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

Vol. XI, No. 4 August 1989 août

CONTENTS

H. OSADA and N. TERAI
Generalization of Lucas' Theorem for Fermat's quotient 115

K. OTA
On p-integrality of a formal group obtained from a hypergeometric function 121

B. CHOCZEWSKI and M. KUCZMA
A remark on doubly stochastic measures and functional equations 127

A. O. BAHYA
Un critere de nuclearité pour certains espaces de type (M) 133

G. GRÄTZER, F.R.S.C. and H. LAKSER
Congruence lattices, automorphism groups of finite lattices and planarity 137

H. D'SOUZA
A general result on local spannedness 143

GENERALIZATION OF LUCAS' THEOREM FOR FERMAT'S QUOTIENT

Hiroyuki Osada

and Nobuhiro Terai

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

Abstract: We define the Fermat's quotient $q_p(m)$ by $q_p(m) = \frac{m^{p-1} - 1}{p}$ where p is an odd prime and (m, p) = 1. Lucas proved that $q_p(2)$ is a square only for p = 3, 7. The purpose of the present paper is to study the equations $q_p(m) = x^l$ where l is a prime.

§ 1. Introduction

Let p be an odd prime number and let m be a positive integer prime to p. We define the Fermat's quotient $q_p(m)$ by $q_p(m) = \frac{m^{p-1} - 1}{p}$. Lucas ([2],[4]) proved that $q_p(2)$ is a square only for p = 3,7.

In the present paper,we consider,as a generalization of Lucas' Theorem, whether the equation

$$q_p(m) = x^l$$

has solutions or not, where l is a prime and x is a positive integer. We prove the following three theorems. :

Theorem 1. *If p is a prime* > 3, *then the equation*

(1) $$q_p(m) = x^2$$

has only solution $(p, m, x) = (5, 3, 4)$.

Theorem 2. If r is an odd prime with $r \neq p$ and the equation

$$q_p(r) = x^r \tag{2}$$

has solutions, then p and r satisfy the congruences

$$2^{r-1} \equiv 1 \pmod{r^2} \quad \text{and} \quad p^{r-1} \equiv 1 \pmod{r^2}.$$

Theorem 3. If l is an odd prime, then the equation

$$q_p(2) = x^l \tag{3}$$

has only solution $p = 3$.

§ 2. Proofs of the theorems

We first prove theorem 1. Then we use the following three Lemmas.

Lemma 1. (Ljunggren [3])

Let p be an odd prime. The Diophantine equation

$$x^4 - py^2 = 1$$

has no solutions in positive integers x and y if $p \neq 5, 29$.

When $p = 5$ or 29, there is only one solution, viz., $(x, y) = (3, 4)$ and $(99, 1820)$ respectively.

Lemma 2. (Nagell [5],[6])

Let n be an odd integer ≥ 3 and let A be a square-free integer ≥ 1. If the class number of the quadratic field $\mathbb{Q}(\sqrt{-A})$ is not

divisible by n, the Diopantine equation

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

has no solutions in integers x and y for y odd and ≥ 1, apart from $x = \pm 11$, $y = 3$ for $A = 2$ and $n = 5$.

The following result is well known. (For the proof, e.g. , see Adachi [1].)

Lemma 3. Let K be the quadratic field with discriminant d. Then the class number of K is small than $\frac{d}{4}$, if $d > 0$, and $\frac{|d|}{3}$, if $d < 0$.

Now suppose $p \equiv 1 \pmod 4$. Since $\frac{p-1}{4}$ is a positive integer, the equation (1) becomes

$$(4) \qquad (m^{(p-1)/4})^4 - px^2 = 1.$$

By Lemma 1, we see that the equation (4) has only solution

$$(p, m, x) = (5, 3, 4).$$

Suppose $p \equiv 3 \pmod 4$. Then $\frac{p-1}{2}$ is odd ≥ 3 since $p \geq 3$. By (1), we have

$$(5) \qquad px^2 + 1 = (m^2)^{(p-1)/2}.$$

We denote by h the class number of the quadratic field $\mathbb{Q}(\sqrt{-p})$. If follows from Lemma 3 that h is small than $\frac{p-1}{2}$ and so h is not divisible by $\frac{p-1}{2}$. Therefore, by Lemma 2, we see that the equation (5) has no solutions (p, m, x). Thus this completes the proof of Theorem 1.

We next prove Theorem 2. By (2), we have

$$(r^{(p-1)/2} + 1)(r^{(p-1)/2} - 1) = px^r$$

Hence we get the following four cases ;
$(r^{(p-1)/2} + 1, r^{(p-1)/2} - 1) =$ (a): $(2y^r, 2^{r-1}pz^r)$, (b): $(2py^r, 2^{r-1}z^r)$, (c): $(2^{r-1}y^r, 2pz^r)$ or (d): $(2^{r-1}py^r, 2z^r)$, where y and z are positive integers with $x = 2yz$.

Suppose $p = 3$. Then (2) becomes $r^2 - 1 = 3x^r$. Since we have

$$r^2 - 1 < 3x^r \quad \text{for} \quad x > 1$$

, (2) has no solutions.

Suppose $p > 3$. We first consider case (a). Since $r^{(p-1)/2} + 1 = 2y^r$ and $\frac{p-1}{2} \geq 2$, we get

$$1 \equiv 2\, y^r \pmod{r^2}$$

, so $$1 \equiv 2^{r-1}y^{r(r-1)} \pmod{r^2}.$$

Since y is prime to r and r is an odd prime, $y^{r(r-1)} \equiv 1 \pmod{r^2}$ holds. Thus we obtain the congruence $2^{r-1} \equiv 1 \pmod{r^2}$. Since we also have $r^{(p-1)/2} - 1 = 2^{r-1}pz^r$, we get

$$-1 \equiv 2^{r-1}pz^r \equiv pz^r \pmod{r^2}$$

, so $$1 \equiv p^{r-1}z^{r(r-1)} \equiv p^{r-1} \pmod{r^2}.$$

Hence we obtain the congruence $p^{r-1} \equiv 1 \pmod{r^2}$.

We next consider case (b). Then since $r^{(p-1)/2} - 1 = 2^{r-1}z^r$, we get

$$-1 \equiv 2^{r-1}z^r \pmod{r^2}$$

, hence $$1 \equiv 2^{(r-1)^2}z^{r(r-1)} \pmod{r^2}.$$

Since $2^{r(r-1)} \equiv z^{r(r-1)} \equiv 1 \pmod{r^2}$, we get

$$1 \equiv 2^{(r-1)^2}z^{r(r-1)} \equiv 2^{(r-1)^2} = 2^{r(r-1)-(r-1)} \equiv 2^{-(r-1)} \pmod{r^2}$$

. Therefore we obtain the cogruence $2^{r-1} \equiv 1 \pmod{r^2}$. Since we also have $r^{(p-1)/2} + 1 = 2py^r$, we get

$$1 \equiv 2py^r \pmod{r^2}$$

, so $1 \equiv 2^{r-1}p^{r-1}y^{r(r-1)} \equiv p^{r-1} \pmod{r^2}$.

Thus we obtain the congruence $p^{r-1} \equiv 1 \pmod{r^2}$.

Simiraly case (c) and case (d) will also yield the congruences

$$2^{r-1} \equiv 1 \pmod{r^2} \quad \text{and} \quad p^{r-1} \equiv 1 \pmod{r^2}$$

respectively. Hence this completes the proof of Theorem 2.

