *and* $\left(\frac{\chi'}{\chi}(s)\right)^k \ll \frac{1}{1+|t|}$ $(k \ge 1)$.

For the proof see [3].

By differentiating (1) k times the functional equation of $Z_k(s)$ is obtained:

Lemma 2. $Z_k(s) = (-1)^k\chi(s)Z_k(1-s)$ *for all* $s \in \mathbb{C}$.

Lemma 3. *Assuming RH, $Z_k(s)$ has at most $O(\log T)$ zeros with ordinates in [0,T] off the critical line.*

Lemma 3 is shown in the same way as in the case $k = 1$ (see [1] or [5]).

Lemma 4. *Assuming R.H., the zeros of $Z_k(s)$ which are not on $\sigma = \frac{1}{2}$ are within a distance $\frac{1}{9}$ from $\sigma = \frac{1}{2}$.*

Proof. On R.H. $\frac{\zeta^{(j)}}{\zeta}(s) \ll (\log t)^{j+1-2\sigma}$ uniformly for $\frac{1}{2} \le \sigma_0 < \sigma \le \sigma_1 < 1$ and $t \ge 2$. The case $j = 1$ is Theorem 14.5 of Titchmarsh [4], and applying Cauchy's theorem in a disk of radius $(\log \frac{t}{2\pi})^{-1}$ around s the bound for $\frac{\zeta^{(j)}}{\zeta}(s)$ for $j > 1$ is obtained. Thus $\frac{Z_k}{\zeta}(s) \ll (\log t)^{k+1-2\sigma} + (\log t)^k$ (cf. Eq. (3)) and the assertion follows immediately.

Lemma 5. *Let $\mathcal{Z}_k(s,T) = \left(\frac{L}{2} + \frac{d}{ds}\right)^k \zeta(s)$, where $L = \log \frac{T}{2\pi}$. Assuming R.H.,*

$$\frac{Z_k'}{Z_k}(s) - \frac{\mathcal{Z}_k'}{\mathcal{Z}_k}(s,T) \ll \frac{U}{T}.$$

for $\sigma \ge \frac{5}{8}$ and $T \le t \le T + U \le 2T$.

Proof. In [1] it was proved upon R.H. that $\frac{Z_1'}{Z_1}(s) - \frac{\mathcal{Z}_1'}{\mathcal{Z}_1}(s,T) \ll \frac{U}{T}$ and the result can be proved by induction on k (see [5]).

Lemma 6. *Assume R.H. At $s = 1$ $\mathcal{Z}_k(s,T)$ has a pole of order $k+1$. There are k zeros of $\mathcal{Z}_k(s,T)$ located at $z_j = 1 - \frac{2}{L}\nu_j + O_k\left(\frac{1}{L^2}\right)$ $(j = 1, \ldots, k)$, where ν_j's are the roots of $\sum_{r=0}^{k} \frac{\nu^r}{r!} = 0$. There are no other zeros or poles of $\mathcal{Z}_k(s,T)$ with $\frac{5}{8} \le \sigma \le 2$. Thus we have*

$$\frac{\mathcal{Z}_k'}{\mathcal{Z}_k}(s - i\delta) = \frac{-(k+1)}{s - i\delta - 1} + \sum_{j=1}^{k} \frac{1}{s - i\delta - z_j} + W(s,T)$$

where $W(s,T)$ is regular for $\frac{5}{8} \le \sigma \le \frac{9}{8}$.

Proof. The statement about the poles follows from the facts that $\zeta^{(k)}(s)$ has a pole of order $k+1$ at $s = 1$ and $\zeta(s)$ and its derivatives don't have poles in $\sigma \ge \frac{5}{8}$. Since we assume R.H. we may consider $W_k(s) =: \left(\frac{2}{L}\right)^k \frac{\mathcal{Z}_k(s,T)}{\zeta(s)} = \sum_{j=0}^{k} \binom{k}{j} \frac{\zeta^{(j)}}{\zeta}(s) \left(\frac{2}{L}\right)^j$.

