

---

SEPTEMBER / SEPTEMBRE 2000

---

IN THIS ISSUE / DANS CE NUMÉRO

- 97 Amir Akbary  
Average values of symmetric square  $L$ -functions at  $\Re(s) = 2$
- 105 Nobuhiro Terai  
A remark on a conjecture concerning Eisenstein numbers
- 111 Michael S. Bingham  
Approximate Martingale central limit theorems on Hilbert space
- 118 Simeon Reich and Alexander J. Zaslavski  
Almost all nonexpansive mappings are contractive
- 125 A. Pianzola  
Line bundles and conjugacy theorems for toroidal Lie algebras

22

No 3

## AVERAGE VALUES OF SYMMETRIC SQUARE $L$ -FUNCTIONS AT $\operatorname{Re}(s) = 2$

AMIR AKBARY

Presented by M. Ram Murty, FRSC

RÉSUMÉ. Soit  $L_{\text{sym}^2(f)}(s)$  la fonction  $L$  du carré symétrique d'une forme primitive de poids 2 et niveau  $N$ . Pour  $N$  premier, on dérive une formule asymptotique pour les valeurs moyennes de  $L_{\text{sym}^2(f)}(s)$  en un point général de la droite  $\operatorname{Re}(s) = 2$  et  $f$  variant dans l'ensemble des formes primitives normalisées.

**1. Introduction.** Many important theorems of number theory are intimately connected with the values of various  $L$ -functions at the edge of their critical strips. For example, the distribution of prime numbers in arithmetic progressions is related to the non-vanishing of Dirichlet  $L$ -functions on the line  $\operatorname{Re}(s) = 1$ . Another famous example is Dirichlet's class-number formula. Here we are interested in a similar situation in the context of modular  $L$ -functions.

Let  $S_2(N)$  be the space of cusp forms of weight 2 for  $\Gamma_0(N)$  with trivial character. The space  $S_2(N)$  has an inner product (Peterson inner product)

$$\langle f, g \rangle = \int_{\Gamma_0(N) \backslash \mathcal{H}} f(z) \overline{g(z)} dx dy$$

where  $\mathcal{H}$  denotes the upper half plane. For  $f \in S_2(N)$  let

$$f(z) = \sum_{n=1}^{\infty} a_f(n) e(nz), \quad e(z) = e^{2\pi iz}$$

be the Fourier expansion of  $f$  at  $i\infty$  and let  $\mathcal{F}_N$  be the set of all normalized ( $a_f(1) = 1$ ) newforms in  $S_2(N)$ .

The *symmetric square  $L$ -function* associated to  $f \in \mathcal{F}_N$  is defined (for  $\operatorname{Re}(s) > 2$ ) by

$$(1) \quad L_{\text{sym}^2(f)}(s) = \zeta_N(2s - 2) \sum_{n=1}^{\infty} \frac{a_f(n^2)}{n^s} = \sum_{\substack{d, e \\ (d, N)=1}} \frac{a_f(e^2)}{d^{2s-2} e^s}$$

---

Received by the editors June 10, 1999.

Research partially supported by Concordia General Research Funds.

AMS subject classification: 11F67.

© Royal Society of Canada 2000.

where  $\zeta_N(s)$  is the Riemann zeta function with the Euler factors corresponding to  $p|N$  removed. It is known that  $L_{\text{sym}^2(f)}(s)$  extends to an entire function (see [4]) and for square free  $N$ , it satisfies a functional equation of the form

$$(2) \quad R(s) = A^s \Gamma\left(\frac{s}{2}\right)^2 \Gamma\left(\frac{s+1}{2}\right) L_{\text{sym}^2(f)}(s) = R(3-s), \quad A = \frac{N}{\pi^{\frac{3}{2}}}.$$

Similar to Dirichlet's class number formula the value of  $L_{\text{sym}^2(f)}(s)$  at the edge of the critical strip (in this case  $s = 2$ ) is of interest. One can show that  $L_{\text{sym}^2(f)}(2)$  is a constant multiple (depending on  $N$ ) of the Petersson inner product of  $f$  and  $f$ , more precisely

$$(3) \quad L_{\text{sym}^2(f)}(2) = \frac{8\pi^3 \phi(N)}{N^2 \prod_{p|N} (1 - \frac{1}{p})} \langle f, f \rangle$$

where  $\phi$  is the Euler totient function. Therefore to study the average values of the Petersson inner product when  $f$  varies in  $\mathcal{F}_N$ , it is enough to find an asymptotic formula for the average values of  $L_{\text{sym}^2(f)}(2)$ . In the case that  $N$  is prime and  $L_{\text{sym}^2(f)}(s)$  satisfies the Lindelöf hypothesis, R. Murty [3] has proved:

**THEOREM.** *If we assume that  $L_{\text{sym}^2(f)}(\frac{3}{2} + it) \ll (N|t|)^\theta$ , for some  $\theta > 0$ , then for  $N$  prime*

$$\sum_{f \in \mathcal{F}_N} L_{\text{sym}^2(f)}(2) = \frac{N}{12} \zeta^2(2) + O(N^{\frac{7}{10} + \frac{1}{5}\theta} \log^3 N).$$

In this note we develop a similar asymptotic formula which works unconditionally. Also our method enables us to derive asymptotic formulae for average values of symmetric square  $L$ -functions at a general point in the line  $\text{Re}(s) = 2$ . The main observation is a modification of Murty's approximate trace formula (Proposition 1). We employ the recent method of Kowalski (see [2, Section 3. 5]) to obtain this.

**2. An approximate trace formula.** In this section we will derive an asymptotic formula for  $\sum_{f \in \mathcal{F}_N} a_f(n)$  in terms of  $N$ . Let  $T$  and  $S$  be positive and non-integer. We start by considering the integral

$$\frac{1}{2\pi i} \int_{(1)} L_{\text{sym}^2(f)}(s+2) T^s \frac{ds}{s} = \sum_{\substack{d^2 e < T \\ (d, N)=1}} \frac{a_f(e^2)}{d^2 e^2} = \sum_{n < T} \frac{g_f(n)}{n^2}$$

(see (1)). Upon moving the line of integration from 1 to  $-2$  and using the functional equation (2), this integral is

$$= L_{\text{sym}^2(f)}(2) + \frac{1}{A} \frac{1}{2\pi i} \int_{(-2)} \frac{\Gamma(\frac{1-s}{2})^2 \Gamma(\frac{2-s}{2})}{\Gamma(\frac{s+2}{2})^2 \Gamma(\frac{s+3}{2})} L_{\text{sym}^2(f)}(1-s) \left(\frac{T}{A^2}\right)^s \frac{ds}{s}.$$

Since  $A = \frac{N}{\pi^{\frac{1}{2}}}$  and  $L_{\text{sym}^2(f)}(s)$  is absolutely convergent for  $\text{Re}(s) > 2$ , this identity implies that

$$\begin{aligned}
 L_{\text{sym}^2(f)}(2) &= \sum_{\substack{d^2 e < T \\ (d, N)=1}} \frac{a_f(e^2)}{d^2 e^2} + O\left(\frac{N^3}{T^2}\right) \\
 (4) \qquad \qquad &= \sum_{\substack{d^2 e < S \\ (d, N)=1}} \frac{a_f(e^2)}{d^2 e^2} + \omega(S, T) + O\left(\frac{N^3}{T^2}\right)
 \end{aligned}$$

where  $\omega(S, T) = \sum_{S \leq n < T} \frac{g_f(n)}{n^2}$ .

We use the following three lemmas to get some information about  $\sum_{f \in \mathcal{F}_N} \frac{L_{\text{sym}^2(f)}(2)}{4\pi\langle f, f \rangle} a_f(n)$ .

LEMMA 1.

$$\sum_{f \in \mathcal{F}_N} \frac{1}{4\pi\langle f, f \rangle} a_f(m) a_f(n) = \delta_{mn} \sqrt{m} \sqrt{n} + O(N^{-\frac{3}{2}}(m, n)^{\frac{1}{2}} mn).$$

PROOF. See [3, Proposition 1]. ■

LEMMA 2.

$$\sum_{f \in \mathcal{F}_N} \frac{1}{4\pi\langle f, f \rangle} \sum_{\substack{d^2 e < S \\ (d, N)=1}} \frac{a_f(e^2)}{d^2 e^2} a_f(n) = (\zeta_N(2) + S^{-\frac{1}{2}} n^{\frac{1}{4}}) \delta_{n=\square} + O(N^{-\frac{3}{2}} n \mathbf{d}(n) S)$$

where  $\mathbf{d}(n)$  is the number of divisors of  $n$  and  $\delta_{n=\square} = 1$  if  $n$  is a square and is zero otherwise.

PROOF. This follows from Lemma 1 and familiar estimates of analytic number theory, see [3, p. 272] for details. ■

LEMMA 3. For any positive integer  $r$ , we have

$$\sum_{f \in \mathcal{F}_N} \frac{1}{4\pi\langle f, f \rangle} \omega(S, T) a_f(n) \ll (\mathbf{d}(n) \sqrt{n} (\log N)^{\frac{1}{2r}} N^{-\frac{1}{2r}}) \left( \sum_{f \in \mathcal{F}_N} (\omega(S, T))^{2r} \right)^{\frac{1}{2r}}.$$

PROOF. From the Hölder inequality, for any  $r$  and  $s$  that  $\frac{1}{2r} + \frac{1}{s} = 1$ , we have

$$\begin{aligned}
 \sum_{f \in \mathcal{F}_N} \frac{1}{4\pi\langle f, f \rangle} \omega(S, T) a_f(n) \\
 \leq \left( \sum_{f \in \mathcal{F}_N} (\omega(S, T))^{2r} \right)^{\frac{1}{2r}} \left( \sum_{f \in \mathcal{F}_N} \left( \frac{1}{4\pi\langle f, f \rangle} |a_f(n)| \right)^s \right)^{\frac{1}{s}}.
 \end{aligned}$$

Since  $|a_f(n)| \leq \mathbf{d}(n)\sqrt{n}$  (Deligne's bound) and  $\frac{1}{4\pi\langle f, f \rangle} \ll \frac{\log N}{N}$  (see [1, Proposition 4]), we have

$$\begin{aligned} & \left( \sum_{f \in \mathcal{F}_N} \left( \frac{1}{4\pi\langle f, f \rangle} |a_f(n)| \right)^s \right)^{\frac{1}{s}} \\ &= \left( \sum_{f \in \mathcal{F}_N} \left( \frac{1}{4\pi\langle f, f \rangle} |a_f(n)| \right)^{s-1} \left( \frac{1}{4\pi\langle f, f \rangle} |a_f(n)| \right) \right)^{\frac{1}{s}} \\ &\ll \left( \frac{\mathbf{d}(n)\sqrt{n} \log N}{N} \right)^{\frac{1}{2r}} (\mathbf{d}(n)\sqrt{n})^{\frac{1}{s}} = \mathbf{d}(n)\sqrt{n}(\log N)^{\frac{1}{2r}} N^{-\frac{1}{2r}}. \end{aligned}$$

■

Now we can state and prove the main result of this section.

**PROPOSITION 1.** *For prime  $N$ , we have*

$$\sum_{f \in \mathcal{F}_N} a_f(n) = \frac{N-1}{12} \delta_{n=\square} + O(N^{-\frac{1}{2}+\delta} n \mathbf{d}(n) + \sqrt{n} \mathbf{d}(n) N^{1-\frac{1}{2r}} (\log N)^C)$$

where  $0 < \delta < 1$ ,  $r \geq \frac{11}{8}$  is an integer,  $C > 0$  is a constant depending on  $\delta$  and  $r$ .

**PROOF.** From (3) and (4) we get

$$\begin{aligned} \sum_{f \in \mathcal{F}_N} a_f(n) &= \sum_{f \in \mathcal{F}_N} \frac{L_{\text{sym}^2(f)}(2)}{L_{\text{sym}^2(f)}(2)} a_f(n) \\ &= \frac{N}{2\pi^2} \left( \sum_{\substack{d^2 e < S \\ (d, N)=1}} \frac{1}{d^2 e^2} \sum_{f \in \mathcal{F}_N} \frac{1}{4\pi\langle f, f \rangle} a_f(e^2) a_f(n) \right. \\ &\quad \left. + \sum_{f \in \mathcal{F}_N} \frac{1}{4\pi\langle f, f \rangle} \omega(S, T) a_f(n) \right) + O\left(\frac{N^4}{T^2} \mathbf{d}(n)\sqrt{n}\right). \end{aligned}$$

Now by applying Lemmas 2 and 3 this expression becomes

$$\begin{aligned} & \left( \frac{N-1}{12} + \frac{N-1}{12N} + \frac{N}{2\pi^2} S^{-\frac{1}{2}} n^{\frac{1}{4}} \right) \delta_{n=\square} + O\left(N^{-\frac{1}{2}} n \mathbf{d}(n) S\right) \\ (5) \quad & + O(\mathbf{d}(n)\sqrt{n}(\log N)^{\frac{1}{2r}} N^{1-\frac{1}{2r}}) \left( \sum_{f \in \mathcal{F}_N} (\omega(S, T))^{2r} \right)^{\frac{1}{2r}} + O\left(\frac{N^4}{T^2} \mathbf{d}(n)\sqrt{n}\right). \end{aligned}$$

Let  $0 < \delta < 1$  and let  $S = N^\delta$ , choose  $r \geq \frac{11}{8}$ , then from [2] (see Lemma 4, p. 64), we know that for  $T < N^{10}$

$$\left( \sum_{f \in \mathcal{F}_N} (\omega(S, T))^{2r} \right)^{\frac{1}{2r}} \ll (\log N)^D$$

where  $D$  is a positive number which depends on  $\delta$ . Applying this inequality in (5) and choosing  $T$  a non-integer bigger than  $N^3$  in (5) yields the result. ■

**3. Mean estimate.** In the following lemma we give a representation of  $L_{\text{sym}^2(f)}(s_0)$  as a sum of two absolutely convergent series.