Finally we prove Theorem 3. The equation (3) clearly has a solution $p = 3$, so we consider (3) with $p > 3$. By (3), we have

$$(2^{(p-1)/2} + 1)(2^{(p-1)/2} - 1) = px^l.$$

Therefore we get $(2^{(p-1)/2} + 1, 2^{(p-1)/2} - 1) = (py^l, z^l)$ or (y^l, pz^l), where y and z are positive integers with $x = yz$. Thus it suffices to show that the eqation

$$2^{(p-1)/2} = t^l \pm 1$$

, where p is a prime > 3 and t is odd ≥ 1, has no solutions (p, l, t). We have $2^{(p-1)/2} = (t \pm 1)(\frac{t^l \pm 1}{t \pm 1})$ and we easily see that $t \pm 1$ and $\frac{t^l \pm 1}{t \pm 1}$ are relatively prime. Hence we obtain

$$(t \pm 1, \frac{t^l \pm 1}{t \pm 1}) = (1, 2^{(p-1)/2}) \text{ or } (2^{(p-1)/2}, 1)$$

, which are obviously impossible since $p > 3$ and t is odd. Therefore this completes the proof of Theorem 3.

References

[1] Adachi, N. , The Diophantine equation $x^2 \pm ly^2 = z^l$ connected with Fermat's Last Theorem, Tokyo J. Math. vol. 11, No. 1

(1988), 85 - 94.

[2] Dickson, L.E. , History of the Theory of Numbers, vol.I , pp. 106 , Chelsea , 1971.

[3] Ljunggren, W., Some remarks on the Diophantine equations $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$, J. London Math. Soc., 41 (1966), 542 - 544.

[4] Lucas, E., Théorie des nomble, Gauthien - Villans , Paris , 1891, Reprinted by A. Blanchard, Paris, 1961, pp. 423.

[5] Nagell, T., Sur l'mpossibilité de quelques équation à deux indéterminées, Norsk Mat. Forenings Skr. , Ser.I , No. 13 (1923), 65 - 82.

[6] Nagell, T., Contributions to the theory of a category of Diophantine equetions of the second degree with two unknowns , Nova Acta Soc. Sci. Upsal. , Ser. IV , vol. 16, No. 2(1955), 1 - 38.

Hiroyuki Osada
Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Tokyo 171
Japan

Nobuhiro Terai
Department of Mathematics
School of Science and Engineering
Waseda University
Okubo, Shinjuku, Tokyo 160, Japan

Received February 24, 1989

ON P-INTEGRALITY OF A FORMAL GROUP OBTAINED FROM A HYPERGEOMETRIC FUNCTION

Kaori Ota[1]

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

§1. Introduction

In this paper, we consider P-integrality of a formal group $F_\theta(x,y)$ obtained from a hypergeometric function. The definition of $F_\theta(x,y)$ is as follows (cf. [1]):

Let N be an integer greater than 1, i an integer between 1 and $N-1$ and P a prime greater than N. Set $\theta = \frac{i}{N}$. For each positive integer n, set

$$a_\theta(n) = \begin{cases} \dfrac{\theta(\theta+1)\dots(\theta+k-1)}{k!} & \text{if } n \equiv 1 \pmod N \text{ and } k = \dfrac{n-1}{N} \geq 1, \\ 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Define

$$f_\theta(x) = \sum_{n=1}^{\infty} \frac{a_\theta(n)}{n} x^n \in \mathbb{Q}[[x]],$$

and

$$F_\theta(x,y) = f_\theta^{-1}\left(f_\theta(x) + f_\theta(y)\right) \in \mathbb{Q}[[x,y]].$$

Honda [1] gave a condition on P-integrality of $F_\theta(x,y)$ in terms of the p-adic order $\mathrm{ord}_P(a_\theta)$ of a_θ, which can be computed easily. (The valuation is normalized so that $\mathrm{ord}_P(P) = 1$.) We say that $F_\theta(x,y)$ is P-integral if $F_\theta(x,y) \in \mathbb{Z}_P[[x,y]]$. If d is the order of P modulo N, i.e., d is the least power of P such that $P^d \equiv 1 \pmod N$, for

[1] *) This work was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) through N. Yui's grants No. A8566 and No. A9451.

each ℓ in $\{1,2,\ldots,d-1\}$ let m_ℓ , J_ℓ be the integers between 1 and N-1 satisfying

(1) $P^\ell m_\ell \equiv 1 \pmod N$

(2) $P^\ell J_\ell \equiv 1 \pmod N$, respectively .

Then F_θ is P-integral if and only if

(3) $m_\ell - J_\ell > 0$ for each $\ell \in \{1,2,\ldots d-1\}$, and F_θ is of Lubin-Tate type if and only if F_θ is P-integral and $\mathrm{ord}_P\left(a_\theta(P^d)\right) = d-1$. Let ϕ denote the Euler phi function. We can prove:

Proposition 1. *If* $\phi(N) \geq 3$, *for each* $1 \in \{1,2,\ldots,N-1\}$ *there always exist infinitely many primes* P *such that* F_θ *is not P-integral for* $\theta = \frac{1}{N}$.

For a prime $P > N$, let $B(N,P)$ be the cardinality of a set $\left\{ 1\leq i\leq N-1 \,\middle|\, F_\theta \text{ is not P-integral for } \theta = \frac{i}{N} \right\}$. Then:

Proposition 2. $B(N,P) = 0$ *if and only if* $P \equiv 1 \pmod N$. $B(N,P) = 1$ *if and only if* $P \equiv -1 \pmod N$. *If* $d = \phi(N)$ *and* ($N\geq 7$ *or* $N=5$) , *then* $B(N,P) = N-1$.

Proposition 3. *Let* N, i, P, d *be as before. If* F_θ *is* P-*integral, then it is of Lubin-Tate type.*

Because of the condition (3), the larger d is, the more rarely F_θ becomes P-integral. However, we do have the following result:

Proposition 4. *For a given* $d > 1$, *let* N *be* d^2 *and* P *a prime greater than* N *such that* $P \equiv 1 \pmod{d}$ *and that the order of* P *modulo* N *is* d. *Then* F_θ *is P-integral for* $\theta = \frac{i}{N}$ *if and only if* $i = d$ *or* $d^2 - d + 1$.

§2. Sketch of Proof

Proposition 1. *Take a prime* P *such that* $P \not\equiv \pm 1 \pmod{N}$. *If* F_θ *is P-integral,* F_θ *is not Q-integral for a prime* Q *congruent to* $-P$ *modulo* N.

Proposition 2. *It is easy to check that*

$$B(N,P) = 0 \text{ if and only if } P \equiv 1 \pmod{N}$$

and that

$$P \equiv -1 \pmod{N} \text{ implies } B(N,P) = 1 .$$

Suppose that $B(N,P) = 1$ and $d > 2$. Then $\frac{1}{N}$ is the only θ for which F_θ is not P-integral. Find $m_1,\dots,m_{d-1}$ satisfying (1). Let i_1 be an integer in $\{1,\dots,N-1\}$ congruent to P modulo N and find $j_1^{(1)},\dots,j_{d-1}^{(1)}$ satisfying (2) for $i = i_1$. Since F_{θ_1} for $\theta_1 = \frac{i_1}{N}$ is P-integral, we see that $m_{d-1} - m_1 > 0$. By taking i_2 in $\{1,\dots,N-1\}$ congruent to P^2 modulo N and finding $j_1^{(2)},\dots,j_{d-1}^{(2)}$ satisfying (2) for $i = i_2$, we see that $m_1 - j_1^{(2)} = m_1 - m_{d-1} < 0$. This implies that F_{θ_2} for $\theta_2 = \frac{i_2}{N}$ is not P-integral. A contradiction. Hence $d = 2$.

Now take i to be 2. Then j_1 satisfying (2) for $i = 2$ is either $2m_1$ or $2m_1 - N$, and $m_1 - j_1 > 0$ implies that $j_1 = 2m_1 - N$ and that $m_1 > N/2$.

Suppose that

$m_1 > \frac{\ell-1}{\ell} N$ for some $\ell \in \{2,\dots,N-2\}$. By taking i to be $\ell+1$ and considering $m_1 - J_1$ for J_1 satisfying (2) for $i = \ell+1$, we can conclude that

$$m_1 > \frac{\ell}{\ell+1} N .$$

Hence $N \frac{N-2}{N-1} < m_1 < N$ and we get $m_1 = N-1$, which is congruent to P modulo N.