The change in the argument of $W_k(s)$ along the rectangle with vertices $2 \pm iT$ and $\frac{5}{8} \pm iT$ is 0 because, for $1 \le j \le k$, $\frac{1}{L^j} \frac{\zeta^{(j)}}{\zeta}(s) = o(L)$ on this rectangle. By the argument principle the number of zeros of $W_k(s)$ is equal to the number of its poles counted according to multiplicity and the latter is k.

Let now $\eta = 1 - \frac{2}{L}\mu$. Since $\frac{\zeta^{(j)}}{\zeta}(\eta) = \frac{(-1)^j j!}{(\eta-1)^j} + \sum_{n=-(j-1)}^{\infty} C_{jn}(\eta-1)^n$, where C_{jn} are constants, we have

$$W_k(\eta) = \sum_{j=0}^{k} \binom{k}{j}\mu^{-j}j! + \sum_{j=0}^{k} \binom{k}{j}\left(\frac{2}{L}\right)^j \sum_{n=-(j-1)}^{\infty} C_{jn}\left(\frac{-2}{L}\mu\right)^n$$

so that if $W_k(\eta) = 0$ then $\mu = \nu + O(\frac{1}{L})$ where $\sum_{r=0}^{k} \frac{\nu^r}{r!} = 0$. Hence we conclude that $Z_k(s,T)$ has k zeros located at $z_j = 1 - \frac{2}{L}\nu_j + O(\frac{1}{L^2})$; $j = 1, \ldots, k$.

Lemma 7. *For $\sigma \geq \frac{9}{8}$, there is an absolutely convergent Dirichlet series such that*

$$\frac{Z_k'}{Z_k}(s,T) = \sum_{m=1}^{\infty} \frac{a_k(m)}{m^s} + O(T^{-1})$$

where, as $T \to \infty$, for any $\epsilon > 0$ $a_k(m) = a_k(m,L) \ll_\epsilon T^\epsilon$ for $m \ll T$.

This result has been proved in [2].

We quote the last lemma from Gonek [3]:

Lemma 8. *Let $\{b_n\}_{n=1}^{\infty}$ be a sequence of complex numbers such that for any $\varepsilon > 0$, $b_n \ll n^\epsilon$. Let $\sigma > 1$ and let j be a non-negative integer. Then for sufficiently large T*

$$\frac{1}{2\pi}\int_1^T \left(\sum_{m=1}^{\infty} b_n n^{-\sigma-it}\right)\chi(1-\sigma-it)\left(\log\frac{t}{2\pi}\right)^j dt = \sum_{1\leq n\leq \frac{T}{2\pi}} b_n(\log n)^j + O\left(T^{\sigma-\frac{1}{2}}(\log T)^j\right).$$

Proof of the Theorem. As the real part of the zeros of $Z_k(s)$ are in $(\frac{1}{2}-\frac{1}{9}, \frac{1}{2}+\frac{1}{9})$ (Lemma 4) the residue theorem allows us to write

$$\sum_{\substack{\rho_k=\beta_k+i\gamma_k \\ T<\gamma_k<T+U}} \zeta(\rho_k+i\delta)\zeta(1-\rho_k-i\delta) = \frac{1}{2\pi i}\int_R \frac{Z_k'}{Z_k}(s)\zeta(s+i\delta)\zeta(1-s-i\delta)ds ,$$

where we take R to be the rectangle with vertices $\frac{5}{8}+iT$, $\frac{5}{8}+i(T+U)$, $\frac{3}{8}+i(T+U)$, $\frac{3}{8}+iT$, described in the positive sense.