LEMMA 4. For any  $x > 0$  and  $s_0 = \sigma_0 + it_0 \in \mathbb{C}$  where  $\sigma_0 \geq \frac{3}{2}$ , let  $\sigma_0 < \eta$  and

$$W(s_0, x) = \frac{1}{2\pi i} \int_{(\eta)} \pi^{-\frac{3}{2}s} \Gamma\left(\frac{s+s_0}{2}\right)^2 \Gamma\left(\frac{s+s_0+1}{2}\right) x^s \frac{ds}{s},$$

$$I_f(s_0, x) = \sum_{\substack{d, c \\ (d, N)=1}} \frac{a_f(e^2)}{e^{\sigma_0 d} d^{2\sigma_0-2}} W\left(s_0, \frac{x}{d^2 e}\right)$$

where  $f \in \mathcal{F}_N$ . Then we have

$$\Gamma\left(\frac{s_0}{2}\right)^2 \Gamma\left(\frac{s_0+1}{2}\right) L_{\text{sym}^2(f)}(s_0) = I_f(s_0, x) + \left(\frac{\pi^{\frac{3}{2}}}{N}\right)^{2s_0-3} I_f\left(3-s_0, \frac{N^2}{x}\right).$$

PROOF. It is similar to the proof of Lemma 3 in [1].

Now we evaluate the values of  $L_{\text{sym}^2(f)}(s_0)$  on average, where  $f$  ranges over all newforms of weight 2 and level  $N$ . From Lemma 4 with  $x = N$  and Proposition 1, we have

$$\begin{aligned} & \sum_{f \in \mathcal{F}_N} L_{\text{sym}^2(f)}(s_0) \\ &= \frac{1}{\Gamma\left(\frac{s_0}{2}\right)^2 \Gamma\left(\frac{s_0+1}{2}\right)} \left( \frac{N-1}{12} \sum_{\substack{d, c \\ (d, N)=1}} \frac{1}{e^{\sigma_0 d} d^{2\sigma_0-2}} W\left(s_0, \frac{N}{d^2 e}\right) \right. \\ (6) \quad & \left. + \left(\frac{\pi^{\frac{3}{2}}}{N}\right)^{2s_0-3} \frac{N-1}{12} \sum_{\substack{d, c \\ (d, N)=1}} \frac{1}{e^{3-s_0} d^{4-2s_0}} W\left(3-s_0, \frac{N}{d^2 e}\right) \right) \\ & + S_1 + S_2 \end{aligned}$$

where

$$\begin{aligned} S_1 &\ll \frac{1}{\Gamma} \left( N^{-\frac{1}{2}+\delta} \sum_{\substack{d, c \\ (d, N)=1}} \frac{e^2 d(e^2)}{e^{\sigma_0 d} d^{2\sigma_0-2}} \left| W\left(s_0, \frac{N}{d^2 e}\right) \right| \right. \\ (7) \quad & \left. + N^{1-\frac{1}{2r}} (\log N)^C \sum_{\substack{d, c \\ (d, N)=1}} \frac{e d(e^2)}{e^{\sigma_0 d} d^{2\sigma_0-2}} \left| W\left(s_0, \frac{N}{d^2 e}\right) \right| \right) \end{aligned}$$

and  $S_2 \ll \frac{1}{N^{2\sigma_0-3}\Gamma}$

$$\left( N^{-\frac{1}{2}+\delta} \sum_{\substack{d, c \\ (d, N)=1}} \frac{e^2 d(e^2)}{e^{3-\sigma_0} d^{4-2\sigma_0}} \left| W\left(3-s_0, \frac{N}{d^2 e}\right) \right| \right)$$

$$(8) \quad +N^{1-\frac{1}{2r}}(\log N)^C \sum_{\substack{d,e \\ (d,N)=1}} \frac{ed(e^2)}{e^{3-\sigma_0}d^{4-2\sigma_0}} \left| W \left( 3 - s_0, \frac{N}{d^2e} \right) \right|.$$

Here,  $\Gamma = |\Gamma(\frac{s_0}{2})|^2 |\Gamma(\frac{s_0+1}{2})|$ . Now we apply the following three lemmas to estimate the terms of (6).

LEMMA 5. Let  $\sigma_0 > \frac{3}{2}$ , then

$$\begin{aligned} & \sum_{\substack{e,d \\ (d,N)=1}} \frac{1}{e^{s_0}d^{2s_0-2}} W \left( s_0, \frac{N}{d^2e} \right) \\ &= \Gamma \left( \frac{s_0}{2} \right)^2 \Gamma \left( \frac{s_0+1}{2} \right) \zeta(s_0)\zeta_N(2s_0-2) + O_{\sigma_0}(N^{\frac{3}{2}-\sigma_0}) \end{aligned}$$

and

$$\sum_{\substack{e,d \\ (d,N)=1}} \frac{1}{e^{3-s_0}d^{4-2s_0}} W \left( 3 - s_0, \frac{N}{d^2e} \right) = O_{\sigma_0}(N^{\sigma_0-\frac{3}{2}})$$

where  $W(s_0, x)$  is defined in Lemma 4.

PROOF. From the definition of  $W(s_0, x)$  it is clear that

$$\begin{aligned} & \sum_{\substack{e,d \\ (d,N)=1}} \frac{1}{e^{s_0}d^{2s_0-2}} W \left( s_0, \frac{N}{d^2e} \right) \\ &= \sum_e \frac{1}{e^{s_0}} \frac{1}{2\pi i} \int_{(\eta)} \pi^{-\frac{3}{2}s} \Gamma \left( \frac{s+s_0}{2} \right)^2 \Gamma \left( \frac{s+s_0+1}{2} \right) \\ & \quad \zeta_N(2s+2s_0-2) \left( \frac{N}{e} \right)^s \frac{ds}{s}. \end{aligned}$$

By moving the line of integration from  $(\eta)$  to the left of  $(\frac{3}{2} - \sigma_0)$ , we get the desired result. The second identity proves in a similar way by choosing  $\eta > \max\{3 - \sigma_0, \sigma_0 - \frac{3}{2}\}$  and moving the line of integration of the corresponding integral to the left of  $(\sigma_0 - \frac{3}{2})$ . ■

LEMMA 6.  $|W(s_0, x)| \leq W(\sigma_0, x)$ .

PROOF. From the Legendre duplication formula, we have

$$\Gamma \left( \frac{s+s_0}{2} \right) \Gamma \left( \frac{s+s_0+1}{2} \right) = \frac{\sqrt{\pi}}{2^{s+s_0-1}} \Gamma(s+s_0).$$

Now by applying this identity in the definition of  $W(s_0, x)$  and writing the  $\Gamma$  functions in terms of integrals, we get

$$\begin{aligned} & W(s_0, x) \\ &= \frac{1}{2\pi i} \frac{\sqrt{\pi}}{2^{s_0-1}} \int_{(\eta)} \left( \int_0^\infty \int_0^\infty t_1^{\frac{s+s_0}{2}-1} t_2^{s+s_0-1} e^{-(t_1+t_2)} dt_1 dt_2 \right) \left( \frac{\pi^{-\frac{3}{2}} x}{2} \right)^s \frac{ds}{s}. \end{aligned}$$

By interchanging the order of integration, we have

$$W(s_0, x) = \frac{\sqrt{\pi}}{2^{s_0-1}} \int_0^\infty t_1^{\frac{s_0}{2}-1} e^{-t_1} \left( \int_{\frac{x t_1^{\frac{1}{2}}}{2\pi^{\frac{3}{2}}}}^\infty t_2^{s_0-1} e^{-t_2} dt_2 \right) dt_1.$$

The result follows by applying the triangle inequality in the above identity. ■

LEMMA 7. Let  $\alpha < \min\{\frac{1+\beta}{2}, \gamma + 1\}$ , then

$$\sum_{\substack{d, e \\ (d, N)=1}} \frac{\mathbf{d}(e^2)}{e^\alpha d^\beta} W\left(\gamma, \frac{N}{d^2 e}\right) \sim \begin{cases} \frac{6}{\pi^2} \frac{\pi^{-\frac{3}{2}(1-\alpha)}}{1-\alpha} \zeta_N(\beta - 2\alpha + 2) \Gamma\left(\frac{\gamma-\alpha+1}{2}\right)^2 \Gamma\left(\frac{\gamma-\alpha+2}{2}\right) N^{1-\alpha} \log^2 N & \text{if } \alpha < 1 \\ \frac{6}{\pi^2} \zeta_N(\beta) \Gamma\left(\frac{\gamma}{2}\right)^2 \Gamma\left(\frac{\gamma+1}{2}\right) \log^3 N & \text{if } \alpha = 1 \end{cases}$$

as  $N \rightarrow \infty$ .

PROOF. First note that  $\sum_{e=1}^\infty \frac{\mathbf{d}(e^2)}{e^s} = \frac{\zeta^3(s)}{\zeta(2s)}$  for  $\text{Re}(s) > 1$ . Now by this identity and the definition of  $W(\cdot, \cdot)$  the above sum is equal to

$$\sum_{(d, N)=1} \frac{1}{d^\beta} \frac{1}{2\pi i} \int_{(\eta)} \pi^{-\frac{3}{2}s} \Gamma\left(\frac{s+\gamma}{2}\right)^2 \Gamma\left(\frac{s+\gamma+1}{2}\right) \frac{\zeta^3(s+\alpha)}{\zeta(2s+2\alpha)} \left(\frac{N}{d^2}\right)^s \frac{ds}{s}.$$

Moving the line of integration to the left of  $(1 - \alpha)$  and calculating the residue at  $s = 1 - \alpha$  yields the result. ■

Now by using Lemma 6 and Lemma 7 in (7) and (8), we get upper bounds for  $S_1$  and  $S_2$ . Applying these upper bounds and Lemma 5 in (6) yields

$$(9) \quad \sum_{f \in \mathcal{F}_N} L_{\text{sym}^2(f)}(s_0) = \zeta(s_0) \zeta_N(2s_0 - 2) \frac{N-1}{12} + O_{\sigma_0}(N^{\frac{5}{2}-\sigma_0}) + O_{\sigma_0} \left( \frac{N^{\frac{5}{2}-\sigma_0+\delta} \log^3 N + N^{3-\sigma_0-\frac{1}{2r}} (\log N)^C}{|\Gamma(\frac{s_0}{2})|^2 |\Gamma(\frac{s_0+1}{2})|} \right)$$

where  $0 < \delta < 1$ ,  $r \geq \frac{11}{\delta}$  is an integer and  $C > 0$  is a constant depending on  $\delta$  and  $r$ . It is clear that if  $\sigma_0 = 2$  the above formula gives us an asymptotic formula, and in this case we can see that the choice of  $\delta = \frac{11}{23}$  and  $r = 23$  gives the optimal error term, thus we proved the following theorem:

THEOREM 1. Let  $N$  be prime, then there exists  $B > 0$  such that for any real number  $t$

$$\sum_{f \in \mathcal{F}_N} L_{\text{sym}^2(f)}(2+it) = \zeta(2+it) \zeta_N(2+2it) \frac{N-1}{12} + O\left(\frac{N^{\frac{43}{16}} (\log N)^B}{|\Gamma(\frac{2+it}{2})|^2 |\Gamma(\frac{3+it}{2})|}\right).$$

COROLLARY 1. *Under the assumptions of Theorem 1*

$$\sum_{f \in \mathcal{F}_N} \langle f, f \rangle = \frac{\pi}{2^7 3^3} N^2 + O(N^{\frac{91}{48}} (\log N)^B).$$

PROOF. In Theorem 1, let  $t = 0$  and then use (3) to write  $L_{\text{sym}^2(f)}(s)$  in terms of  $\langle f, f \rangle$ . ■

NOTE. It is worth mentioning that (9) is an asymptotic formula if  $\sigma_0 = \text{Re}(s_0) > 2 - \frac{1}{48}$ .

ACKNOWLEDGEMENT. The author wishes to thank Ram Murty, Kumar Murty and Ali Rajaei for many helpful discussions related to this work.