Suppose that $d = \phi(N)$. Then $\{m_1,\dots,m_{d-1}\}$ satisfying (1) together with 1 form a complete set of representatives for $(\mathbf{Z}/N\mathbf{Z})^*$. If $(i,N) = 1$, $J_1,\dots,J_{d-1}$ satisfying (2) are all relatively prime to N and mutually distinct. If $1 \notin \{J_1,\dots,J_{d-1}\}$, then $\{J_1,\dots,J_{d-1}\} = \{m_1,\dots,m_{d-1}\}$ and (3) can not be satisfied for some ℓ. If $J_\ell = 1$ for some $\ell \in \{1,\dots,d-1\}$, then $i = m_{d-\ell}$ and $m_{d-\ell} = \max\{m_t \mid 1 \le t \le d-1\}$. Hence $m_{d-\ell} = N-1$ and $P^{2\ell} \equiv 1 \pmod N$, so that $\ell = \frac{d}{2}$. If $d \ge 3$, there exists an integer k in $\{1,\dots,d-1\}$ such that $1 < m_k < m_\ell$. Take the minimum, m_{k_o}, of all such m_k's. Then $m_{k_o} - J_{k_o} \le 0$ and (3) is not satisfied for k_o. If $d = 1$ or 2, then $N = 2$, 3, 4 or 6; these values of N are excluded by the hypothesis. If $(i,N) = t > 1$, set $i = ti'$ and $N = tN'$. Then $(i',N') = 1$ and we can prove the assertion in a similar way by considering i', N' instead of i, N.

Proposition 3. *We only need to compute* $\mathrm{ord}_P\left(a_\theta(P^d)\right)$. *Set* $f = \frac{P^d-1}{N}$ *and* $\theta = \frac{i}{N}$. *For each* ℓ *in* $\{1,\dots,d-1\}$, *choose* t_ℓ *such that*

$$1 \le t_\ell \le P^\ell - 1 \quad \text{and} \quad t_\ell \equiv -iN^{-1} \pmod{P^\ell} .$$

Note that $t_1 \le t_2 \le \ldots \le t_{d-1}$. Then the number of integers i , $i + N, \ldots, i + (f-1)N$ which are divisible by P^ℓ is equal to $\left[\frac{f-1-t_\ell}{P^\ell}\right] + 1$, where $[x]$ denotes the largest integer not exceeding x for any real x . Hence

$$\mathrm{ord}_P\left\{i(i+N) \ldots (i+(f-1)N)\right\} = \sum_{\ell=1}^{d-1} \left[\frac{f-1-t_\ell}{P^\ell}\right] + (d-1) .$$

On the other hand, for each ℓ in $\{1,\ldots,d-1\}$ we can show by using the P-integrality of F_θ that, if $t_{\ell-1} < t_\ell$, no integer among $f-1-t_{\ell-1}$, $f-1-t_{\ell-1}-1, \ldots, f-1-(t_\ell-1)$ is divisible by P^ℓ . Here we set $t_0 = 0$. Hence $\left[\frac{f}{P^\ell}\right] = \left[\frac{f-1-t_\ell}{P^\ell}\right]$. So we have

$$\mathrm{ord}_P(f!) = \sum_{\ell=1}^{d-1}\left[\frac{f}{P^\ell}\right] = \sum_{\ell=1}^{d-1}\left[\frac{f-1-t_\ell}{P^\ell}\right] .$$

Therefore

$$\begin{aligned}\mathrm{ord}_P\left(a_\theta(P^d)\right) &= \mathrm{ord}_P\left\{i(i+N) \ldots (i+(f-1)N)\right\} - \mathrm{ord}_P\left(f!N^f\right) \\ &= d - 1 .\end{aligned}$$

Proposition 4. Let $X_d(P)$ be a set

$$\left\{ 1 \le i \le N-1 \mid F_\theta \text{ is P-integral for } \theta = \frac{i}{N} \right\} .$$

For each ℓ in $\{1,\ldots,d-1\}$, let m_ℓ be the integer satisfying (1). Since $P \equiv 1 \pmod d$, $m_\ell \equiv 1 \pmod d$ for each ℓ . So $m_\ell = 1 + dn_\ell$ for some $n_\ell \in \{1,\ldots,d-1\}$. Here $n_1,\ldots,n_{d-1}$ are mutually distinct, so that $\{n_1,\ldots,n_{d-1}\} = \{1,\ldots,d-1\}$. We see that an integer J_ℓ satisfying (2) for $i = d$ is d for each ℓ . Hence $m_\ell - J_\ell > 0$ for each ℓ . For $i = d^2 - d + 1$, we can show that $m_\ell - J_\ell = d$ for each ℓ , where J_ℓ are integers satisfying (2) for this i . To prove the converse, let i be an element of $X_d(P)$, find $J_1,\ldots,J_{d-1}$ satisfying

(2) and set $\min\{m_\ell - j_\ell \mid 1 \le \ell \le d-1\} = t$. When $t = 1$, there exists ℓ_0 in $\{1,\dots,N-1\}$ such that $m_{\ell_0} - j_{\ell_0} = 1$. So $j_{\ell_0} \equiv 0 \pmod d$ and we get $i \equiv 0 \pmod d$. This implies that $j_\ell \equiv 0 \pmod d$ and $j_\ell = i$ for each ℓ. Hence by considering $m_k - j_k$ for k with $m_k = 1+d$, we get $i = d$. When $t > 1$, there exists ℓ_0 such that $j_{\ell_0} < d$. If $i = j_0, j_1, \dots, j_{d-1}$ are mutually distinct, each j_ℓ has a form $j_{\ell_0} + dr_\ell$, where $\{r_0,\dots,r_{d-1}\} = \{0,\dots,d-1\}$. From the P-integrality of F_θ, we see that $r_\ell = n_\ell - 1$ for $\ell \ge 1$ and that $r_0 = d-1$. Also $j_{\ell_0} \equiv i m_{\ell_0} \equiv i(1+d) \pmod{d^2}$ implies that $i \equiv 1 \pmod d$. Therefore $i = d^2 - d + 1$. For the case when $i = j_0, j_1, \dots, j_{d-1}$ are not mutually distinct, we get a contradiction.

References

[1] T. Honda, Formal groups obtained from generalized hypergeometric functions, Osaka J. Math., 9 (1972), 447-462.

Department of Mathematics
Tsuda College
Kodaira Tokyo, 187 Japan

Received March 10, 1989

A REMARK ON DOUBLY STOCHASTIC MEASURES AND FUNCTIONAL EQUATIONS

Bogdan Choczewski and Marek Kuczma

Presented by J. Aczél, F.R.S.C.

1. Let $I=[0,1]$ be the closed unit interval. A measure μ defined on the Borel subsets of the unit square $I\times I$ is called doubly stochastic if for every Borel subset $A\subset I$ we have

$$\mu(A\times I)=\mu(I\times A)=|A|,$$

where $|A|$ denotes the one-dimensional Lebesgue measure of the set A.

Let $f:I\to I$ be a function fulfilling the conditions:

(i) $f:I\to I$ is an increasing homeomorphism of I into itself and $f(x)<x$ for $x\in(0,1)$.

Several authors (cf., e.g., [5], [6]) have studied doubly stochastic measures with support contained in the set (a hairpin)

$$H = \{(x,y)\in I\times I:\ y=f(x) \text{ or } x=f(y)\}.$$

In particular, H. Sherwood and M. D. Taylor [6] have shown that, if μ is such a measure, then the function

(1) $$\varphi(x) = \mu(\{(t,f(t))\in I\times I:\ t\in[0,x]\}), \quad x\in I,$$

is a non-negative, monotonic and continuous solution of the functional equation

(2) $$\varphi[f(x)]+\varphi(x) = f(x)$$

in I; and, conversely, every non-negative, monotonic and continuous solution $\varphi:I\to\mathbb{R}$ of equation (2) generates a doubly stochastic measure μ on $I\times I$ supported on the set H and fulfilling condition (1).