On R.H., by Lemmas 3 and 4, only $O(L)$ of the zeros of $Z_k(s)$ are off the critical line and for such zeros ρ_k to the right of $\sigma = \frac{1}{2}$ $|\zeta(\rho_k)|^2 \ll T^{\frac14}$. Thus

$$(5) \quad \sum_{\substack{\rho_k = \frac12 + i\gamma_k \\ T<\gamma_k<T+U}} \left|\zeta(\tfrac{1}{2} + i\gamma_k + i\delta)\right|^2 = \frac{1}{2\pi i} \int_R \frac{Z_k'}{Z_k}(s)\zeta(s+i\delta)\zeta(1-s-i\delta)ds + O(T^{\frac14}L) .$$

We can assume without loss of generality that the contour R is at a distance $\gg L^{-1}$ from the zeros of $Z_k(s)$. Then the integral along the horizontal sides is $\ll T^{\frac12}$ and it can be absorbed into the last error term. Using the functional equations of $\zeta(s)$ and $\frac{Z_k'}{Z_k}(s)$, Lemma 1 and the well-known result $\int\limits_T^{T+U} \left|\zeta(\frac12 + it)\right|^2 dt = UL + O(U) + O(T^{\frac12+\epsilon})$ (see Theorem 7.4 [4]), with $U = T^{\frac34}$, (5) is reduced to

$$(6) \quad \sum_{T<\gamma_k<T+U} |\zeta(\frac{1}{2} + i\gamma_k + i\delta)|^2 = \frac{1}{2\pi i} \int\limits_{\frac58+iT}^{\frac58+i(T+U)} \frac{Z_k'}{Z_k}(s)\big(\zeta(s+i\delta)\big)^2\chi(1-s-i\delta)ds$$

$$= 2\,\mathrm{Re}\, I + \frac{UL^2}{2\pi} + O(UL) , \qquad \text{say} .$$

In the integrand of I changing $\frac{Z_k'}{Z_k}(s)$ to $\frac{Z_k'}{Z_k}(s,T)$ (cf. Lemma 5), produces an error of $O\Big(U^2T^{\frac{-7}{8}+\epsilon}\Big)$. Next, in order to use the Dirichlet series approximation to $\frac{Z_k'}{Z_k}(s-i\delta,T)$ we move the integral to $\sigma = \frac98$ where the approximating series is absolutely convergent. Then by Lemma 7, estimating the integral on the horizontal sides trivially, we have

$$I = \frac{1}{2\pi i} \int\limits_{\frac98+iT}^{\frac98+i(T+U)} \sum_{m=1}^{\infty} \frac{a_k(m)m^{i\delta}}{m^s} \chi(1-s)\big(\zeta(s)\big)^2 ds + O(T^{\frac58}) + O(U^2T^{-\frac78+\epsilon}) .$$

Applying Lemma 8 we get

$$I = \sum_{\frac{T}{2\pi} \le mn \le \frac{T+U}{2\pi}} a_k(m)\, m^{i\delta} d(n) + O_\epsilon(T^{\frac58+\epsilon}) .$$

This sum is converted back to another integral via Perron's inversion formula so that

$$I = \left[\frac{1}{2\pi i} \int\limits_{\frac98-iT}^{\frac98+iT} \frac{Z_k'}{Z_k}(s-i\delta,T)\big(\zeta(s)\big)^2 ds \frac{x^s}{s} ds + O_\epsilon\left(x^{\frac98}T^{-1} + x^\epsilon\right)\right]\Bigg|_{x=\frac{T}{2\pi}}^{x=\frac{T+U}{2\pi}} + O_\epsilon(T^{\frac58+\epsilon}) .$$

The last integral can be evaluated using the residue theorem by carrying the line of integration to $\sigma = \frac{5}{8}$. The residues are calculated from the information in Lemma 6 and returning to (6) we obtain

$$\sum_{\substack{\rho_k = \frac{1}{2} + i\gamma_k \\ T < \gamma_k < T+U}} |\zeta(\tfrac{1}{2} + i\gamma_k + i\delta)|^2 = \frac{UL^2}{2\pi} \Big[1 + 2\mathrm{Re}\Big\{\sum_{j=1}^{k} \frac{e^{-2\nu_j + 2\pi\alpha i} - (-2\nu_j + 2\pi\alpha i) - 1}{(-2\nu_j + 2\pi\alpha i)^2}\Big\}$$
$$+ 2(k+1)\frac{\cos(2\pi\alpha) - 1}{(2\pi\alpha)^2}\Big] + O(UL)$$

where $\delta = \frac{2\pi\alpha}{L}$ with $|\alpha| \leq 2$, say. This is the desired result with $U = T^{\frac{3}{4}}$ from which the theorem is readily deduced.