#### REFERENCES

1. W. Duke, *The critical order of vanishing of automorphic L-functions with large level*. Invent. Math. **119**(1995), 165–174.
2. E. Kowalski, *The rank of the Jacobian of modular curves: analytic methods*. Ph. D. Thesis, Rutgers University, 1998.
3. R. Murty, *The analytic rank of  $J_0(N)(\mathbb{Q})$* . CMS Conf. Proc. **15**(1995), 263–277.
4. G. Shimura, *On the holomorphy of certain Dirichlet series*. Proc. London Math. Soc. Ser. **3** **31**(1975), 79–98.

*Department of Mathematics and Statistics  
Concordia University  
1455 de Maisonneuve Blvd. West  
Montréal, Quebec  
H3G 1M8  
email: akbary@cicma.concordia.ca*

## A REMARK ON A CONJECTURE CONCERNING EISENSTEIN NUMBERS

NOBUHIRO TERAJ

Presented by M. Ram Murty, FRSC

**ABSTRACT.** By using elementary methods, it is shown that when  $a, b, c$  are *Eisenstein numbers*, the Diophantine equation  $a^{2x} + a^x b^y + b^{2y} = c^z$  has only the positive integral solution  $(x, y, z) = (1, 1, 2)$  under some conditions.

**RÉSUMÉ.** En utilisant des méthodes élémentaires, on montre que, si  $a, b, c$  sont des nombres d'Eisenstein, l'équation diophantienne  $a^{2x} + a^x b^y + b^{2y} = c^z$  n'admet qu'une solution en entiers positifs  $(x, y, z) = (1, 1, 2)$  sous certaines conditions.

**1. Introduction.** Jeśmanowicz [J] conjectured that if  $a, b, c$  are *Pythagorean numbers*, i.e., positive integers satisfying  $a^2 + b^2 = c^2$ , then the Diophantine equation

$$a^x + b^y = c^z$$

has only the positive integral solution  $(x, y, z) = (2, 2, 2)$  (cf. Sierpiński [S1], [S2]). If  $a, b, c$  are positive integers satisfying  $a^2 + ab + b^2 = c^2$ , we call  $a, b, c$  *Eisenstein numbers*. There are some similar properties between Pythagorean numbers and Eisenstein numbers.

As an analogue to Jeśmanowicz's conjecture, in the previous paper Terai and Takakuwa [TT] we proposed the following (cf. Terai [Te1], [Te2]):

**CONJECTURE.** *If  $a, b, c$  are fixed positive integers satisfying  $a^2 + ab + b^2 = c^2$  with  $(a, b) = 1$ , then the Diophantine equation*

$$(1) \quad a^{2x} + a^x b^y + b^{2y} = c^z$$

*has only the positive integral solution  $(x, y, z) = (1, 1, 2)$ .*

In [TT], we showed that when  $a$  or  $b$  is a power of a prime, the Conjecture above holds under some conditions. The proof is based on the results concerning the Diophantine equations of second degree established by using properties of  $\mathbb{Q}(\sqrt{-3})$ . We also deduced that when  $a = p^e q^f$  or  $b = p^e q^f$ , where  $p, q$  are odd primes, an upper bound of  $y$  or  $x$  of equation (1) is derived by applying a result

---

Received by the editors July 15, 1999.  
AMS subject classification: 11D61.  
© Royal Society of Canada 2000.

$m$	$l$	$p^{i_1}$	$q^{i_2}$	$r^{i_3}$	$a$	$b$	$c$
8	3	11	5	19	55	57	97
10	3	13	7	23	91	69	139
20	3	23	17	43	391	129	469
28	3	31	$5^2$	59	775	177	877
12	5	17	7	29	119	145	239
22	5	$3^3$	17	$7^2$	1323	245	619
24	5	29	19	53	551	265	721
12	7	19	5	31	95	217	277

Table 1

due to Bugeaud [B], which is proved by means of estimates for linear forms in two logarithms.

In this paper, using elementary methods as in [TT], we prove that when  $a$  and  $b$  have two prime factors, the Conjecture above holds under some conditions. In fact, we establish the following:

**THEOREM 1.** *Let  $p, q, r, l$  be odd primes with  $q \equiv 5, 7 \pmod{12}$  satisfying*

$$p^{i_1} = m + l, \quad q^{i_2} = m - l, \quad r^{i_3} = 2m + l,$$

where  $i_1, i_2, i_3$  are positive integers, and  $m$  is even such that  $m > l$ ,  $m \not\equiv 0 \pmod{l}$  and  $m \not\equiv l \pmod{3}$ . Let  $a, b, c$  be the following Eisenstein numbers:

$$a = p^{i_1} q^{i_2}, \quad b = l r^{i_3}, \quad c = m^2 + ml + l^2.$$

Then equation (1) has only the positive integral solution  $(x, y, z) = (1, 1, 2)$ .

**THEOREM 2.** *Let  $p, q, r$  be odd primes with  $q \equiv 5, 7 \pmod{12}$  satisfying*

$$p^{j_1} = m + 2^e, \quad q^{j_2} = m - 2^e, \quad r^{j_3} = m + 2^{e-1},$$

where  $j_1, j_2, j_3$  are positive integers, and  $m$  is odd such that  $m > 2^e$  and  $e \geq 2$ . Let  $a, b, c$  be the following Eisenstein numbers:

$$a = p^{j_1} q^{j_2}, \quad b = 2^{e+1} r^{j_3}, \quad c = m^2 + m2^e + 2^{2e}.$$

Then equation (1) has only the positive integral solution  $(x, y, z) = (1, 1, 2)$ .

In Table 1 and Table 2 we give some examples of the values of  $m, l (e), p, q, r, a, b, c$  satisfying the conditions of Theorems 1, 2, respectively.

**2. Lemmas.** We need the following lemmas in the proof of Theorems 1, 2.

**LEMMA 1** ([TT]). *Eisenstein numbers  $a, b, c$  with  $(a, b) = 1$  and  $a - b \equiv 1 \pmod{3}$  are given as follows:*

$$a = u^2 - v^2, \quad b = v(2u + v), \quad c = u^2 + uv + v^2,$$

where  $u, v$  are positive integers such that  $(u, v) = 1, u > v$  and  $u \not\equiv v \pmod{3}$ .

$m$	$e$	$p^{j_1}$	$q^{j_2}$	$r^{j_3}$	$a$	$b$	$c$
9	2	13	5	11	65	88	133
21	2	$5^2$	17	23	425	184	541
23	2	$3^3$	19	$5^2$	513	200	637
45	2	$7^2$	41	47	2009	376	2221
15	3	23	7	19	161	304	409
39	3	47	31	43	1457	688	1897
21	4	37	5	29	185	928	1033
51	5	83	19	67	1577	4288	5257

Table 2

LEMMA 2.

(1) (Nagell [N1]). The Diophantine equation

$$x^2 + x + 1 = y^n$$

has only the positive integral solution  $(x, y, n) = (18, 7, 3)$  with  $n \geq 2$ .

(2) (Nagell [N2]). The Diophantine equation

$$x^2 + 3 = y^n$$

has only the positive integral solution  $(x, y, n) = (1, 2, 2)$  with  $n \geq 2$ .

(3) (Nagell [N3]). The Diophantine equation

$$3x^2 + 1 = y^n$$

has no positive integral solutions  $x, y, n$  with  $n \geq 3$ .

(4) (Ljunggren [L]). The Diophantine equation

$$3x^2 + 1 = 4y^n$$

has no positive integral solutions  $x, y, n$  with  $y > 1$  and  $n \geq 3$ .

**3. Proof of Theorem 1.** Suppose that our assumptions are all satisfied. Let  $(x, y, z)$  be a solution of (1).

We first show that  $z$  is even. Since  $c \equiv 3m^2 \pmod{q}$  and  $q \equiv 5, 7 \pmod{12}$ , we have  $\left(\frac{c}{q}\right) = \left(\frac{3}{q}\right) = -1$ , where  $\left(\frac{\cdot}{\cdot}\right)$  denotes the Jacobi symbol. Hence equation (1) implies that  $z$  is even, say  $z = 2Z$ .

Then by Lemma 1, we have

$$(E_1) \quad a^x = u^2 - v^2, \quad b^y = v(2u + v), \quad c^Z = u^2 + uv + v^2,$$

or

$$(E_2) \quad a^x = v(2u + v), \quad b^y = u^2 - v^2, \quad c^Z = u^2 + uv + v^2,$$

where  $u, v$  are positive integers such that  $(u, v) = 1$ ,  $u > v$  and  $u \not\equiv v \pmod{3}$ .

First consider  $(E_1)$ . If  $v = 1$ , then  $c^Z = u^2 + u + 1$ . Lemma 2, (1) implies that  $Z = 1$ . Then  $c = m^2 + ml + l^2 = u^2 + u + 1$  and so  $u < ml$ . Thus  $b^y = v(2u + v) = 2u + 1 < 2ml + 1 < l(2m + l) = b$ , which is impossible. Hence  $v = l^y$  and  $2u + v = r^{i_3 y}$ .

If  $u - v = 1$ , then  $3(2v + 1)^2 + 1 = 4c^Z$ . Lemma 2, (4) implies that  $Z = 1, 2$ . We show that the cases  $Z = 1, 2$  do not occur.

When  $Z = 1$ , we have  $c = m^2 + ml + l^2 = 3v^2 + 3v + 1$  and so  $v < m$ . Hence since  $q^{i_2} = m - l \geq 3$ , we have  $a^x = u^2 - v^2 = 2v + 1 < 2m + 1 < (m + l)(m - l) = a$ , which is impossible.

When  $Z = 2$ , then it follows from Lemma 1 that

$$u, v = h^2 - k^2, \quad k(2h + k); \quad c = h^2 + hk + k^2,$$

where  $h, k$  are positive integers such that  $(h, k) = 1$ ,  $h > k$  and  $h \not\equiv k \pmod{3}$ . Thus we obtain

$$u + v = h(2k + h) = a^x = p^{i_1 x} q^{i_2 x}.$$

This means that  $h = q^{i_2 x}$  and  $2k + h = p^{i_1 x}$ . So  $2k = p^{i_1 x} - q^{i_2 x}$ . In particular,  $k$  is divisible by  $\frac{p^{i_1} - q^{i_2}}{2} = l$ . On the other hand, since  $v = l^y = k(2h + k)$ , we have  $k = l^y$  and  $2h + k = 1$ , which is impossible.

Consequently we have  $v = l^y$ ,  $u - v = q^{i_2 x}$ ,  $u + v = p^{i_1 x}$ . Eliminating  $u$  and  $v$  yields

$$p^{i_1 x} - q^{i_2 x} = 2 \cdot l^y.$$

Taking the equation modulo 4 implies that  $x$  is odd. Suppose that  $x > 1$ . Then  $x \equiv 0 \pmod{l}$ . Indeed, since  $x$  is odd, we have

$$\begin{aligned} l^{y-1} &= \frac{p^{i_1 x} - q^{i_2 x}}{2l} = \frac{p^{i_1 x} - q^{i_2 x}}{p^{i_1} - q^{i_2}} \\ &= p^{i_1(x-1)} + p^{i_1(x-2)} \cdot q^{i_2} + \dots + p^{i_1} \cdot q^{i_2(x-2)} + q^{i_2(x-1)}, \end{aligned}$$

so  $0 \equiv xm^{x-1} \pmod{l}$ . Since  $m \not\equiv 0 \pmod{l}$ , we see that  $x \equiv 0 \pmod{l}$ .

We claim that  $p^{i_1 l} - q^{i_2 l} = 2l^2 L$ , where  $L > 1$  is odd  $\not\equiv 0 \pmod{l}$ . Indeed,

$$p^{i_1 l} - q^{i_2 l} = (m + l)^l - (m - l)^l = 2l^2(m^{l-1} + lt) = 2l^2 L$$

with  $t$  odd  $> 0$ . Hence  $2 \cdot l^y = p^{i_1 x} - q^{i_2 x}$  is divisible by  $p^{i_1 l} - q^{i_2 l} = 2l^2 L$ , which is impossible. Therefore we obtain  $x = 1$  and so  $y = 1$ ,  $u = m$ ,  $v = l$ ,  $Z = 1$ .

Next consider  $(E_2)$ . If  $v = 1$ , then  $c^Z = u^2 + u + 1$ . Lemma 2, (1) implies that  $Z = 1$ . Then  $c = m^2 + ml + l^2 = u^2 + u + 1$  and so  $u < ml$ . Hence  $b^y = u^2 - v^2 = u^2 - 1 < m^2 l^2 - 1 = (ml + 1)(ml - 1) < l(2m + l) = b$ , which is impossible. Thus  $v = q^{i_2 x}$  and  $2u + v = p^{i_1 x}$ . So  $u \equiv 0 \pmod{l}$ , because  $2u = p^{i_1 x} - q^{i_2 x}$  and  $p^{i_1} - q^{i_2} = 2l$ .