2. In the present paper we are going to investigate the mutual relation between the relevant properties of φ. Instead of (2) we shall consider a slightly more general equation

(3) $$\varphi[f(x)]+\varphi(x) = h(x).$$

We assume that:

(ii) $h:I\to\mathbb{R}$ is continuous in I and such that the expression

(4) $$R(x) = h(x)-h[f(x)], \quad x\in I,$$

is non-negative in I. Moreover,

(5) $$h(0)=0,\ h(1)=1.$$

(iii) There exists a $\xi\in(0,1)$ such that the function (4) is non-decreasing in $(0,\xi)$ and non-increasing in $(\xi,1)$.

Remark 1. The choice of the values of $h(0)$ and $h(1)$ is not essential. Note that a function $\varphi:I\to\mathbb{R}$ satisfies equation (3) in I if

and only if the function $\psi(x)=a\varphi(x)+b$, $x\in I$, satisfies in I the equation $\psi[f(x)]+\psi(x) = ah(x)+2b$. Consequently if $h(0)\neq h(1)$ conditions (5) may be realized by a suitable choice of a and b.

The iterates f^n of f are defined for all integers n by the recurrence

$$f^0(x)=x,\quad f^{n+1}(x)=f[f^n(x)],\quad n\in\mathbb{Z},\ x\in I.$$

It is easily seen that for every $n\in\mathbb{Z}$ the function f^n is an increasing homeomorphism of I onto itself. Moreover, for every $x\in(0,1)$ the sequence $(f^n(x))_{n=-\infty}^{\infty}$ is strictly decreasing and

$$\lim_{n\to\infty} f^n(x) = 0\,,\qquad \lim_{n\to-\infty} f^n(x) = 1 \tag{6}$$

(cf.[3,Theorem 0.5]).

We start off with some lemmas.

On setting $x=0$ and $x=1$ in (3) we get from (5) the following

Lemma 1. *Let (i) and (ii) be fulfilled. If a function $\varphi:I\to\mathbb{R}$ satisfies equation (3) in I, then $\varphi(0)=0$ and $\varphi(1)=\frac{1}{2}$.*

Next we have

Lemma 2. *Let (i) and (ii) be fulfilled.*

a) There exists a unique function $\varphi_1:I\to\mathbb{R}$ which satisfies equation (3) in I and is continuous at $x=0$. This function is given by the formula

$$\varphi_1(x) = \sum_{n=0}^{\infty}(-1)^n h[f^n(x)]\,,\ x\in[0,1);\quad \varphi_1(1) = \frac{1}{2} \tag{7}$$

and is, in fact, continuous in the interval $[0,1)$. If, moreover, function (4) is nondecreasing in the interval $(0,\xi)$ (for a $\xi\in(0,1)$), then so is also φ_1.

b) There exists a unique function $\varphi_2:I\to\mathbb{R}$ which satisfies equation (3) in I and is continuous at $x=1$. This function is given by the formula

$$\varphi_2(0)=0\ ;\quad \varphi_2(x) = \frac{1}{2} + \sum_{n=1}^{\infty}(-1)^n(h[f^{-n}(x)]-1)\,,\ x\in(0,1] \tag{8}$$

and is, in fact, continuous in the interval $(0,1]$. If, moreover, function (4) is nonincreasing in the interval $(\xi,1)$ (for a $\xi\in(0,1)$), then φ_2 is nondecreasing in $(\xi,1)$.

Proof.

a) Suppose that a function $\varphi_1:I\to\mathbb{R}$ satisfies equation (3) in I. We have from (3) by induction

$$\varphi_1(x) = (-1)^k\varphi_1[f^k(x)] + \sum_{n=0}^{k-1}(-1)^n h[f^n(x)]\,,\ k\in\mathbb{N},\ x\in I. \tag{9}$$

By Lemma 1

(10) $$\varphi_1(0)=0,\ \varphi_1(1)=\frac{1}{2}$$

Since φ_1 is continuous at $x=0$ we must have

(11) $$\lim_{x\to 0}\varphi_1(x) = 0 .$$

Letting in (9) k tend to infinity we obtain (7) for $x\in(0,1)$ in virtue of (11) and (6). Relation (7) for all $x\in I$ (and hence also the uniqueness of φ_1) results now from (10).

The existence of φ_1 and its continuity in $[0,1)$ are a consequence of the fact that the series in (7) converges almost uniformly in $[0,1)$ ([3,Theorem 2.14]; cf. also [2]). It is a matter of straightforward verification to check that φ_1 given by (7) actually satisfies equation (3) in I.

Formula (7) implies that

(12) $$\varphi_1(x) = \sum_{n=0}^{\infty} R[f^{2n}(x)] \quad \text{for } x\in(0,1),$$

where the function R is defined by (4). If R is nondecreasing in $(0,\xi)$, then the monotonicity of φ_1 in $(0,\xi)$ results from that of R and of f^n, $n=0,2,4,\ldots$, and from the fact that for $n\geq 0$ the functions f^n map the interval $(0,\xi)$ into itself.

Assertion b) follows by the same argument when applied to the equivalent form of (3)

$$[\varphi[f^{-1}(x)]-\tfrac{1}{2}] + [\varphi(x)-\tfrac{1}{2}] = h[f^{-1}(x)]-1 .$$

As for the monotonicity statement, observe that formula (8) yields

(13) $$\varphi_2(x) = \frac{1}{2} - \sum_{n=-1}^{-\infty} R[f^{2n}(x)] \qquad \text{for } x\in(0,1).$$

Finally, we have

Lemma 3. Let (i) and (ii) be fulfilled.

a) The function φ_1 (cf.(7)) is the only nonnegative solution of equation (3) in I.

b) The function φ_2 (cf.(8)) is the only solution of equation (3) in I which is bounded from above by 1/2.

Proof.

a) Let $\varphi:I\to\mathbb{R}$ be a nonnegative solution of equation (3) in I. The equality $\varphi=\varphi_1$ (and hence the uniqueness of φ) results from [1] and from Lemma 1 (cf.also [6]). On the other hand, it follows from (12) and (10) that φ_1 actually is nonnegative in I.

Assertion b) results in a similar way.

3. The following theorem is the main result of the present paper.

Theorem 1. Let hypotheses (i)–(iii) be fulfilled, and let $\varphi: I \to \mathbb{R}$ be a solution of equation (3) in I. The following conditions are equivalent:

(α) φ is monotonic in I.

(β) φ is continuous in I.

(γ) $0 \le \varphi(x) \le \frac{1}{2}$ for $x \in I$.

A solution fulfilling (α)–(γ) exists if and only if

$$\sum_{n=-\infty}^{\infty} R[f^{2n}(x)] = \frac{1}{2} \qquad \text{for } x \in (0,1), \tag{14}$$

and if such a solution exists, it is unique and is given by formula (7), or, equivalently, formula (8).

Proof.

Assume (α). Since φ is monotonic (by Lemma 1 necessarily non-decreasing), there exist limits of $\varphi(x)$ for $x \to 0$ and $x \to 1$, and by (3)

$$\lim_{x \to 0} \varphi(x) = 0, \qquad \lim_{x \to 1} \varphi(x) = 1/2 . \tag{15}$$

Relations (15) together with Lemma 1 show that φ is continuous at $x=0$ and at $x=1$. By Lemma 2

$$\varphi = \varphi_1 = \varphi_2 . \tag{16}$$

Hence, again by Lemma 2, φ is continuous in I.

Assume (β). Then we have (16) in virtue of Lemma 2, whence (γ) results by Lemma 3.

Assume (γ). Lemma 3 implies (16). According to Lemmas 1 and 2, φ is nondecreasing in I.

The above argument shows that, if equation (3) has a solution $\varphi: I \to \mathbb{R}$ fulfilling (α)–(γ), then we must have (16), whence by (12) and (13) we obtain (14). In the other direction, if (14) holds, then $\varphi_1 = \varphi_2$. By Lemmas 2 and 3 the function φ given by (16) fulfils conditions (α)–(γ).

The uniqueness of φ as well as formulas (7) and (8) are a consequence of (16).