References

[1] J.B. Conrey and A. Ghosh, A mean value theorem for the Riemann zeta-function at its relative extrema on the critical line, *J. London Math. Soc. (2)* **32** (1985), 193-202.

[2] J.B. Conrey and A. Ghosh, Zeros of derivatives of the Riemann zeta-function near the critical line, preprint.

[3] S.M. Gonek, Mean values of the Riemann zeta-function and its derivatives, *Invent. Math.* **75** (1984), 123-141.

[4] E.C. Titchmarsh, *The Theory of the Riemann Zeta-function* (2nd ed.), Oxford University Press, 1986.

[5] C.Y. Yildirim, Zeta function theory: Pair correlation and value distribution, Thesis, University of Toronto, 1990.

[6] C.Y. Yildirim, A sum over the zeros of partial sums of e^z, to appear.

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

Received July 16, 1990

DETERMINATION DU DEGRE OPTIMAL d_m DE MONOMORPHIE POUR LES STRUCTURES RELATIONNELLES AU PLUS m-AIRES.

par Claude FRASNAY

Presenté par P. Ribenboim, F.R.S.C.

Rappelons qu'une structure relationnelle $r = (E, (m_i)_{i\in I}, (r_i)_{i\in I})$ est un triplet tel que $0 \leqslant m_i < \omega$ et $r_i \subseteq E^{m_i}$ pour tout $i \in I$. Pour $0 \leqslant n < \omega$, un telle structure r est dite n-monomorphe si, quels que soient $X \subseteq E$ et $Y \subseteq E$ de cardinal $|X| = |Y| = n$, les deux restrictions $r|X$ et $r|Y$ sont isomorphes.

Pour $0 \leqslant m \leqslant \omega$ et $0 \leqslant p \leqslant \omega$, notons R_p^m la classe des structures relationnelles r d'arités $m_i \leqslant m$ et de cardinalité $|E| \geqslant p$. Pour $0 \leqslant q \leqslant \omega$, notons M_q la classe des structures relationnelles r qui sont n-monomorphes pour tout $n < q$. Par exemple, $R_0^\omega = M_0$ est la classe de toutes les structures relationnelles et, pour $m < \omega$, R_0^m est la classe des structures relationnelles au plus m-aires tandis que R_ω^m est la classe des structures relationnelles au plus m-aires de cardinalité infinie. Bien entendu, pour $m < \omega$, $p < \omega$, $q < \omega$, on a les inclusions $R_p^m \subseteq R_p^{m+1} \subseteq R_p^\omega$, $R_\omega^m \subseteq R_{p+1}^m \subseteq R_p^m$, $M_\omega \subseteq M_{q+1} \subseteq M_q$ et, pour abréger, on dit que $M_\omega = \bigcap_{n<\omega} M_n$ est la classe des structures relationnelles monomorphes.

En 1964, nous avons démontré pour les relations un théorème de compacité monomorphique que M. POUZET a étendu en 1976 aux structures relationnelles. Avec les notations ci-dessus, ce théorème prend la forme suivante : "Pour tout $m<\omega$, il existe $p<\omega$ et $q<\omega$ vérifiant la condition $R_p^m \cap M_q = R_p^m \cap M_\omega$ ". Plus précisément (pour m donné), si l'on note Δ_m l'ensemble des couples (p,q) vérifiant la condition précitée, $pr_2(\Delta_m)$ est un intervalle $[d_m, \rightarrow[$ qui définit le <u>degré optimal d_m de monomorphie</u> pour les structures relationnelles au plus m-aires. On peut lui associer de manière minimale un cardinal $p_m<\omega$ et ainsi, dès qu'une structure relationnelle r au plus m-aire et de cardinalité $\geq p_m$ est n-monomorphe pour tout $n\leq d_m$ alors cette structure r est n-monomorphe pour tout $n<\omega$.