If  $u - v = 1$ , then  $3(2v + 1)^2 + 1 = 4c^Z$ . Lemma 2, (4) implies that  $Z = 1, 2$ . We show that the cases  $Z = 1, 2$  do not occur.

When  $Z = 1$ , we have  $c = m^2 + ml + l^2 = 3v^2 + 3v + 1$  and so  $v < m$ . Hence  $b^y = u^2 - v^2 = 2v + 1 < 2m + 1 < l(2m + l) = b$ , which is impossible.

When  $Z = 2$ , then it follows from Lemma 1 that

$$u + v = h(2k + h) = b^y = l^y r^{i_3 y}, \quad c = h^2 + hk + k^2,$$

where  $h, k$  are positive integers such that  $(h, k) = 1$ ,  $h > k$  and  $h \not\equiv k \pmod{3}$ . Then the fact that  $u \equiv 0 \pmod{l}$  implies that  $v \equiv 0 \pmod{l}$ , which contradicts  $(u, v) = 1$ .

Consequently we have  $v = q^{i_2 x}$ ,  $2u + v = p^{i_1 x}$ ,  $u - v = l^y$ ,  $u + v = r^{i_3 y}$ . Eliminating  $u$  and  $v$  yields

$$l^y + r^{i_3 y} = p^{i_1 x} - q^{i_2 x}.$$

Taking the equation modulo  $l$  yields

$$(2m)^y \equiv m^x - m^x \equiv 0 \pmod{l},$$

which is impossible, since  $m \not\equiv 0 \pmod{l}$ . ■

**4. Proof of Theorem 2.** Suppose that our assumptions are all satisfied. Let  $(x, y, z)$  be a solution of (1).

We first show that  $z$  is even. Since  $c \equiv 3m^2 \pmod{q}$  and  $q \equiv 5, 7 \pmod{12}$ , we have  $(\frac{c}{q}) = (\frac{3}{q}) = -1$ . Hence equation (1) implies that  $z$  is even, say  $z = 2Z$ . By Lemma 1, we have two cases  $(E_1)$ ,  $(E_2)$  as in the proof of Theorem 1.

First consider  $(E_1)$ . If  $u - v = 1$ , then  $3(2v + 1)^2 + 1 = 4c^Z$ . Lemma 2, (4) implies that  $Z = 1, 2$ . We show that the cases  $Z = 1, 2$  do not occur.

When  $Z = 1$ , we have from (1)

$$a^{2x} + a^x b^y + b^{2y} = c^z = c^{2Z} = c^2 = a^2 + ab + b^2.$$

Thus we have  $x = y = 1$  and so  $b = b^y = u^2 - v^2 = 2v + 1$ . Since  $4r^{2j_3} > c$ , we obtain

$$4c = 4c^Z = 3(2v + 1)^2 + 1 = 3b^2 + 1 = 3 \cdot 2^{2e} \cdot 4r^{2j_3} + 1 > 3 \cdot 2^{2e} c + 1,$$

which is impossible.

When  $Z = 2$ , then it follows from Lemma 1 that

$$u + v = h(2k + h) = a^x = p^{j_1 x} q^{j_2 x}, \quad c = h^2 + hk + k^2,$$

where  $h, k$  are positive integers such that  $(h, k) = 1$ ,  $h > k$  and  $h \not\equiv k \pmod{3}$ . This means that  $h = q^{j_2 x}$  and  $2k + h = p^{j_1 x}$ , so  $2k = p^{j_1 x} - q^{j_2 x} \equiv 0 \pmod{8}$ , because  $p^{j_1} - q^{j_2} = 2^{e+1} \equiv 0 \pmod{8}$ . Thus  $k \equiv 0 \pmod{4}$ . Since  $v$  is even,

$v = k(2h + k)$  and so  $v \equiv 0 \pmod{4}$ . Hence from  $(E_1)$ , we have  $v = 2^{(e+1)y-1}$  and  $2u + v = 2 \cdot r^{j_3y}$ . In view of  $v = k(2h + k)$  and  $k \equiv 0 \pmod{4}$ , we see that  $k = 2^{(e+1)y-2}$  and  $2h + k = 2$ , which is impossible.

Consequently we have  $u - v = q^{j_2x}$  and  $u + v = p^{j_1x}$ . Eliminating  $u$  yields  $2v = p^{j_1x} - q^{j_2x} \equiv 0 \pmod{8}$ . This means that  $v \equiv 0 \pmod{4}$ . Thus  $v = 2^{(e+1)y-1}$  and  $2u + v = 2 \cdot r^{j_3y}$ . Hence we obtain

$$p^{j_1x} - q^{j_2x} = 2^{(e+1)y}.$$

Since  $p^{j_1} + q^{j_2} = 2m$  with  $m$  odd  $> 1$ , we see that  $x$  must be odd. Suppose that  $x > 1$ . Note that  $\frac{p^{j_1x} - q^{j_2x}}{p^{j_1} - q^{j_2}}$  is odd  $> 1$ , since  $p, q, x$  are odd. Then  $2^{(e+1)y}$  is divisible by  $\frac{p^{j_1x} - q^{j_2x}}{p^{j_1} - q^{j_2}}$ , which is impossible. Therefore we obtain  $x = 1$  and so  $y = 1, v = 2^e, u = m, Z = 1$ .

Next consider  $(E_2)$ . If  $v = 1$ , then we have  $Z = 1$  as in the proof of Theorem 1. From (1), we have  $x = y = 1$  and so  $a = 2u + 1$ . Since  $p^{2j_1} > c$ , we obtain

$$4c = 4c^Z = (2u + 1)^2 + 3 = a^2 + 3 = p^{2j_1}q^{2j_2} + 3 > 9c + 3,$$

which is impossible. Consequently  $v = q^{j_2x}$  and  $2u + v = p^{j_1x}$ . Thus  $2u = p^{j_1x} - q^{j_2x} \equiv 0 \pmod{8}$ . This means that  $u \equiv 0 \pmod{4}$ , which is impossible, because  $u$  is odd. ■

#### REFERENCES

- [B] Y. Bugeaud, *On the diophantine equation  $x^2 - p^m = \pm y^n$* . Acta Arith. **80**(1997), 213–223.
- [J] L. Jeśmanowicz, *Some remarks on Pythagorean numbers*. (Polish) Wiadom. Mat. **1**(1955/1956), 196–202.
- [L] W. Ljunggren, *Über die Gleichungen  $1 + Dx^2 = 2y^n$  und  $1 + Dx^2 = 4y^n$* . Det Kgl. Norske Videnskabers Selskab, Forhandl. (30) **15**(1942), Trondheim.
- [N1] T. Nagell, *Des équations indéterminées  $x^2 + x + 1 = y^n$  et  $x^2 + x + 1 = 3y^n$* . Norsk. Mat. Forenings Skrifter **2**(1921), 12–14.
- [N2] ———, *Sur l'impossibilité de quelques équations à deux indéterminées*. Norsk. Mat. Forenings Skrifter **13**(1923), 65–82.
- [N3] ———, *Contributions to the theory of a category of diophantine equations of the second degree with two unknowns*. Nova Acta Soc. Sci. Upsal. Ser. IV (2) **16**(1955), 1–38.
- [S1] W. Sierpiński, *On the equation  $3^x + 4^y = 5^z$* . (Polish) Wiadom. Mat. **1**(1955/1956), 194–195.
- [S2] ———, *Elementary Theory of Numbers*. PWN-Polish Scientific Publishers, 1988.
- [TT] N. Terai and K. Takakuwa, *On a Diophantine equation concerning Eisenstein numbers*. Submitted.
- [Te1] N. Terai, *The Diophantine equation  $x^2 + q^m = p^n$* . Acta Arith. **63**(1993), 351–358.
- [Te2] ———, *Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations*. Acta Arith. **90**(1999), 17–35.

*Division of General Education  
Ashikaga Institute of Technology  
268-1 Omae, Ashikaga  
Tochigi 326-8558  
Japan  
email: terai@ashitech.ac.jp*

## APPROXIMATE MARTINGALE CENTRAL LIMIT THEOREMS ON HILBERT SPACE

MICHAEL S. BINGHAM

Presented by Vlastimil Dlab, FRSC

**ABSTRACT.** This paper presents two variants of a central limit theorem for an array of random variables which take their values in a real separable Hilbert space. Each row of the array is assumed to satisfy an “approximate martingale condition” that has some similarity to the martingale property, but is of a local rather than a global nature.

**RÉSUMÉ.** Cet article présente deux variants d’un théorème central limite pour des rangs de variables aléatoires qui prennent leurs valeurs dans une espace Hilbertienne réelle et séparable. Chaque rang est supposé satisfaire une “condition martingale approximative” qui ressemble un peu à la propriété martingale, mais qui est de nature locale plutôt que globale.

**1. Preliminaries.** In recent years many central limit theorems have been established for triangular arrays of real random variables in which each row is a sequence of martingale differences; see for example the book by Hall and Heyde [3]. Also in the literature can be found central limit theorems for Hilbert space valued martingales; for example Morrow [4], Morrow and Philipp [5], Philipp [8]. In this paper, however, the martingale condition will be replaced by a condition that provides local rather than global centring.

Throughout,  $H$  will denote a real separable Hilbert space with inner product  $(\cdot, \cdot)$ . Regarding  $H$  as an additive abelian group, the set of continuous homomorphisms of  $H$  into the multiplicative group of complex numbers with modulus one can be identified with  $H$  itself. Specifically,  $y \in H$  is identified with the homomorphism (character)

$$x \mapsto \langle x, y \rangle := \exp[i(x, y)], \quad x \in H.$$

All random variables in this paper will be assumed to be defined on the same underlying probability space  $(\Omega, \mathcal{F}, P)$  and to be measurable with respect to the Borel subsets of their image space. Let  $X$  be an  $H$ -valued random variable with distribution  $\mu$ . The characteristic function of  $\mu$ , or of  $X$ , is then the function  $\hat{\mu}$

---

Received by the editors June 10, 1999.

AMS subject classification: Primary: 60B12; secondary: 60B10.

© Royal Society of Canada 2000.

defined on  $H$  by

$$\hat{\mu}(y) := E[\langle X, y \rangle] = \int_H \langle x, y \rangle \mu(dx), \quad y \in H.$$

The correspondence between probability measures  $\mu$  on the Borel subsets of  $H$  and their characteristic functions  $\hat{\mu}$  is bijective. For information on probability measures on  $H$  we refer the reader to Parthasarathy [7] or Araujo and Giné [1].

The connection between the weak convergence of a sequence of probability measures and the convergence of their characteristic functions is not as straightforward in the case of an infinite dimensional Hilbert space as it is for the finite dimensional case, because weak relative compactness is not guaranteed by pointwise convergence of the characteristic functions.

**DEFINITION 1.** A nonnegative definite linear operator  $S$  on  $H$  is called an  $S$ -operator if it has finite trace; i.e., for some (and therefore every) orthonormal basis  $\{e_j : j = 1, 2, \dots\}$  of  $H$ ,  $\sum_{j=1}^{\infty} (S e_j, e_j) < \infty$ . A set  $(S_\alpha)_{\alpha \in A}$  of  $S$ -operators is called compact if, for any orthonormal basis  $\{e_j : j = 1, 2, \dots\}$  of  $H$ ,

$$(i) \quad \sup_{\alpha \in A} \sum_{j=1}^{\infty} (S_\alpha e_j, e_j) < \infty$$

$$(ii) \quad \lim_{N \rightarrow \infty} \sup_{\alpha \in A} \sum_{j=N}^{\infty} (S_\alpha e_j, e_j) = 0.$$

Then we have the following compactness criterion (Parthasarathy [7, Theorem 2.3, p. 155]).

**LEMMA 1.** A set  $\mathcal{K}$  of probability measures on  $H$  is relatively compact in the weak topology if and only if for every  $\varepsilon > 0$  the following condition holds. For each  $\mu \in \mathcal{K}$  there is an  $S$ -operator  $S_{\mu, \varepsilon}$  such that

$$1 - \mathcal{R}\hat{\mu}(y) \leq (S_{\mu, \varepsilon} y, y) + \varepsilon \quad \text{for all } y \in H$$

and  $\{S_{\mu, \varepsilon} : \mu \in \mathcal{K}\}$  is a compact set of  $S$ -operators. (Here  $\mathcal{R}$  denotes taking the real part.)

**COROLLARY 1.** A sequence  $(\mu_n)$  of probability measures on  $H$  is relatively compact if for every  $\varepsilon > 0$  there exists an  $S$ -operator  $S_\varepsilon$  such that

$$1 - \mathcal{R}\hat{\mu}_n(y) \leq (S_\varepsilon y, y) + \varepsilon \quad \text{for all } y \in H$$

whenever  $n$  is sufficiently large (depending on  $\varepsilon$ , but not on  $y$ ).

Some of what follows involves the concept of stable convergence in law for  $H$ -valued random variables. This idea was introduced for real valued random variables by Rényi [9] and was generalised to locally compact abelian groups in Bingham [2].