Remark 2. If $\varphi: I \to \mathbb{R}$ is a solution of (3), then the inequality

$$\varphi(x) \ge 0 \qquad \text{for } x \in I$$

is a consequence of (α) and (β), but alone it does not imply either; cf. Lemma 3(a) and also [6].

Remark 3. The series appearing in (14) converges almost uniformly in (0,1) and thus it represents a continuous function in (0,1), but, in general, this function need not be constant (cf. also Remark 7 below). However, if it is, the constant must be $\frac{1}{2}$. Thus condition

(14) may also be replaced by

$$\sum_{n=-\infty}^{\infty} R[f^{2n}(x)] = \text{const} \qquad \text{for } x\in(0,1). \tag{14'}$$

4. Now let us assume

(iv) There exists a $\xi\in(0,1)$ such that the function $x \mapsto x-f(x)$ is nondecreasing in $(0,\xi)$ and nonincreasing in $(\xi,1)$.

Remark 4. We have $x-f(x)=R[f^{-1}(x)]$, where R is defined by (4) with h=f. But since f is an increasing homeomorphism, the existence of a corresponding $\xi=\xi_1$ for R is equivalent to the existence of a corresponding $\xi=\xi_2$ for $R\circ f^{-1}$, the two points being related by the formula $\xi_1=f(\xi_2)$.

Taking h=f in Theorem 1 we obtain

Theorem 2. Let hypotheses (i) and (iv) be fulfilled, and let $\varphi:I\to\mathbb{R}$ be a solution of equation (2) in I. Then conditions $(\alpha),(\beta),(\gamma)$ are equivalent to each other. A solution $\varphi:I\to\mathbb{R}$ of the equation

$$\varphi[f(x)]+\varphi(x) = f(x) \tag{2}$$

exists if and only if

$$\sum_{n=-\infty}^{\infty} (f^{2n}(x)-f^{2n+1}(x)) = \frac{1}{2} \qquad \text{for } x\in(0,1). \tag{17}$$

When it exists such a solution is unique and is given by the formula

$$\varphi(x) = \begin{cases} 0 & \text{for } x=0, \\ \sum_{n=1}^{\infty} (-1)^{n+1} f^n(x) = \frac{1}{2} + \sum_{n=0}^{\infty} (-1)^{n+1} (f^{-n}(x)-1) & \text{for } x\in(0,1), \\ 1/2 & \text{for } x=1. \end{cases} \tag{18}$$

Corollary. Let f be a function fulfilling conditions (i) and (iv). There exists a doubly stochastic measure μ supported on the hairpin H if and only if f fulfils (17). When it exists, such a measure is unique and is generated by relation (1), where φ is given by (18).

Remark 5. If the function f is convex, condition (iv) is certainly fulfilled (cf. [4,Theorem 7.3.5]; note that then also the function $x \mapsto f(x)-x$ is convex), but (iv) can also be fulfilled in other situations. Thus our Theorem 2 improves on Theorem 3.4 in [6]. Moreover, our proof of the equivalence of (17) to the existence of a monotonic solution $\varphi:I\to\mathbb{R}$ of (2) is simpler than that in [6].

Remark 6. It may well happen that condition (14) (resp.(17)) is not fulfilled, i.e. equation (3) (resp.(2)) has no monotonic solution $\varphi:I\to\mathbb{R}$. Such is the case, e.g., for the equation $\varphi(x^2)+\varphi(x) = x$ (cf. [7], and also [3]) as well as for the equation $\varphi(x^2)+\varphi(x) = x^2$ (cf.[5]).

REFERENCES

[1] J. Burek, Über einseitig beschränkte Lösungen linearer Funktionalgleichungen. Math. Nachr. 36 (1968), 67-72.

[2] M. Kuczma, On the functional equation $\phi(x) + \phi[f(x)] = F(x)$, Ann. Polon. Math. 6 (1959), 281-287.

[3] M. Kuczma, Functional Equations in a Single Variable, Monografie Mat. 46, Polish Scientific Publishers, Warszawa, 1968, 383 pp.

[4] M. Kuczma, An Introduction to the Theory of Functional Equations and Inequalities. Cauchy's Equation and Jensen's Inequality, Prace Naukowe Uniwersytetu Śląskiego w Katowicach 489. Polish Scientific Publishers, Warszawa-Kraków-Katowice, 1985, 523 pp.

[5] T.L. Seethoff, R.C. Shiflett, Doubly stochastic measures with prescribed support, Z. Wahrscheinichkeitstheorie verw. Gebiete 41 (1978), 283-288.

[6] M. Sherwood, M. D. Taylor, Doubly stochastic measures with hairpin support, to appear.

[7] H. Szmuszkowicz, O pewnym szeregu potęgowym lakunarnym, Roczniki P.T.M., Prace Mat. 3 (1959), 201-204.

Department of Mathematics
Academy of Mining and Metallurgy
30-059 Kraków, Poland

Department of Mathematics
Silesian University
40-007 Katowice, Poland

Received March 19, 1989

UN CRITERE DE NUCLEARITE POUR CERTAINS ESPACES DE TYPE(M).

A.O.BAHYA

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

Abstract: In this note , we give a positive answer, in the separable case, to a question raised by G.Isac in [2]. It concerns the nuclearity of locally convex M-spaces .

I.Introduction. Dans cette note , nous donnons une reponse positive, dans le cas séparable , à un problème posé par G.Isac dans [2]. Nous montrons qu'un espace localement convexe separé E, de type (M) ,séparable et topologiquement complet est nucléaire si, et seulement si, le cône de ses éléments positifs est nucléaire.Nous utilisons , pour cela,une nouvelle caractérisation des espaces localement convexes de type(L) qui est une extension d'un résultat dans [1] .

II. Préliminaires.Nous dirons qu'un lattice localement convexe (F,τ) est de type (L)(resp . de type (M)) si sa topologie τ peut être definie par une base$\mathcal{B}$ de semi-normes telleque, pour tout $p\in\mathcal{B}$on a :

(1) $\forall x,y \in E,\quad |x| \leq |y| \Rightarrow p(x) \leq p(y)$ et (2).$\forall x , y\geq 0, p(x+y)=p(x)+p(y)$ (resp.(1) et (2') : $\forall x,y\geq 0$, $p(x\vee y) = p(x) \vee p(y)$).

Une semi-norme qui verifie (1) (resp.(2), resp.(2')) sera dite solide (resp.additive , resp. une M-semi-norme).

Si K est un cône convexe (ie $K+K\subset K$ et $\lambda K\subset K$, quelque soit $\lambda \geq 0$), alors on note par K' l'ensemble $K'=\{f\in E' ; f(x)\geq 0 , \forall x \in K\}$.

Definition [2]. Un cône convexe K dans un espace localement convexe separé (E,τ) est dit nucléaire , s'il existe une base $\mathcal{B}$ de semi-normes definissant τ et telle que :

$$\forall p\in\mathcal{B} , \exists f_p\in K' : \forall x \in K , p(x) \leq f_p(x) .$$

III. Critère de nucléarité . Nous donnons tout d'abord la caracterisation suivante des espaces localement convexes de type (L).

Proposition III.1. Soit (E,τ) un lattice localement convexe separé dont le cône des éléments positifs est noté par K. Alors (E,τ) est de type (L) si, et seulement si :

(a) La fonction $x \longmapsto |x|$ est continue en zéro .

(b) Le cône K est nucléaire .