Durant la période 1964-1984; les travaux ayant mené au calcul exact des valeurs d_m se décomposent de la manière suivante : en 1964-65, nous avons obtenu $d_0=0$, $d_1=1$, $d_2=3$, $d_3=4$ et $d_4=5$ ou 6, ainsi que l'encadrement $m+1\leq d_m\leq 9m^2$ pour $m\geq 5$. En 1977, W. HODGES, A.H. LACHLAN et S. SHELAH ont obtenu la très fine majoration $d_m\leq 2m-2$ pour $m\geq 5$. En 1983, P.J. CAMERON a pu trancher notre alternative sur d_4 en faveur de $d_4=6$. Enfin, en 1984, à l'occasion du Séminaire de Montréal consacré à l'Algèbre universelle et à la Théorie des relations, nous avons obtenu $d_m = 2m-2$ pour tout $m\geq 3$. En faisant intervenir (pour tout $x\in Q$) la partie entière $[x]\in Z$ ($[x] \leq x < [x]+1$) et la partie positive $x^+ = Max(0, x)$, on peut écrire pour tout $m<\omega$ la formule explicite : $d_m=2m-2+[2-\frac{m}{2}]^+$.

Comme $R_\omega^m \cap M_q = R_\omega^m \cap M_{q+1}$ pour tout $q \geq d_m$, il nous suffisait (pour obtenir $d_m > 2m-3$) de trouver pour $m \geq 3$ une relation m-aire de support ω qui soit n-monomorphe pour tout $n \leq 2m-3$ et qui ne soit pas $(2m-2)$-monomorphe. Pour celà, introduisons sur ω deux bons ordres α et β : α est le bon ordre usuel et β se déduit de α en intervertissant les éléments $m-2$, $m-1$, autrement dit

$$\begin{cases} 0<1<2<\ldots<m-3<m-2<m-1<m<\ldots & (\text{mod. } \alpha) \\ 0<1<2<\ldots<m-3<m-1<m-2<m<\ldots & (\text{mod. } \beta) \end{cases}$$

Posons $A = \{0,1,2,\ldots, 2m-3\}$, $B = \{1,2,3,\ldots, 2m-2\}$ et définissons une application $X \longmapsto a_X$ de $P_{2m-3}(\omega)$ sur A en posant $a_X = \operatorname{Min}_\alpha (A-X)$. Par exemple $a_X = 0$ pour tout $X \in P_{2m-3}(B)$, et $a_X = n$ pour $X \in P_{2m-3}(A)$, $X = A-\{n\}$.

Sur chaque $X \in P_{2m-3}(\omega)$ comme support, on introduit une chaîne θ_X de la manière suivante :

$$\begin{cases} \theta_X = \alpha|X \text{ pour } a_X \in \{0,1,2,\ldots,m-3\} \\ \theta_X = \alpha|X = \beta|X \quad \text{pour } a_X \in \{m-2,\ m-1\} \\ \theta_X = \beta|X \quad \text{pour } a_X \in \{m,\ m+1,\ldots,\ 2m-3\} \end{cases}$$

De manière générale, appelons <u>vibration m-aire</u> suscitée par une chaîne φ de support E et notons $v(\varphi)$ la relation m-aire de support E satisfaite par les m-uples $(x_0,x_1,x_2,\ldots,x_{m-1}) \in E^m$ vérifiant les trois conditions suivantes :

$$\begin{cases} \text{les } m \text{ éléments } x_0,x_1,\ldots,x_{m-1} \text{ sont deux à deux distincts} \\ x_0 \text{ minore } \{x_1,x_2,\ldots,x_{m-2}\} \quad (\text{mod. } \varphi) \\ x_{m-1} \text{ majore } \{x_1,x_2,\ldots,x_{m-2}\} \quad (\text{mod. } \varphi) \end{cases}$$

Pour les restrictions aux parties F de E et pour les images isomorphiques par les bijections $f : E \rightarrow E'$, on peut vérifier que $v(\varphi|F) = v(\varphi)|F$ et $v(\tilde{f}(\varphi)) = \tilde{f}(v(\varphi))$.