**DEFINITION 2.** The sequence  $(X_n)$  of  $H$ -valued random variables on the probability space  $(\Omega, \mathcal{F}, P)$  converges stably in law to the probability distribution  $\mu$  on  $H$  if  $(X_n)$  converges in law to  $\mu$  and  $\lim_{n \rightarrow \infty} P([X_n \in A] \cap F)$  exists for all  $F \in \mathcal{F}$  and every continuity set  $A$  of  $\mu$ .

Let  $L^1$  denote the space of complex-valued random variables on  $(\Omega, \mathcal{F}, P)$  that have finite expectations. Recall that a sequence  $(Z_n)$  in  $L^1$  is said to converge weakly in  $L^1$  to  $Z \in L^1$  if  $E(Z_n W) \rightarrow E(Z W)$  as  $n \rightarrow \infty$  holds for every bounded  $W$  in  $L^1$ ; or equivalently, if  $E(Z_n 1(F)) \rightarrow E(Z 1(F))$  as  $n \rightarrow \infty$  holds for each  $F \in \mathcal{F}$ . See Neveu [6].

The following lemma clarifies the nature of stable weak convergence and shows its relationship to weak  $L^1$  convergence. It can be proved in essentially the same way as Lemma 2 in Bingham [2].

**LEMMA 2.** Let  $(X_n)$  be a sequence of  $H$ -valued random variables on  $(\Omega, \mathcal{F}, P)$  and let  $\mu_n$  denote the distribution of  $X_n$ . The following three statements are equivalent.

- (i)  $(X_n)$  converges stably in law to a probability distribution  $\mu$  on  $H$ .
- (ii) For each  $F \in \mathcal{F}$  with  $P(F) > 0$ , the conditional distribution of  $X_n$  given  $F$  converges weakly to a probability distribution  $\mu^F$  on  $H$ .
- (iii)  $(\mu_n)$  is weakly relatively compact and for each  $y \in H$  there is a  $Z(y) \in L^1$  such that  $\langle X_n, y \rangle$  converges weakly in  $L^1$  to  $Z(y)$  as  $n \rightarrow \infty$ .

When the above convergences occur then  $\mu = \mu^\Omega$  and, for  $F \in \mathcal{F}$  with  $0 < P(F) < 1$ ,

$$\begin{aligned} \mu &= P(F)\mu^F + P(F^c)\mu^{F^c} \quad \text{and} \\ \mu^F(y) &= E(Z(y) | F), \quad y \in H. \end{aligned}$$

**DEFINITION 3.** A probability distribution  $\mu$  on  $H$  is called Gaussian if its characteristic function is of the form

$$\hat{\mu}(y) = \exp \left[ i(x_0, y) - \frac{1}{2}(Sy, y) \right], \quad y \in H$$

where  $x_0$  is a fixed point of  $H$  and  $S$  is a fixed  $S$ -operator on  $H$ . (In this paper only symmetric Gaussian distributions will appear; *i.e.*, we shall have  $x_0 = 0$ .)

Let us call a mapping  $\omega \mapsto S(\omega)$  defined on  $\Omega$  a random  $S$ -operator on  $H$  if

- (i) for each  $\omega \in \Omega$ ,  $S(\omega)$  is an  $S$ -operator on  $H$  and
- (ii) for each  $y \in H$ ,  $\omega \mapsto (S(\omega)y, y)$  is a real-valued random variable.

As is customary in probability theory, we shall suppress the  $\omega$  in the notation and write  $S$  for  $S(\omega)$ . Suppose then that we have a random  $S$ -operator  $S$  on  $H$ . It follows that the function

$$y \mapsto E \left( \exp \left[ -\frac{1}{2}(Sy, y) \right] \right), \quad y \in H$$

is the characteristic function of a mixture of (symmetric) Gaussian distributions.

2. **The central limit theorems.** Suppose that we are given an adapted triangular array  $\{S_{n,j}, \mathcal{F}_{n,j} : 0 \leq j \leq k_n, n \geq 1\}$  of  $H$ -valued random variables defined on the probability space  $(\Omega, \mathcal{F}, P)$ . That is, for each  $n \geq 1$ ,  $\{\mathcal{F}_{n,j} : 0 \leq j \leq k_n\}$  is an increasing sequence of sub- $\sigma$ -fields of  $\mathcal{F}$  (i.e., a filtration) and  $\{S_{n,j} : 0 \leq j \leq k_n\}$  is adapted to this filtration (i.e.,  $S_{n,j}$  is  $\mathcal{F}_{n,j}$ -measurable for each  $j$ ) with  $S_{n,0} = 0$ . The sequence  $(k_n)$  of integers is nondecreasing and goes to  $\infty$  as  $n \rightarrow \infty$ . Define the differences  $\{X_{n,j} : 1 \leq j \leq k_n\}$  by  $X_{n,j} = S_{n,j} - S_{n,j-1}$ .

**THEOREM 1.** *Consider an adapted triangular array of  $H$ -valued random variables as above and suppose that the following conditions hold. For every neighbourhood  $N$  of 0 in  $H$ ,*

$$(1) \quad P(X_{n,j} \notin N \text{ for some } j = 1, 2, \dots, k_n) \rightarrow 0 \quad \text{as } n \rightarrow \infty.$$

*There is a bounded neighbourhood  $M$  of 0 in  $H$  such that the random variables  $X'_{n,j} := 1(X_{n,j} \in M)X_{n,j}$  satisfy*

$$(2) \quad \sum_{j=1}^{k_n} |E[(X'_{n,j}, y) \mid \mathcal{F}_{n,j-1}]| \xrightarrow{P} 0 \quad \text{as } n \rightarrow \infty \text{ for each } y \in H$$

and

$$(3) \quad \sum_{j=1}^{k_n} (X'_{n,j}, y)^2 \xrightarrow{P} (Sy, y) \quad \text{as } n \rightarrow \infty \text{ for each } y \in H$$

where  $S$  is a random  $S$ -operator on  $H$ . (Here  $\xrightarrow{P}$  denotes convergence in probability.) Assume also that there is a fixed  $S$ -operator  $T$  on  $H$  such that

$$(4) \quad E\left(\sum_{j=1}^{k_n} |E[(X'_{n,j}, y) \mid \mathcal{F}_{n,j-1}]|\right) \leq \sqrt{(Ty, y)} \quad \text{for each } y \in H$$

and

$$(5) \quad E\left(\sum_{j=1}^{k_n} (X'_{n,j}, y)^2\right) \leq (Ty, y) \quad \text{for each } y \in H$$

both hold for all sufficiently large  $n$ . Finally, assume also that the filtrations are nested; i.e.,

$$(6) \quad \mathcal{F}_{n,j} \subseteq \mathcal{F}_{n+1,j} \quad \text{for all } n, j.$$

Then  $S_{n,k_n}$  converges stably in law as  $n \rightarrow \infty$ ; for each  $F \in \mathcal{F}$  with  $P(F) > 0$  the conditional distribution of  $S_{n,k_n}$  given  $F$  converges weakly to the mixture of Gaussian distributions on  $H$  with the characteristic function

$$y \mapsto E\left(\exp\left[-\frac{1}{2}(Sy, y)\right] \mid F\right), \quad y \in H.$$

PROOF. Let  $\mu_n$  denote the distribution of  $S_{n,k_n}$ . We first use Corollary 1 to show that  $(\mu_n)$  is weakly relatively compact. For any  $y \in H$

$$\begin{aligned} 1 - \mathcal{R}\hat{\mu}_n(y) &= \mathbb{E}[\mathcal{R}(1 - \langle S_{n,k_n}, y \rangle)] \\ &= \mathbb{E}\left[\mathcal{R}\left\{\sum_{j=1}^{k_n} \left(\prod_{k=1}^{j-1} \langle X_{n,k}, y \rangle\right) (1 - \langle X_{n,j}, y \rangle)\right\}\right] \\ &= \mathbb{E}\left[\mathcal{R}\left\{\sum_{j=1}^{k_n} \left(\prod_{k=1}^{j-1} \langle X_{n,k}, y \rangle\right) \mathbb{E}[1 - \langle X_{n,j}, y \rangle \mid \mathcal{F}_{n,j-1}]\right\}\right] \\ &\leq \mathbb{E}\left[\sum_{j=1}^{k_n} |\mathbb{E}[1 - \langle X_{n,j}, y \rangle \mid \mathcal{F}_{n,j-1}]|\right] \\ &= \mathbb{E}\left[\sum_{j=1}^{k_n} |\mathbb{E}[-i(X_{n,j}, y) + \alpha_{n,j} \mid \mathcal{F}_{n,j-1}]|\right] \end{aligned}$$

where  $|\alpha_{n,j}| \leq (X_{n,j}, y)^2$ . Therefore

$$(7) \quad \mathbb{E}[\mathcal{R}(1 - \langle S_{n,k_n}, y \rangle)] \leq \mathbb{E}\left[\sum_{j=1}^{k_n} |\mathbb{E}[(X_{n,j}, y) \mid \mathcal{F}_{n,j-1}]|\right] + \mathbb{E}\left[\sum_{j=1}^{k_n} (X_{n,j}, y)^2\right].$$

Let  $A_n := [X_{n,j} \in M \text{ for all } j = 1, 2, \dots, k_n]$ . Then  $X'_{n,j} = X_{n,j}$  on  $A_n$  and, replacing  $X_{n,j}$  by  $X'_{n,j}$  in (7) with  $S'_{n,k_n} := \sum_{j=1}^{k_n} X'_{n,j}$ , we obtain

$$\begin{aligned} 1 - \mathcal{R}\hat{\mu}_n(y) &= \mathbb{E}[\mathcal{R}(1 - \langle S_{n,k_n}, y \rangle)(1(A_n) + 1(A_n^c))] \\ (8) \quad &= M_n(y) + \mathbb{E}\left[\sum_{j=1}^{k_n} (X'_{n,j}, y)^2\right] + 2P(A_n^c) \end{aligned}$$

where

$$M_n(y) := \mathbb{E}\left[\sum_{j=1}^{k_n} |\mathbb{E}[(X'_{n,j}, y) \mid \mathcal{F}_{n,j-1}]|\right].$$

Given  $\varepsilon > 0$  and  $y \in H$ , we have either (i)  $M_n(y) < \varepsilon$  or (ii)  $M_n(y) \geq \varepsilon$ . In the latter case  $M_n(y/\varepsilon) \geq 1$  and, using (4),

$$M_n(y)/\varepsilon = M_n(y/\varepsilon) \leq (M_n(y/\varepsilon))^2 \leq (T(y/\varepsilon), y/\varepsilon) = ((T/\varepsilon)y, y)/\varepsilon$$

so  $M_n(y) \leq ((T/\varepsilon)y, y)$ . Combining cases (i) and (ii) we obtain

$$(9) \quad M_n(y) \leq ((T/\varepsilon)y, y) + \varepsilon \quad \text{for all } y \in H.$$

From (1), (5), (8) and (9) it follows that

$$1 - \mathcal{R}\hat{\mu}_n(y) \leq ((T + T/\varepsilon)y, y) + 3\varepsilon \quad \text{for all } y \in H$$

whenever  $n$  is sufficiently large. Since  $T+T/\varepsilon$  is an  $S$ -operator, Corollary 1 shows that  $(\mu_n)$  is relatively compact.

By Lemma 2, the proof of Theorem 1 will be complete if we show that, for every  $y \in H$ ,

$$(10) \quad \langle S_{n,k_n}, y \rangle \rightarrow \exp \left[ -\frac{1}{2} (Sy, y) \right] \quad \text{weakly in } L^1$$

as  $n \rightarrow \infty$ . In order to do so, because of (1), we can and shall assume without loss of generality that  $X_{n,j} \in M$  for all  $n$  and  $j$  where  $M$  is a bounded symmetric neighbourhood of 0 in  $H$  such that (2), (3), (4) and (5) hold. The required result (10) can then be proved by the same arguments as were used in the proof of the Theorem in Bingham [2] provided we think of  $\Phi(y)$  as  $(Sy, y)$  and take  $g(x, y) = (1(x \in M)x, y)$  for all  $x, y \in H$ . Note that the assumed boundedness of  $M$  implies that  $|g(x, y)| < \infty$  for each  $y \in H$ .

**THEOREM 2.** *Let  $\{S_{n,j}, \mathcal{F}_{n,j} : 0 \leq j \leq k_n, n \geq 1\}$  satisfy the assumptions (1), (2), (3), (4) and (5) in Theorem 1, but replace the nesting condition (6) by the following measurability condition: for each  $y \in H$  there exists an integer  $m$  such that  $(Sy, y)$  is  $\mathcal{F}_{n,m}$ -measurable for all sufficiently large  $n$ . Then the distribution of  $S_{n,k_n}$  converges weakly to the mixture of Gaussian distributions with characteristic function*

$$y \mapsto E \left( \exp \left[ -\frac{1}{2} (Sy, y) \right] \right), \quad y \in H.$$

**PROOF.** We can show that  $(\mu_n)$  is relatively compact exactly as in the proof of Theorem 1. Using similar arguments to those used to prove the Corollary to the Theorem in Bingham [2], we obtain that for each  $y \in H$

$$\hat{\mu}_n(y) \rightarrow E \left( \exp \left[ -\frac{1}{2} (Sy, y) \right] \right) \quad \text{as } n \rightarrow \infty.$$

**ACKNOWLEDGEMENT.** Part of the research for this paper was done when the author was visiting the Mathematics Institute at the University of Tübingen in the Federal Republic of Germany, supported by a grant from the German Academic Exchange Service (DAAD). The author thanks both of these organisations for their hospitality and generosity.