Preuve . On suppose que (E,τ) est un espace de type (L) . Alors τ peut être definie par une base $\mathcal{B}$ de semi-normes verifiant les proprietés (1) et (2). L'affirmation (a) resulte de (1) car, pour tout $p\in\mathcal{B}$ et tou $x \in E$ on a : $p(|x|)=p(x)$. En outre , d'aprés la proposition 6 de [3], K est nucléaire . Reciproquement si K est nucléaire , il existe une base $\mathcal{B}$ de semi-normes definissant τ telle que :

$$\forall p\in \mathcal{B} \ , \quad \exists\, \delta_p \in K' \ : \forall x \in K, \ \ p(x) \leq \delta_p(x) \ .$$

Donc, pour tout $x \in K$, $\delta_p(x) \geq 0$. On pose alors $p'(x)=\delta_p(|x|)$, quelque soit $x \in E$. Puisque , $|x+y|\leq|x| + |y|$ et $|\alpha x| = |\alpha|.|x|$, pour tous $x,y \in E$ et $\alpha\in\mathbb{R}$, p' est une semi-norme qui vérifie les propriétés (1) et (2) car δ_p est monotone croissante sur K. Il reste à prouver que la topologie définie par les semi-normes $(p')_{p\in\mathcal{B}}$ est équivalente à τ. Soit U un voisinage de zéro pour τ; il existe un voisinage V de zero pour τ, qui est équilibré et tel que : $V - V \subset U$.

Or il existe $p\in\mathcal{B}$ et $\varepsilon>0$ tels que $\varepsilon B_p \subset V$ (où $B_p=\{x \in E;\ p(x)\leq 1\}$ car $\mathcal{B}$ est une base de semi-normes definissant τ .

Soit $E'_{\delta_p} = \{x\in K \ ; \ \delta_p(x) \leq 1\}$. Alors $B'_{\delta_p} \subset B_p$ (car , $p(x) \leq \delta_p(x)$, quelque soit $x \in K$). D'où $\varepsilon B'_{\delta_p} \subset \varepsilon B_p \subset V$. Montrons que $\{x \in E \ ; \ p'(x) \leq \varepsilon\} \subset V$.

Soit $x\in E$ telque $p'(x) \leq \varepsilon$. Alors on a : $\delta_p(x^+) + \delta_p(x^-) \leq \varepsilon$.

Puisque δ_p est positive sur K on a : $\delta_p(x^+) = \lambda\varepsilon$ où $\lambda\in[0,1]$.

Si $\lambda = 0$ alors $\delta_p(\varepsilon^{-1}x^+) = \varepsilon^{-1}\delta_p(x^+) = 0 \leq 1$, d'où $\varepsilon^{-1}x^+ \in B'_{\delta p} \subset B_p$ et donc $x^+ \in V$. Si $\lambda \neq 0$ alors $\lambda^{-1}\varepsilon^{-1}x^+ \in B'_{\delta p}$ donc $x^+ \in \lambda V \subset V$ (car V est équilibré). Donc dans tous les cas $x^+ \in V$. On a de même $x^- \in V$. donc : $x = x^+ - x^- \in V-V \subset U$.

De la continuité de la fonction $x \longmapsto |x|$ et de la fonction δ_p, il resulte que, la boule $\{x \in E;\ p'(x) \leq \varepsilon\}$ est un voisinage de zéro pour τ, quelque soit p' et $\varepsilon > 0$.

Corollaire III.2. [1]. Soit $(E, \|\cdot\|)$ un lattice de Banach. Alors E est de type (L) si et seulement si :

(a) la fonction $x \longmapsto |x|$ est continue en zéro.

(b) le cône des éléments positifs de E est bien basé.

Preuve: D'après ([2], corollaire, p 162), un cône convexe, dans un espace de Banach est nucléaire si, et seulement si, il est bien basé.

Dans [2], G. Isac pose le problème suivant :

Problème : Si (E, τ) est un espace localement convexe et de type (M) dont le cône des éléments positifs est nucléaire, est-ce que l'espace E est nucléaire ?

En relation avec ce problème, nous obtenons le :

Théorème III.3. Soit (E,τ) un espace localement convexe separé, de type (M), topologiquement complet et séparable. Alors les assertions suivantes sont équivalentes :

(a) E est nucléaire.

(b) $K = \{x \in E\ ;\ x \geq 0\}$ est un cône nucléaire.

Preuve. (a) entraine (b) : Lorsque E est nucléaire alors, d'après ([4], theorème 3), τ peut être definie par une base de semi-normes solides et additive sur le cône K. Ainsi (E,τ) est de type (L). Donc K est nucléaire, d'après la proposition 6 de [3]. (b) entraine (a) : On a tout d'abord que l'application $x \longmapsto |x|$ est continue en zéro puisque

(E,τ) est de type (M) et donc τ peut être definie par une famille de semi-normes solides . En outre , puisque l'on suppose que K est nucléaire, (E,τ) est de type (L) d'après la proposition III.1. Ainsi τ peut être définie par une base de semi-normes qui sont solides et additives (car (E,τ) est de type (L)) et par une base de M-semi-normes solides (car (E,τ) est de type (M)). Donc d'après le théorème 3 de [4], (E,τ) est un espace nucléaire .

Remerciements. L'auteur remercie M. le Pr.G. Isac, du collège militaire royal S^{t}_{e} - Jean (Québec , Canada) ,pour l'avoir initié à la théorie des cônes et M. le Pr. M. Oudddess , de l'E.N.S (RABAT), pour de nombreuses et stimilantes discussions .

REFERENCES .

[1] G. ISAC . " Cônes localement bornés et cônes completement reguliers. Application à l'analyse non lineaire " . Seminaire d'analyse modérne. Univ. de Sherbrooke 17 (1980) , 1-168 .

[2] G.ISAC. "Un critère de sommabilité absolue dans les espaces localement convexes ordonnés. Cônes nucléaires" . Mathématica , Tome 25 (48) , N°2, 1983 ,pp . 159 -169.

[3] G.ISAC ."Supernormal cones and absolute summability". Libertas Mathematica, vol.5, 1985.p. 17-32.

[4] N.POPA. " Un critère de nucléarité pour les treillis".C.R. Acad . Sc. Paris, t. 269(1er septembre 1969).Serie A, 355-356.

[5] H.H. SCHAEFER ." Topological vector spaces" . Springer- Verlag (Graduate texts in Mathématics) Fith printing (1986).

Ecole Normale Supérieure Takaddoum
Avenue Oued Akreuch
RP:51 18 , Rabat (Maroc).

Received May 3, 1989

CONGRUENCE LATTICES, AUTOMORPHISM GROUPS OF FINITE LATTICES AND PLANARITY

G. GRÄTZER FRSC AND H. LAKSER

University of Manitoba

Abstract. It was proved by R. P. Dilworth (unpublished) that every finite distributive lattice D can be represented as the lattice of congruence relations of a finite lattice L. We strengthen Dilworth's Theorem by making L *very small and planar*. R. Frucht proved that every finite group G can be represented as the automorphism group of a finite lattice L. We combine the results of Dilworth and Frucht, proving the *independence* of the congruence lattice and the automorphism group of a finite lattice. The present authors proved in 1986 that every $\{0,1\}$-homomorphism of finite distributive lattices can be represented as the restriction-homomorphism of the congruence lattice of a finite lattice L to the congruence lattice of an ideal L' of L. We strengthen this result by constructing L and L' *planar and rigid*.

1. Background. Let L be a lattice. It was proved in N. Funayama and T. Nakayama [2] that the congruence lattice of L is distributive. For a finite lattice L, the converse of this result was proved by R. P. Dilworth: Every finite distributive lattice D can be represented as the lattice of congruence relations of a suitable finite lattice L. The first published proof of this result is in G. Grätzer and E. T. Schmidt [7]. For another proof of this result by the present authors, see [3, pp. 81–84].

Now consider the automorphism group of L. The characterization theorem of the automorphism group of a finite lattice is due to R. Frucht [1]: Every finite group G can be represented as the automorphism group of a suitable finite lattice L. In fact, Frucht's construction yields a simple lattice of length three.

Given a lattice L and a convex sublattice L', it is well known that the map

$$\operatorname{Con} L \to \operatorname{Con} L'$$

determined by restriction is a lattice homomorphism preserving 0 and 1. Based on the proof of Dilworth's representation theorem given in [3], it was shown by the present authors in [4] that, conversely, any $\{0,1\}$-preserving homomorphism of finite distributive lattices can be realized by restricting the congruence lattice of a finite lattice L to the congruence lattice of an ideal L' of L; for an alternate proof, see E. T. Schmidt [10].