Revenant à la famille des chaînes $\theta_X(X \in P_{2m-3}(\omega))$, introduisons la famille des vibrations m-aires $v(\theta_X)$ et montrons que les relations m-aires $v(\theta_X)$ (de cardinalité $2m-3 \geq m$) sont deux à deux compatibles. Trois cas sont à envisager pour $X \in P_{2m-3}(\omega)$ et $Y \in P_{2m-3}(\omega)$ tels que $a_X \leq a_Y$ (mod. α) :

(1) $0 \leq a_X \leq a_Y \leq m-1$: alors $v(\theta_X) = v(\alpha|X) = v(\alpha)|X$ et $v(\theta_Y) = v(\alpha|Y) = v(\alpha)|Y$ sont compatibles.

(2) $m-2 \leq a_X \leq a_Y \leq 2m-3$: alors $v(\theta_X) = v(\beta|X) = v(\beta)|X$ et $v(\theta_Y) = v(\beta|Y) = v(\beta)|Y$ sont compatibles.

(3) $0 \leq a_X \leq m-3$ et $m \leq a_Y \leq 2m-3$: alors $v(\theta_X) = v(\alpha)|X$ et $v(\theta_Y) = v(\beta)|Y$. Comme $a_X \in \{0,1,2,\ldots,m-3\}-X$ et $\{0,1,2,\ldots,m-1\} \subseteq Y$, il est commode de partager Y en 4 parties $\{a_X\}$, Y_1, $\{m-2, m-1\}$, Y_2 (de cardinaux respectifs : 1, $m-3$, 2, $m-3$) en posant : $Y_1 = \{0,1,2,\ldots,m-3\}-\{a_X\}$ et $Y_2 = Y - \{0,1,2,\ldots,m-2, m-1\}$.

Dès lors : $X \cap Y \subseteq Y_1 \cup \{m-2, m-1\} \cup Y_2$. Si un m-uple $(x_0,x_1,\ldots,x_{m-1}) \in (X \cap Y)^m$ satisfait <u>l'une ou l'autre</u> des deux vibrations $v(\alpha)|X \cap Y$, $v(\beta)|X \cap Y$, alors nécessairement $x_0 \in Y_1$ et $x_{m-1} \in Y_2$, donc ce m-uple satisfait <u>l'une et l'autre</u>. Ainsi : $v(\alpha)|X \cap Y = v(\beta)|X \cap Y$ et les deux vibrations $v(\theta_X)$, $v(\theta_Y)$ sont encore compatibles dans ce cas.

Puisque les vibrations $v(\theta_X)$ sont deux à deux compatibles lorsque X parcourt $P_{2m-3}(\omega)$, il existe une et une seule relation m-aire r de support ω telle que : $v(\theta_X) = r|X$ pour tout $X \in P_{2m-3}(\omega)$. Puisque deux vibrations m-aires de même cardinalité finie sont isomorphes, il en résulte que r est n-monomorphe pour tout $n \leq 2m-3$. Par contre, montrons que les deux restrictions $r|A$ et $r|B$ (de cardinalité $2m-2$) ne sont pas isomorphes.

De manière générale, disons qu'une relation m-aire ρ de support E est jointive et (plus précisément) qu'un élément $u \in E$ est un joint pour ρ dès qu'il existe deux m-uples $(x_0, x_1, \ldots, x_{m-1}) \in E^m$ et $(y_0, y_1, \ldots, y_{m-1}) \in E^m$ satisfaisant tous les deux la relation ρ et tels que $u = x_{m-1} = y_0$. Il est clair que toute image isomorphique d'une relation jointive est une relation jointive.