#### REFERENCES

1. A. Araujo and E. Giné, *The Central Limit Theorem for Real and Banach Valued Random Variables*. John Wiley & Sons, New York, 1980.
2. M. S. Bingham, *A central limit theorem for approximate martingale arrays with values in a locally compact abelian group*. *Math. Z.* **192**(1986), 409–419.
3. P. Hall and C. C. Heyde, *Martingale Limit Theory and Its Application*. Academic Press, New York, 1980.
4. G. J. Morrow, *A weak invariance principle for Hilbert space valued martingales*. *Illinois J. Math.* **27**(1983), 659–669.

5. G. J. Morrow and W. Philipp, *An almost sure invariance principle for Hilbert space valued martingales*. Trans. Amer. Math. Soc. **273**(1982), 231–250.
6. J. Neveu, *Mathematical Foundations of the Calculus of Probability*. Holden-Day, San Francisco, 1965.
7. K. R. Parthasarathy, *Probability Measures on Metric Spaces*. Academic Press, New York, 1967.
8. W. Philipp, *A note on almost sure approximation of weakly dependent random variables*. Monatsh. Math. **102**, 227–236 (1963)
9. A. Rényi, *On Stable Sequences of Events*. Sankyā Ser. A, **25**(1963), 293–302.

*Department of Mathematics*  
*University of Hull*  
*Hull HU6 7RX*  
*England*  
*email: m.s.bingham@maths.hull.ac.uk*

## ALMOST ALL NONEXPANSIVE MAPPINGS ARE CONTRACTIVE

SIMEON REICH AND ALEXANDER J. ZASLAVSKI

Presented by Jonathan M. Borwein, FRSC

**ABSTRACT.** We show that most nonexpansive mappings (in the sense of Baire's category) are, in fact, contractive.

**RÉSUMÉ.** Nous démontrons que la plupart des applications nonexpansive (dans le sens de la catégorie de Baire) sont, en effet, contractives.

**Introduction.** Nonexpansive mapping theory has flourished during the last thirty-five years with many results and applications. See, for example, [2], [5], [6] and the references mentioned there. In contrast with the iterates of nonexpansive mappings which in general do not converge, it is known that the iterates of contractive mappings converge in all complete metric spaces [10]. However, it is also known [4] that the iterates of most nonexpansive mappings (in the sense of Baire's category) do converge to their unique fixed points. In this paper we improve upon this result by showing that most nonexpansive mappings are, in fact, contractive. Such an approach, when a certain property is investigated for a whole function space and not just for a single operator, is common in the theory of dynamical systems [9], optimization [7], variational analysis [3] and optimal control [12].

**1. Contractive mappings.** Let  $(X, \rho)$  be a metric space and let  $R^1$  denote the real line. We say that a mapping  $c: R^1 \rightarrow X$  is a metric embedding of  $R^1$  into  $X$  if  $\rho(c(s), c(t)) = |s - t|$  for all real  $s$  and  $t$ . The image of  $R^1$  under a metric embedding will be called a metric line. The image of a real interval  $[a, b] = \{t \in R^1 : a \leq t \leq b\}$  under such a mapping will be called a metric segment. Assume that  $(X, \rho)$  contains a family  $M$  of metric lines such that for each pair of distinct points  $x$  and  $y$  in  $X$  there is a unique metric line in  $M$  which passes through  $x$  and  $y$ . This metric line determines a unique metric segment joining  $x$  and  $y$ . We denote this segment by  $[x, y]$ . For each  $0 \leq t \leq 1$  there is a unique point  $z$  in  $[x, y]$  such that  $\rho(x, z) = t\rho(x, y)$  and  $\rho(z, y) = (1 - t)\rho(x, y)$ .

---

Received by the editors June 24, 1999.

AMS subject classification: 47H09, 47H10, 58F99.

Key words and phrases: contractive mapping, fixed point set, generic property, nonexpansive mapping, uniform space.

© Royal Society of Canada 2000.

This point will be denoted by  $(1-t)x \oplus ty$ . We will say that  $X$ , or more precisely  $(X, \rho, M)$ , is a hyperbolic space if

$$\rho\left(\frac{1}{2}x \oplus \frac{1}{2}y, \frac{1}{2}x \oplus \frac{1}{2}z\right) \leq \frac{1}{2}\rho(y, z)$$

for all  $x, y$  and  $z$  in  $X$ . A set  $K \subset X$  is called  $\rho$ -convex if  $[x, y] \subset K$  for all  $x$  and  $y$  in  $K$ . It is clear that all normed linear spaces are hyperbolic. A discussion of more examples of hyperbolic spaces and in particular of the Hilbert ball can be found, for example, in [10]. In the sequel we will repeatedly use the following fact (cf. [6, pp. 77, 104] and [11]): If  $(X, \rho, M)$  is a hyperbolic space, then

$$(1.1) \quad \rho((1-t)x \oplus tz, (1-t)y \oplus tw) \leq (1-t)\rho(x, y) + t\rho(z, w)$$

for all  $x, y, z$  and  $w$  in  $X$  and  $0 \leq t \leq 1$ .

Assume that  $(X, \rho)$  is a hyperbolic complete metric space and let  $K$  be a bounded closed  $\rho$ -convex subset of  $X$ . Denote by  $\mathcal{A}$  the set of all operators  $A: K \rightarrow K$  such that

$$(1.2) \quad \rho(Ax, Ay) \leq \rho(x, y) \quad \text{for all } x, y \in K.$$

In other words, the set  $\mathcal{A}$  consists of all the nonexpansive self-mappings of  $K$ . Set

$$d(K) = \sup\{\rho(x, y) : x, y \in K\}.$$

We equip the set  $\mathcal{A}$  with the metric  $h(\cdot, \cdot)$  defined by

$$h(A, B) = \sup\{\rho(Ax, Bx) : x \in K\}, \quad A, B \in \mathcal{A}.$$

Clearly the metric space  $(\mathcal{A}, h)$  is complete.

We say that a mapping  $A \in \mathcal{A}$  is contractive if there exists a decreasing function  $\phi^A: [0, d(K)] \rightarrow [0, 1]$  such that

$$(1.3) \quad \phi^A(t) < 1 \quad \text{for all } t \in (0, d(K)]$$

and

$$(1.4) \quad \rho(Ax, Ay) \leq \phi^A(\rho(x, y))\rho(x, y) \quad \text{for all } x, y \in K.$$

The notion of a contractive mapping as well as its modifications and applications were studied by many authors. See, for example, [1], [8]. We now quote a convergence result which is valid in all complete metric spaces [10].

**THEOREM 1.1.** *Assume that  $A \in \mathcal{A}$  is contractive. Then there exists  $x_A \in K$  such that  $A^n x \rightarrow x_A$  as  $n \rightarrow \infty$ , uniformly on  $K$ .*

For each  $A, B \in \mathcal{A}$  and each  $\alpha \in (0, 1)$ , define the operator  $\alpha A \oplus (1-\alpha)B$  by

$$(1.5) \quad (\alpha A \oplus (1-\alpha)B)x = \alpha Ax \oplus (1-\alpha)Bx, \quad x \in K.$$

Note that  $\alpha A \oplus (1-\alpha)B \in \mathcal{A}$  by (1.1). Next, we note the following fact.

PROPOSITION 1.1. *If  $A \in \mathcal{A}$  is contractive,  $B \in \mathcal{A}$  and  $\alpha \in (0, 1)$ , then the operators  $AB$ ,  $BA$  and  $\alpha A \oplus (1 - \alpha)B$  are also contractive.*

Now we show that most of the mappings in  $\mathcal{A}$  (in the sense of Baire's category) are, in fact, contractive.

THEOREM 1.2. *There exists a set  $\mathcal{F}$  which is a countable intersection of open everywhere dense sets in  $\mathcal{A}$  such that each  $A \in \mathcal{F}$  is contractive.*

PROOF. Fix  $\theta \in K$ . For each  $A \in \mathcal{A}$  and each  $\gamma \in (0, 1)$  define  $A_\gamma \in \mathcal{A}$  by

$$(1.6) \quad A_\gamma x = (1 - \gamma)Ax \oplus \gamma\theta, \quad x \in K.$$

Clearly the set  $\{A_\gamma : A \in \mathcal{A}, \gamma \in (0, 1)\}$  is everywhere dense in  $\mathcal{A}$ .

Let  $A \in \mathcal{A}$  and  $\gamma \in (0, 1)$ . The inequality (1.1) implies that

$$(1.7) \quad \rho(A_\gamma x, A_\gamma y) \leq (1 - \gamma)\rho(x, y)$$

for all  $x, y \in K$ . For each integer  $i \geq 1$  define

$$(1.8) \quad U(A, \gamma, i) = \{B \in \mathcal{A} : h(A_\gamma, B) < 4^{-i-1}\gamma d(K)\}.$$

We will show that for each  $A \in \mathcal{A}$ ,  $\gamma \in (0, 1)$  and each integer  $i \geq 1$ , the following property holds:

P(1) For each  $B \in U(A, \gamma, i)$  and each  $x, y \in K$  satisfying  $\rho(x, y) \geq 4^{-i}d(K)$ , the inequality  $\rho(Bx, By) \leq (1 - 2^{-1}\gamma)\rho(x, y)$  is valid.

Indeed, let  $A \in \mathcal{A}$ ,  $\gamma \in (0, 1)$  and let  $i \geq 1$  be an integer. Assume that

$$(1.9) \quad B \in U(A, \gamma, i), \quad x, y \in K \quad \text{and} \quad \rho(x, y) \geq 4^{-i}d(K).$$

By (1.8), (1.9) and (1.7),

$$\begin{aligned} \rho(Bx, By) &\leq \rho(A_\gamma x, A_\gamma y) + 2^{-1} \cdot 4^{-i}\gamma d(K) \\ &\leq (1 - \gamma)\rho(x, y) + 2^{-1}4^{-i}\gamma d(K) \\ &\leq (1 - \gamma)\rho(x, y) + 2^{-1}\gamma\rho(x, y) \\ &= (1 - 2^{-1}\gamma)\rho(x, y). \end{aligned}$$

Thus property P(1) holds. Now define

$$\mathcal{F} = \bigcap_{q=1}^{\infty} \cup \{U(A, \gamma, i) : A \in \mathcal{A}, \gamma \in (0, 1), i \geq q\}.$$

Clearly  $\mathcal{F}$  is a countable intersection of open everywhere dense sets in  $\mathcal{A}$ . We claim that any  $B \in \mathcal{F}$  is contractive. To this end, assume that  $q$  is a natural number. There exist  $A \in \mathcal{A}$ ,  $\gamma \in (0, 1)$  and an integer  $i \geq q$  such that  $B \in U(A, \gamma, i)$ . By property P(1), for each  $x, y \in K$  satisfying  $\rho(x, y) \geq 4^{-q}d(K)$  we have  $\rho(Bx, By) \leq (1 - 2^{-1}\gamma)\rho(x, y)$ . Since  $q$  is an arbitrary natural number we conclude that  $B$  is contractive. Theorem 1.2 is proved.

**2. Attractive sets.** In this section we study nonexpansive mappings which are contractive with respect to a given subset of their domain.

Assume that  $(X, \rho)$  is a hyperbolic complete metric space and that  $K$  is a closed (not necessarily bounded)  $\rho$ -convex subset of  $X$ . Once again, denote by  $\mathcal{A}$  the set of all mappings  $A: K \rightarrow K$  such that

$$(2.10) \quad \rho(Ax, Ay) \leq \rho(x, y) \quad \text{for all } x, y \in K.$$

For each  $x \in K$  and each subset  $E \subset K$ , let  $\rho(x, E) = \inf\{\rho(x, y) : y \in E\}$ . For each  $x \in K$  and each  $r > 0$ , set

$$(2.11) \quad B(x, r) = \{y \in K : \rho(x, y) \leq r\}.$$

Fix  $\theta \in K$ . For the set  $\mathcal{A}$  we consider the uniformity determined by the following base:

$$(2.12) \quad E(n, \epsilon) = \{(A, B) \in \mathcal{A} \times \mathcal{A} : \rho(Ax, Bx) \leq \epsilon, x \in B(\theta, n)\},$$

where  $\epsilon > 0$  and  $n$  is a natural number. Clearly the space  $\mathcal{A}$  with this uniformity is metrizable and complete. We equip the space  $\mathcal{A}$  with the topology induced by this uniformity.