2. Results. In this section, we summarize the related new results of the authors; see [5] and [6] for the proofs.

Firstly, the "improved" form of Dilworth's Theorem:

This research was supported by the NSERC of Canada.

THEOREM 1. *Let D be a finite distributive lattice with more than one element. Then there exists a finite planar lattice L with no proper automorphism such that the congruence lattice of L is isomorphic to D. The lattice L can be chosen to have $O(|J(D)|^3)$ elements, where $J(D)$ is the set of nonzero join-irreducible elements in D.*

Compare this with earlier proofs yielding lattices with $O(2^{|J(D)|})$ elements (or more) and order dimension $|J(D)|$ (or higher). We believe that the new construction provides the simplest known proof of Dilworth's result.

Secondly, we show that the congruence lattice and the automorphism group of a finite lattice are *independent*:

THEOREM 2. *Let D be a finite distributive lattice with more than one element, and let G be a finite group. Then there exists a finite lattice L such that the congruence lattice of L is isomorphic to D, and the automorphism group of L is isomorphic to G.*

The proof utilizes Frucht's result but does not use Dilworth's Theorem.

Combining Frucht's result with the result of G. Sabidussi [8], the automorphism group of a lattice is characterized as an arbitrary group. We obtain:

THEOREM 3. *Let D be a finite distributive lattice with more than one element, and let G be an arbitrary group. Then there exists a lattice L such that the congruence lattice of L is isomorphic to D, and the automorphism group of L is isomorphic to G.*

Thirdly, we apply the new lattice construction to prove the following theorem, which improves the result of [4] by showing that we can enforce *planarity*:

THEOREM 4. *Let D, D' be finite distributive lattices, and let $\psi : D \to D'$ be a $\{0,1\}$-preserving lattice homomorphism. Then there exist a finite planar lattice L, an ideal L' of L, and lattice isomorphisms*

$$\varrho : D \to \operatorname{Con} L, \qquad \varrho' : D' \to \operatorname{Con} L'$$

such that $\psi\varrho'$ is the composition of ϱ with the restriction of $\operatorname{Con} L$ to $\operatorname{Con} L'$. Moreover, the lattices L and L' have no nontrivial automorphisms.

By a *nontrivial* automorphism we mean one that is distinct from the identity mapping.

Finally, we combine Theorem 4 with automorphism groups. In general, automorphisms of a lattice do not restrict to automorphisms of its ideals. However, we can construct lattices where this does happen:

THEOREM 5. *Let D, D' be finite distributive lattices with more than one element, and let $\psi : D \to D'$ be a $\{0,1\}$-preserving lattice homomorphism. Let G, G' be groups, and let $\eta : G \to G'$ be a group homomorphism. Then there are a lattice L, an ideal L' in L, lattice isomorphisms*

$$\varrho : D \to \operatorname{Con} L, \qquad \varrho' : D' \to \operatorname{Con} L',$$

and group isomorphisms

$$\tau : G \to \operatorname{Aut} L, \qquad \tau' : G' \to \operatorname{Aut} L'$$

such that, for each $x \in D$, the congruence relation $x\psi\varrho'$ on L' is the restriction to L' of the congruence relation $x\varrho$ on L, and, for each $g \in G$, the automorphism $g\eta\tau'$ of L' is the restriction of the automorphism $g\tau$ of L.

If G and G' are finite, then the lattice L can be chosen to be finite.

Note that we do not claim that the lattice L in Theorem 4 can be chosen to be planar.

3. Method. To illustrate the constructions, we shall use the lattice A of Figure 1. Note that the diagram also shows $J(A)$ whose elements are labeled.

We shall describe the lattices L and L' of Theorem 4 in two special cases. Let us consider the distributive lattices $D = \mathfrak{C}_2$ (the two-element chain $\{0, e\}$ with $0 < e$) and $D' = A$. Let $\psi : D \to D'$ satisfy $\psi : e \mapsto 1$, $0 \mapsto 0$. The resulting lattice L is depicted in Figure 2. The generator of the ideal L' is drawn as $\bullet$. It is easy to see that in L' every prime interval is projective to one with a label; that prime intervals with the same label are projective: that the congruences generated by labeled prime intervals form a poset as illustrated in Figure 1. Hence, the congruence lattice of L' is isomorphic to $D' = A$. The lattice L is obviously simple.

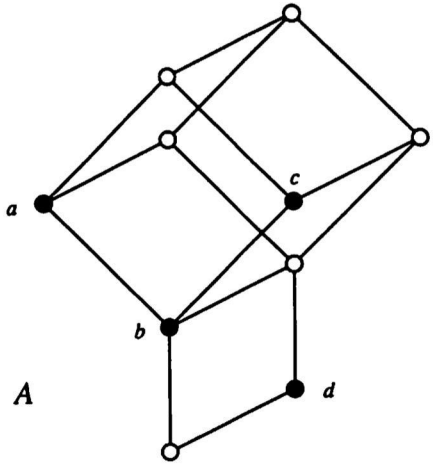
This method can be generalized to all cases in Theorem 4 except if $|D'| = 2$. To illustrate this case, we consider the lattices $D = A$ and $D' = \mathfrak{C}_2$. Let ψ be determined by setting $\psi : b \mapsto e$, $d \mapsto 0$. The lattice L we construct is depicted in Figure 3, where the generator of the ideal L' is drawn as $\bullet$. Again, it is easy to see that the congruence lattice of L is isomorphic to $D = A$, the lattice L' is simple, and the restriction-homomorphism is the same as ψ.

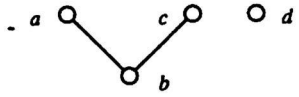
References

1. R. Frucht, *Lattices with a given group of automorphisms*, Canad. J. Math. **2** (1950), 417–419.
2. N. Funayama and T. Nakayama, *On the distributivity of a lattice of lattice-congruences*, Proc Imp. Acad. Tokyo **18** (1942), 553–554.
3. G. Grätzer, "General Lattice Theory," Academic Press, New York, N. Y.; Birkhäuser Verlag, Basel; Akademie Verlag, Berlin, 1978.
4. G. Grätzer and H. Lakser, *Homomorphisms of distributive lattices as restrictions of congruences*, Canad. J. Math. **38** (1986), 1122–1134.
5. _____, *On the automorphism group and the congruence lattice of a finite lattice*, Manuscript.
6. _____, *Homomorphisms of distributive lattices as restrictions of congruences. II. Restrictions of automorphisms*, Manuscript.
7. G. Grätzer and E. T. Schmidt, *On congruence lattices of lattices*, Acta Math. Acad. Sci. Hungar. **13** (1962), 179–185.
8. G. Sabidussi, *Graphs with given infinite groups*, Monatsch. Math. **68** (1960), 64–67.
9. E. T. Schmidt, *On the length of the congruence lattice of a lattice*, Algebra Universalis **5** (1975), 98–100.
10. _____, *Homomorphisms of distributive lattices as restrictions of congruences*, Acta Sci. Math. (Szeged) **51** (1987), 209–215.
11. S.-K. Teo, *Representing finite lattices as complete congruence lattices of complete lattices*, Abstracts of papers presented to the Amer. Math. Soc. 88T-06-207.