Or $r|A$ est une relation jointive puisque A contient (comme parties de cardinal 2m-3) :

$$X = A - \{m-3\} = \{0, 1, \ldots, m-4, m-2, m-1, m, \ldots, 2m-3\}$$

et $$Y = A - \{m\} = \{0, 1, \ldots, m-4, m-3, m-2, m-1, \ldots, 2m-3\}$$

pour lesquelles $a_X = m-3$ et $a_Y = m$. Ainsi $r|X = v(\alpha)|X$ est satisfaite par $(m-2, m-1, m, \ldots, 2m-3)$ et $r|Y = v(\beta)|Y$ est satisfaite par $(0, 1, \ldots, m-3, m-1, m-2)$, donc $u = m-2$ est un joint pour la relation $r|A$.

Par contre, puisque $a_X = 0$ pour tout $X \in P_{2m-3}(B)$, il en résulte $r|X = v(\alpha)|X$, donc $r|B = v(\alpha)|B = v(\alpha|\beta)$ est une vibration m-aire de cardinalité 2m-2. Or une telle relation ne peut être jointive : en effet s'il existe un joint $u = x_{m-1} = y_0$ pour une vibration m-aire $v(\varphi)$ de support E, cet élément u majore strictement une (m-1)-partie $\{x_0, x_1, \ldots, x_{m-2}\}$ de E et minore strictement une (m-1)-partie $\{y_1, y_2, \ldots, y_{m-1}\}$ de E, ce qui impose $|E| \geqslant 2m-1$.

Ainsi $r|B$ est une relation m-aire non jointive alors que $r|A$ est une relation m-aire jointive : elles ne sont donc pas isomorphes et la relation r n'est pas (2m-2)-monomorphe.

Références :

P.J. CAMERON 1983 - Orbits of permutation groups on unordered sets (III-IV). Journal London Math. Soc. vol. 27, p. 229-247.

C. FRASNAY 1965 - Quelques problèmes concernant les ordres totaux et les relations monomorphes (thèse, Paris). Annales Institut Fourier, Grenoble, vol. 15, p. 415-524.

C. FRASNAY 1984 - Relations enchaînables, rangements et pseudo-rangements. Orders : Description and Roles, Pouzet-Richard édit., Annals of Discrete Math. 23, p. 235-268, North-Holland (Amsterdam).

W. HODGES, A.H. LACHLAN, S. SHELAH 1977 - Possible orderings of an indiscernible sequence. Bulletin London Math. Soc., vol. 9 p. 212-215.

M. POUZET 1976 - Application d'une propriété combinatoire des parties d'un ensemble aux groupes et aux relations. Zeitschrift Math. Logik Grundlag., vol. 150, p. 117-134.

Cette courte liste comprend uniquement les publications auxquelles nous avons fait allusion. La plus récente bibliographie (et la plus abondante) sur le sujet et son contexte se trouve dans l'ouvrage suivant :

R. FRAISSE 1985 - Theory of Relations. Studies in Logic and the Foundations of Mathematics, vol. 118, North-Holland (Amsterdam).

Reçu le 27 juin 1990

FRASNAY CLAUDE
84 CHEMIN.DE BESSAYRE
31240 ST-JEAN (France)

Mailing Addresses

1.	W. Banaszczyk	Institute of Mathematics University of Lódź ul. S. Banach, 22 90-238 Lódź, Poland
2.	H. Ben-El-Mechaieckh	Department of Mathematics Brock University St. Catharines, Ontario, Canada L2S 3A1
3.	C. Frasnay	84, Chemin de Bessayre 31240 St-Jean, France
4.	Y. Hellegouarch	Université de Caen F-1400 Caen, France
5.	J. Mala	Department of Mathematics Teacher's Training College H-4401, Nyiregyháza, Hungary
6.	R.A. Mollin	Department of Mathematics and Statistics University of Calgary Calgary, Alberta, Canada T2N 1N4
7.	T. Nóbrega	Departamento de Matemática / UNESP 15055 - Sao José do Rio Preto - SP Brazil
8.	M.M. Parmenter	Department of Mathematics Memorial University St. John's, Newfoundland, Canada A1C 5S7
9.	A. Száz	Institute of Mathematics Lajos Kossuth University H-4010 Debrecen, Hungary
10.	C.Y. Yildirim	Department of Mathematics University of Toronto Toronto, Ontario, Canada M5S 1A1