Let  $F$  be a nonempty closed  $\rho$ -convex subset of  $K$ . Denote by  $\mathcal{A}^{(F)}$  the set of all  $A \in \mathcal{A}$  such that  $Ax = x$  for all  $x \in F$ . Clearly  $\mathcal{A}^{(F)}$  is a closed subset of  $\mathcal{A}$ . We consider the topological subspace  $\mathcal{A}^{(F)} \subset \mathcal{A}$  with the relative topology. An operator  $A \in \mathcal{A}^{(F)}$  is said to be contractive with respect to  $F$  if for any natural number  $n$  there exists a decreasing function  $\phi_n^A: [0, \infty) \rightarrow [0, 1]$  such that

$$(2.13) \quad \phi_n^A(t) < 1 \quad \text{for all } t > 0$$

and

$$(2.14) \quad \rho(Ax, F) \leq \phi_n^A(\rho(x, F))\rho(x, F) \quad \text{for all } x \in B(\theta, n).$$

Clearly this definition does not depend on our choice of  $\theta$ .

We begin our discussion of such mappings by proving that the set  $F$  attracts all the iterates of  $A$ .

**THEOREM 2.1.** *Let  $A \in \mathcal{A}^{(F)}$  be contractive with respect to  $F$ . Then there exists  $B \in \mathcal{A}^{(F)}$  such that  $B(K) = F$  and  $A^n x \rightarrow Bx$  as  $n \rightarrow \infty$ , uniformly on  $B(\theta, r)$  for any natural number  $r$ .*

**PROOF.** We may assume without loss of generality that  $\theta \in F$ . Then for each real  $s > 0$ ,

$$(2.15) \quad C(B(\theta, s)) \subset B(\theta, s) \quad \text{for all } C \in \mathcal{A}^{(F)}.$$

Now let  $r$  be any natural number. If we show that there exists  $B: B(\theta, r) \rightarrow F$  such that

$$(2.16) \quad A^n x \rightarrow Bx \text{ as } n \rightarrow \infty, \text{ uniformly on } B(\theta, r),$$

then the theorem will follow because  $B$  is nonexpansive and  $Bx = x$  for all  $x \in F \cap B(\theta, r)$ .

There exists a decreasing function  $\phi_r^A: [0, \infty) \rightarrow [0, 1]$  such that

$$(2.17) \quad \phi_r^A(t) < 1 \quad \text{for all } t > 0$$

and

$$(2.18) \quad \rho(Ax, F) \leq \phi_r^A(\rho(x, F))\rho(x, F) \quad \text{for all } x \in B(\theta, r).$$

Let  $\epsilon \in (0, 1)$ . Choose a natural number  $m \geq 4$  such that

$$(2.19) \quad \phi_r^A(\epsilon r)^m < 8^{-1}\epsilon.$$

Let  $x \in B(\theta, r)$ . We will show that

$$(2.20) \quad \rho(A^m x, F) < \epsilon r.$$

Assume the contrary. Then for each  $i = 0, \dots, m$ ,  $\rho(A^i x, F) \geq \epsilon r$ , and by (2.9) and (2.6),

$$\begin{aligned} A^i x \in B(\theta, r), \rho(A^{i+1} x, F) &\leq \phi_r^A(\rho(A^i x, F))\rho(A^i x, F) \\ &\leq \phi_r^A(\epsilon r)\rho(A^i x, F). \end{aligned}$$

When combined with (2.10) these inequalities imply that

$$\rho(A^m x, F) \leq \phi_r^A(\epsilon r)^m \rho(x, F) \leq 8^{-1}\epsilon \rho(x, \theta) \leq 8^{-1}\epsilon r,$$

a contradiction. Therefore (2.11) is valid and for each  $x \in B(\theta, r)$  there exists  $C_\epsilon(x) \in F$  such that  $\rho(A^m x, C_\epsilon(x)) < \epsilon r$ . This implies that for each  $x \in B(\theta, r)$ ,

$$(2.21) \quad \rho(A^i x, C_\epsilon(x)) < \epsilon r \quad \text{for all integers } i \geq m.$$

Since  $\epsilon$  is an arbitrary number in  $(0, 1)$  we conclude that for each  $x \in B(\theta, r)$ ,  $\{A^i x\}_{i=1}^\infty$  is a Cauchy sequence and there exists  $Bx = \lim_{i \rightarrow \infty} A^i x$ . Clearly

$$(2.22) \quad \rho(Bx, C_\epsilon(x)) \leq \epsilon r \quad \text{for all } x \in B(\theta, r).$$

Since (2.13) is true for any  $\epsilon$  in  $(0, 1)$ , we conclude that  $B(B(\theta, r)) \subset F$ . By (2.13) and (2.12), for each  $x \in B(\theta, r)$ ,  $\rho(A^i x, Bx) \leq 2\epsilon r$  for all integers  $i \geq m$ . Finally, since  $\epsilon \in (0, 1)$  is arbitrary, we conclude that (2.7) is valid. This completes the proof of Theorem 2.1.

We continue with an analog of Proposition 1.1.

**PROPOSITION 2.1.** *Assume that  $A, B \in \mathcal{A}^{(F)}$  and that  $A$  is contractive with respect to  $F$ . Then the operators  $AB$  and  $BA$  are also contractive with respect to  $F$ .*

We now show that if  $\mathcal{A}^{(F)}$  contains a retraction, then almost all the mappings in  $\mathcal{A}^{(F)}$  are contractive with respect to  $F$ .

THEOREM 2.2. *Assume that there exists*

$$(2.23) \quad Q \in \mathcal{A}^{(F)} \quad \text{such that } Q(K) = F.$$

*Then there exists a set  $\mathcal{F} \subset \mathcal{A}^{(F)}$  which is a countable intersection of open everywhere dense sets in  $\mathcal{A}^{(F)}$  such that each  $B \in \mathcal{F}$  is contractive with respect to  $F$ .*

PROOF. We may assume that  $\theta \in F$ . Then for each real  $r > 0$ ,

$$(2.24) \quad C(B(\theta, r)) \subset B(\theta, r) \quad \text{for all } C \in \mathcal{A}^{(F)}.$$

For each  $A \in \mathcal{A}^{(F)}$  and each  $\gamma \in (0, 1)$ , define  $A_\gamma \in \mathcal{A}^{(F)}$  by

$$(2.25) \quad A_\gamma x = (1 - \gamma)Ax \oplus \gamma Qx, \quad x \in K.$$

The inequality (1.1) implies that for each  $A \in \mathcal{A}^{(F)}$ ,  $A_\gamma \rightarrow A$  as  $\gamma \rightarrow 0$  in  $\mathcal{A}^{(F)}$ . Therefore the set  $\{A_\gamma : A \in \mathcal{A}^{(F)}, \gamma \in (0, 1)\}$  is everywhere dense in  $\mathcal{A}^{(F)}$ . Let  $A \in \mathcal{A}^{(F)}$  and  $\gamma \in (0, 1)$ . Evidently,

$$\begin{aligned} \rho(A_\gamma x, F) &= \inf_{y \in F} \{ \rho((1 - \gamma)Ax \oplus \gamma Qx, y) \} \\ &\leq \inf_{y \in F} \{ \rho((1 - \gamma)Ax \oplus \gamma Qx, (1 - \gamma)y \oplus \gamma Qx) \} \\ &\leq \inf_{y \in F} \{ (1 - \gamma)\rho(Ax, y) \} \leq (1 - \gamma)\rho(x, F) \end{aligned}$$

for all  $x \in K$ . Thus

$$(2.26) \quad \rho(A_\gamma x, F) \leq (1 - \gamma)\rho(x, F) \quad \text{for all } x \in K.$$

For each integer  $i \geq 1$  denote by  $U(A, \gamma, i)$  an open neighborhood of  $A_\gamma$  in  $\mathcal{A}^{(F)}$  for which

$$(2.27) \quad U(A, \gamma, i) \subset \{B \in \mathcal{A}^{(F)} : (B, A_\gamma) \in E(2^i, 8^{-i}\gamma)\}$$

(see (2.3)). We will show that for each  $A \in \mathcal{A}^{(F)}$ , each  $\gamma \in (0, 1)$  and each integer  $i \geq 1$ , the following property holds:

P(2) For each  $B \in U(A, \gamma, i)$  and each  $x \in B(\theta, 2^i)$  satisfying  $\rho(x, F) \geq 4^{-i}$ , the inequality  $\rho(Bx, F) \leq (1 - 2^{-1}\gamma)\rho(x, F)$  is true.

Indeed, let  $A \in \mathcal{A}^{(F)}$ ,  $\gamma \in (0, 1)$  and let  $i \geq 1$  be an integer. Assume that

$$(2.28) \quad B \in U(A, \gamma, i), \quad x \in B(\theta, 2^i) \quad \text{and} \quad \rho(x, F) \geq 4^{-i}.$$

Using (2.17), (2.18) and (2.19) we see that

$$\begin{aligned} \rho(Bx, F) &\leq \rho(A_\gamma x, F) + 8^{-i}\gamma \leq (1 - \gamma)\rho(x, F) + 8^{-i}\gamma \\ &\leq (1 - \gamma)\rho(x, F) + 2^{-1}\gamma\rho(x, F) \leq (1 - 2^{-1}\gamma)\rho(x, F). \end{aligned}$$

Thus property P(2) holds for each  $A \in \mathcal{A}^{(F)}$ , each  $\gamma \in (0, 1)$  and each integer  $i \geq 1$ . Define

$$\mathcal{F} = \bigcap_{q=1}^{\infty} \cup \{U(A, \gamma, i) : A \in \mathcal{A}^{(F)}, \gamma \in (0, 1), i \geq q\}.$$

Clearly  $\mathcal{F}$  is a countable intersection of open everywhere dense sets in  $\mathcal{A}^{(F)}$ . Let  $B \in \mathcal{F}$ . To show that  $B$  is contractive with respect to  $F$  it is sufficient to show that for each  $r > 0$  and each  $\epsilon \in (0, 1)$  there is  $\kappa \in (0, 1)$  such that  $\rho(Bx, F) \leq \kappa\rho(x, F)$  for each  $x \in B(\theta, r)$  satisfying  $\rho(x, F) \geq \epsilon$ . Let  $r > 0$  and  $\epsilon \in (0, 1)$ . Choose a natural number  $q$  such that  $2^q > 8r$  and  $2^{-q} < 8^{-1}\epsilon$ . There exist  $A \in \mathcal{A}^{(F)}$ ,  $\gamma \in (0, 1)$  and an integer  $i \geq q$  such that  $B \in U(A, \gamma, i)$ . By property P(2), for each  $x \in B(\theta, r) \subset B(\theta, 2^i)$  satisfying  $\rho(x, F) \geq \epsilon > 2^{-i}$ , the following inequality holds:  $\rho(Bx, F) \leq (1 - 2^{-1}\gamma)\rho(x, F)$ . Thus  $B$  is contractive with respect to  $F$ . This completes the proof of Theorem 2.2.

#### REFERENCES

1. Ya. I. Alber, S. Guerre-Delabriere and L. Zelenko, *The principle of weakly contractive mappings in metric spaces*. Comm. Appl. Nonlinear Anal. (1) 5(1998), 45–68.
2. H. H. Bauschke, J. M. Borwein and A. S. Lewis, *The method of cyclic projections for closed convex sets in Hilbert space*. Recent Developments in Optimization Theory and Nonlinear Analysis, Contemp. Math. 204(1997), 1–38.
3. J. M. Borwein, W. B. Moors and X. Wang, *Generalized subdifferentials: a Baire categorical approach*. Preprint, 1999.
4. F. S. De Blasi and J. Myjak, *Sur la convergence des approximations successives pour les contractions non linéaires dans un espace de Banach*. C. R. Acad. Sci. Paris 283(1976), 185–187.
5. K. Goebel and W. A. Kirk, *Topics in Metric Fixed Point Theory*. Cambridge University Press, Cambridge, 1990.
6. K. Goebel and S. Reich, *Uniform Convexity, Hyperbolic Geometry, and Nonexpansive Mappings*. Marcel Dekker, New York and Basel, 1984.
7. A. D. Ioffe and A. J. Zaslavski, *Variational principles and well-posedness in optimization and calculus of variations*. SIAM J. Control Optim, accepted for publication.
8. M. A. Krasnosel'skii and P. P. Zabreiko, *Geometrical Methods of Nonlinear Analysis*. Springer, Berlin, 1984.
9. J. Myjak, *Orlicz type category theorems for functional and differential equations*. Dissert. Math. (Rozprawy Mat.) 206(1983), 1–81.
10. E. Rakotch, *A note on contractive mappings*. Proc. Amer. Math. Soc. 13(1962), 459–465.
11. S. Reich and I. Shafrir, *Nonexpansive iterations in hyperbolic spaces*. Nonlinear Anal. 15(1990), 537–558.
12. A. J. Zaslavski, *Existence of solutions of optimal control problems without convexity assumptions*. Nonlinear Anal., accepted for publication.

Department of Mathematics  
 The Technion-Israel Institute of Technology  
 32000 Haifa  
 Israel  
 email: sreich@tx.technion.ac.il  
 ajzasl@tx.technion.ac.il

## LINE BUNDLES AND CONJUGACY THEOREMS FOR TOROIDAL LIE ALGEBRAS

A. PIANZOLA

Presented by Robert V. Moody, FRSC

**ABSTRACT.** We link the Picard group of  $\text{Spec } R$  to the question of conjugacy of maximal abelian diagonalizable subalgebras of  $R \otimes \mathfrak{g}$ .

**RÉSUMÉ.** Nous faisons le lien entre le groupe de Picard de  $\text{Spec } R$  et la question de conjugation de sous-algèbres abéliennes maximales diagonalisables de  $R \otimes \mathfrak{g}$ .

Throughout  $k$  will denote a field of characteristic zero. Unless specifically mentioned otherwise *all algebras, tensor products, vector spaces, and schemes are over  $k$ .*

One of the central results of classical Lie theory is Chevalley's theorem establishing that all split Cartan subalgebras of a simple finite dimensional Lie algebra  $\mathfrak{g}$  are conjugate under its adjoint group. The analogous result for invariant (*i.e.*, symmetrizable) Kac-Moody algebras is due to Peterson and Kac (see [PK] and also Ch. 7 of [MP]). As a consequence of their work one knows that all maximal abelian  $k$ -diagonalizable subalgebras of the loop algebra  $k[t, t^{-1}] \otimes \mathfrak{g}$  are conjugate. (We reserve the terminology "Cartan subalgebra" for nilpotent subalgebras which are self-normalized. See [BP].) Now it is reasonable to expect that conjugacy questions for loop algebras, or more generally for algebras of the form  $R \otimes \mathfrak{g}$ , can be dealt with in a direct fashion. The following result is a small step in this direction.

**THEOREM 1.** *Let  $\mathfrak{g}$  be a finite dimensional split simple Lie algebra and  $\mathcal{G}$  its simply connected Chevalley-Demazure group scheme. Let  $R$  be an integral domain and  $\mathfrak{X} = \text{Spec } R$  its corresponding scheme. Assume that the Picard group of  $\mathfrak{X}$  is trivial and  $\mathfrak{X}(k)$  is not empty. Then all regular maximal abelian  $k$ -diagonalizable subalgebras of  $R \otimes \mathfrak{g}$  are conjugate under  $\mathcal{G}(R)$ .*

Let  $\mathfrak{g}$ ,  $\mathcal{G}$ ,  $\mathfrak{X}$ , and  $R$  be as in the statement of Theorem 1. The residue field of an element  $x$  of  $\mathfrak{X}$  will be denoted by  $k(x)$ . For convenience in what follows

---

Received by the editors November 11, 1999.

The author was supported by NSERC operating grant A9343. He also expresses his sincere gratitude to Olivier Mathieu for his encouragement and insightful observations all along the development of this work.

AMS subject classification: 14L15, 17B01, 22E65.

© Royal Society of Canada 2000.

the group  $\mathfrak{G}(k(x))$  will be denoted simply by  $\mathfrak{G}(x)$ , and the corresponding group homomorphism  $\mathfrak{G}(R) \rightarrow \mathfrak{G}(x)$  by  $P \mapsto P(x)$ .

The constructions of the last paragraph above can be repeated, *mutatis mutandi*, if we replace  $\mathfrak{G}$  by its Lie algebra functor  $\mathfrak{g}(\ )$ . Since  $\mathfrak{g}$  is finite dimensional we have that  $\mathfrak{g}(\ ) = \text{Hom}_{k\text{-alg}}(S(\mathfrak{g}^*), \ )$ . Thus  $\mathfrak{g}(F) = F \otimes \mathfrak{g}$  for any associative commutative unital algebra  $F$ . In particular  $\mathfrak{g} \simeq \mathfrak{g}(k)$ .

Let  $f_{\text{reg}} \in S(\mathfrak{g}^*)$  be the polynomial function defining the basic Zariski open dense set of regular elements of  $\mathfrak{g}$  (see [Bbk, Ch. VII]). Let  $F$  as before be an associative commutative unital algebra. Since  $f_{\text{reg}}$  is defined over  $k$ , we can think of it as a polynomial function on the free  $F$ -module  $\mathfrak{g}(F)$ . An element  $p$  of  $\mathfrak{g}(F)$  will be said to be *regular*<sup>1</sup> if  $f_{\text{reg}}(p)$  is a unit of  $F$ , and to be *k-diagonalizable* if  $\text{ad } p$  is diagonalizable when viewed as a  $k$ -linear endomorphism of  $\mathfrak{g}(F)$ . Finally a subalgebra of  $\mathfrak{g}(F)$  will be said to be *regular* if it contains a regular element.

PROPOSITION 1. *Let  $p \in \mathfrak{g}(R)$ . Then*

- (i) *If  $p$  is regular then  $p(x) \in \mathfrak{g}(x)$  is regular for all  $x \in \mathfrak{X}$ .*
- (ii) *If  $p$  is k-diagonalizable then  $\text{ad } p(x) \in \text{End}_{k(x)\text{-lin}} \mathfrak{g}(x)$  is k-diagonalizable for all  $x \in \mathfrak{X}$ .*
- (iii) *Assume that  $p$  is k-diagonalizable and  $f_{\text{reg}}(p) \neq 0$ . Then  $p$  is regular. In addition if  $x_0 \in \mathfrak{X}(k)$ , then  $p(x)$  and  $p(x_0)$  belong to the same orbit under the adjoint action of  $\mathfrak{G}(x)$  on  $\mathfrak{g}(x)$ .*

PROOF. The first two parts are easy. From the assumptions in (iii) one easily concludes that  $f_{\text{reg}}(p) \in k^\times$ , hence that  $p$  is regular. Given  $x \in \mathfrak{X}$  then, there is no loss of generality in assuming that  $p(x)$  and  $p(x_0)$  belong to a split Cartan subalgebra  $\mathfrak{h}$  of  $\mathfrak{g}(x)$ . Now if these two elements were not to belong to the same  $\mathfrak{G}(x)$ -orbit, there would exist a polynomial function  $f \in S(\mathfrak{h}^*)^W$  which would distinguish them. That this is not the case follows from the following two observations: Firstly that  $f$  is a linear combination of polynomial functions of the form  $\mathfrak{h} \ni h \mapsto \text{tr}_V(\rho(h))^n$  where  $n \in \mathbb{N}$  and  $\rho: \mathfrak{g}(x) \rightarrow \text{gl}(V)$  is a finite dimensional representation of  $\mathfrak{g}(x)$ , and secondly that the eigenvalue assumption on  $\text{ad } p$  implies that the value of  $\text{tr}_V(\rho(p(x)))$  does not depend on  $x \in \mathfrak{X}$ . ■

Fix an element  $x_0$  of  $\mathfrak{X}(k)$ . Let  $p \in \mathfrak{g}(R)$  be regular and  $k$ -diagonalizable, and set  $p_0 = p(x_0)$ . Proposition 1 (iii) yields that  $p_0$  belongs to a unique split Cartan subalgebra  $\mathfrak{h}_0$  of  $\mathfrak{g}$ . Let  $\mathfrak{T}_0$  be the split torus of  $\mathfrak{G}$  corresponding to  $\mathfrak{h}_0$ . Once again we invoke Proposition 1 (iii), this time to see that when  $p$  is viewed as an element of  $\text{Hom}_{k\text{-alg}}(S(\mathfrak{g}^*), R)$ , it factors through the ideal defining the Zariski closed orbit  $\mathfrak{G}(k) \cdot p_0 \subset \mathfrak{g}$  (here and in what follows  $\cdot$  denotes the appropriate adjoint action). As a consequence we deduce the existence of a compatible morphism of schemes  $\Psi_p: \mathfrak{X} \rightarrow \mathfrak{G}/\mathfrak{T}_0$ . The next result is then clear.

<sup>1</sup> This definition was suggested to me by J-P. Serre. See also Exposé XIII of SGA.

PROPOSITION 2. *The following are equivalent.*

- (i)  $\mathfrak{p}$  can be conjugated to  $\mathfrak{p}_0$  by  $\mathfrak{G}(R)$ .
- (ii) There exists a morphism  $\widehat{\Psi}_{\mathfrak{p}}: \mathfrak{X} \rightarrow \mathfrak{G}$  rendering the following diagram commutative

$$\begin{array}{ccc}
 & & \mathfrak{G} \\
 & \nearrow \widehat{\Psi}_{\mathfrak{p}} & \downarrow q \\
 \mathfrak{X} & \xrightarrow{\quad} & \mathfrak{G}/\mathfrak{I}_0 \\
 & \searrow \Psi_{\mathfrak{p}} & 
 \end{array}$$

- (iii) The pull-back  $\mathfrak{X} \times_{\mathfrak{G}/\mathfrak{I}_0} \mathfrak{G}$  is a trivial principal  $\mathfrak{I}_0$ -bundle over  $\mathfrak{X}$ . ■

PROOF OF THEOREM 1. Let  $\mathfrak{h}$  be a maximal abelian and  $k$ -diagonalizable subalgebra of  $\mathfrak{g}(R)$  containing a regular element  $\mathfrak{p}$  of  $\mathfrak{g}(R)$ . The assumption on  $\text{Pic}(\mathfrak{X})$  ensures that the bundle of Proposition 2 (iii) is trivial, hence that there exists  $P \in \mathfrak{G}(R)$  such that  $P \cdot \mathfrak{h} \subset \mathfrak{z}_{\mathfrak{g}(R)} \mathfrak{p}_0 = R \otimes \mathfrak{h}_0$ . But since  $P \cdot \mathfrak{h}$  is  $k$ -diagonalizable we have that  $P \cdot \mathfrak{h} \subset k \otimes \mathfrak{h}_0$ . Finally because  $\mathfrak{h}$  is maximal, this last inclusion is in fact an equality. ■

REMARK 1. Let  $\mathfrak{h}$  be an abelian and  $k$ -diagonalizable subalgebra of  $\mathfrak{g}(R)$ . If  $F$  is the field of quotients of  $R$ , then  $F \otimes \mathfrak{h}$  is an abelian diagonalizable subalgebra of  $\mathfrak{g}(F)$ . As a consequence of this  $\mathfrak{h} \subset \mathfrak{k}$  for some split Cartan subalgebra  $\mathfrak{k}$  of  $\mathfrak{g}(F)$  [Slg, I, §3, Theorem 2]. It then follows from  $\mathfrak{h}$  being  $k$ -diagonalizable that  $\dim_k \mathfrak{h} \leq \text{rank}(\mathfrak{g})$ . If this last is an equality then  $\mathfrak{h}$  is dense in  $\mathfrak{k}$ , hence regular.

REMARK 2. The assumption on  $\text{Pic}(\mathfrak{X})$  is not superfluous as can be easily seen from the case  $\mathfrak{X} = \mathfrak{G}/\mathfrak{I}_0$ .

REMARK 3. Toroidal Lie algebras correspond to the case when  $\mathfrak{X}$  is a split torus. Since  $R$  is then a noetherian factorial domain (Laurent polynomials in finitely many variables)  $\text{Pic}(\mathfrak{X})$  is trivial and the Theorem applies.

REMARK 4. Since  $\mathfrak{g}(R)$  is perfect, it admits a universal central extension  $\epsilon$ . The elements of  $\mathfrak{G}(R)$  extend to automorphisms of  $\epsilon$  in a natural way. Theorem 1 then holds if we replace  $\mathfrak{g}(R)$  by  $\epsilon$ , and  $\mathfrak{h}_0$  by  $\mathfrak{h}_0 + \text{centre}(\epsilon)$ .

REMARK 5. Theorem 1 allows us to describe the structure of the group of automorphisms of  $\mathfrak{g}(R)$ . This as well the case of non regular maximal abelian and  $k$ -diagonalizable will be considered in future work.

REFERENCES

[BP] Y. Billig and A. Pianzola, *On Cartan subalgebras*. J. Algebra **171**(1995), 397–412.  
 [Bbk] N. Bourbaki, *Groupes et algèbres de Lie, Ch. 7 et 8*. Hermann, 1975.  
 [DG] M. Demazure et P. Gabriel, *Groupes Algébriques*. Tome I, North Holland, 1970.  
 [SGA] M. Demazure et A. Grothendieck, *Séminaire de Groupes Algébriques*. Lecture Notes in Math. **151–153**, Springer-Verlag, 1970.  
 [Slg] G. Seligman, *Rational methods in Lie algebras*. Lecture Notes in Pure and Appl. Math. **17**, M. Dekker, 1976.

- [MP] R. V. Moody and A. Pianzola, *Lie algebras with triangular decompositions*. J. Wiley & Sons, 1995.
- [PK] D. Peterson and V. Kac, *Infinite flag varieties and conjugacy theorems*. Proc. Nat. Acad. Sci. U.S.A. **80**(1983), 1778–1782.

*Department of Mathematical Sciences*  
*University of Alberta*  
*Edmonton, Alberta*  
*T6G 2G1*