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba, Canada R2T 2N2

Received May 29, 1989





$J(A)$

Figure 1

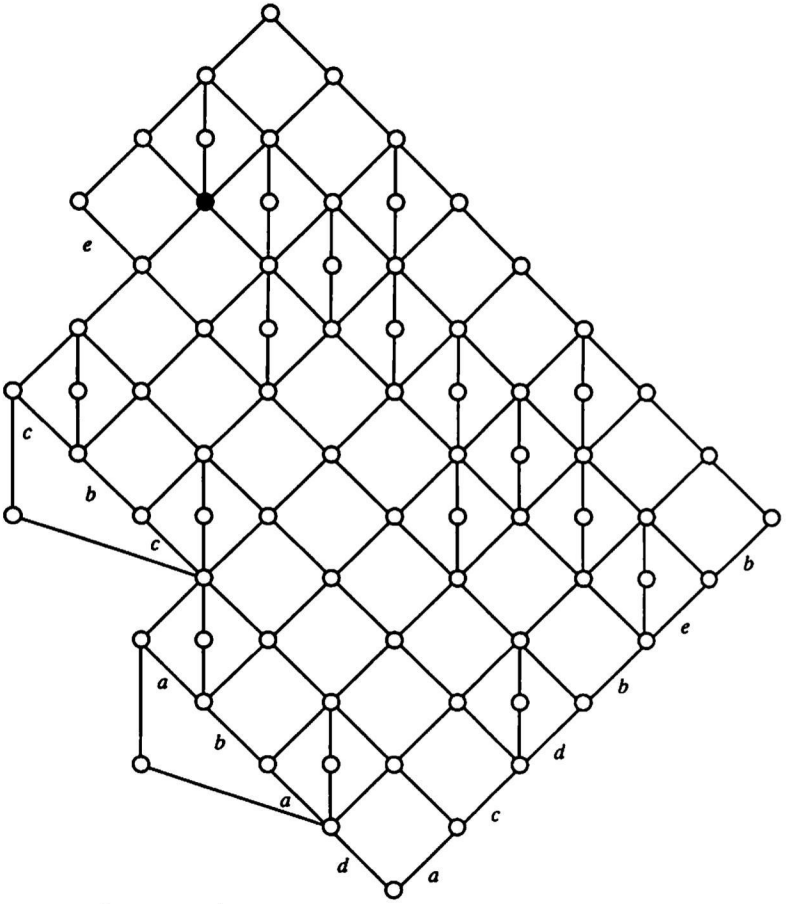


Figure 2

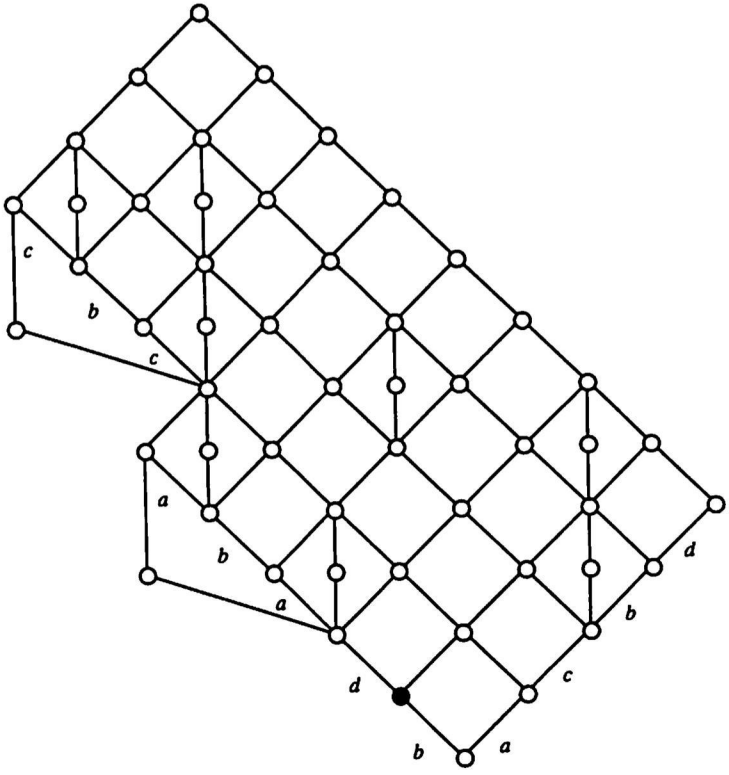


Figure 3

A general result on local spannedness

by

Harry D'Souza

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

In this article we give a simple proof to show that if X is a complex projective manifold with $dim\, X \geq 3$, and L an ample and spanned line bundle on X, and if (X', L') is a reduction of (X, L), then L' is locally spanned. L is such that the intersection of (n-2) generic members of |L| is a smooth elliptic surface of Kodaira dimension $\kappa(S) = 1$, and moreover $\kappa(A) \geq 0$, where $A \in |K_X + (n-2)L|$.

Introduction

In a crucial result in [D], it is shown that for a pair (X,L), where X is a smooth threefold, if L is very ample then for the reduction (X',L'), L' is locally very ample. The aim of this article is to generalize this result to smooth varieties of similar kind of *arbitrary dimension*, by weakening the very ample hypothesis on L, to ample and globally spanned, and prove that L' the associated line bundle of the reduction (X',L') is locally ample and spanned. This technical result allows for considerable simplification of the proofs of theorems involving biregular classification of these types of varieties. The counterexample in (1.5) shows that the hypothesis on A *cannot* be relaxed to simply $\kappa(S) \geq 0$.

Notation and background material

(0.1) Throughout this paper X is a complex projective manifold of dimension $n \geq 3$. L is an ample line bundle on X, such that the intersection of (n - 2) generic members of |L| is a smooth elliptic surface of Kodaira dimension $\kappa(S) = 1$. We also assume that $\kappa(A) \geq 0$, where $A \in |K_X + (n-2)L|$,

the linear system associated with $K_X \otimes L^{n-2}$.

(0.2) Let (X', L') be a reduction of (X, L), (see [D; (0.6)]).

(0.3) Let L be a line bundle over X. Let $A_1, \ldots, A_{n-2}$ be the general members of the linear system $|L|$ and let $X_i = \cap_{1 \leq j \leq n-i} A_j$, then $\dim(X_i) = i$. We will often denote X_2 by S, and we have the following descending chain $X \supset X_{n-1} \supset \ldots \supset X_3 \supset X_2 = S$.

(0.4) **Remark:** (i) Since S is smooth, by Bertini's theorem, X_i is smooth for all i.

(ii) As in (0.3), we have a similar descending chain $X' \supset X'_{n-1} \supset \ldots \supset X'_3 \supset X'_2 = S'$.

(iii) Since S' is a minimal model of S, $\kappa(S') = 1$.

Main results

(1.1) **Theorem:** *Let* (X, L) *and* (X', L') *be as in* (0.1) *and* (0.2), *then* L' *is ample on* X'.

Proof: Follows immediately from [Fu; 5.7]

□

(1.2) **Lemma:** *Let* (X, L) *be as in* (0.1) *and* X' *be as in* (0.2), *then there exists a morphism* $p_n : X' \to C$, *such that* $p_n^*(M) = K_{X'} \otimes L'^{(n-2)}$, *where* $\dim C = 1$, *and* M *is a line bundle on* C.

Proof: By [D; (0.11)] we know that there is a line bundle M over

a curve C, such that $K_{X'_3} \otimes L' = p_3^*(M)$. So, in [S], on going over the structure theorem following (2.1) in [S], for $\sigma(X,L) \leq 3$, and noting that $\sigma(X,L)=3$ if $\kappa(A) \geq 0$; we see that $K_{X'} \otimes L'^{(n-2)}$ is semi-ample and numerically effective. Hence by using adjunction repeatedly, and using [S; (2.1)], we see by Lefschetz theorem that $K_{X'} \otimes L'^{(n-2)} = p_n^*(M)$.

□

(1.3) **Theorem**: *Let* (X, L) *be as in* (1.0). *Assume moreover that* L *is spanned by global sections, then* L' *is locally spanned with respect to* p_n

Proof: We first show that $K_{X'} \otimes L'^2$ is spanned by global sections, and then we show that $K_{X'} \otimes L'^{(n-1)}$ is spanned by global sections by using induction on $i = \dim(X_i) \geq 3$.

Let $S' = X'_2$ (see 0.4). We first prove the following:

Claim: $L'_{S'}.L'_{S'} \geq 5$.

Proof (of claim): Suppose $L'_{S'}.L'_{S'} \leq 4$, then by Catelnuovo's inequality [Ha], and on noting that S' is an elliptic surface we see that $g(L'_{S'}) \leq 1$, but by [A-S; (0.2) *and see also* (1.1) end of proof there], these are Gorenstein del Pezzo surfaces. Since $\kappa(S') = 1$, this is impossible. This proves the claim.

Now since on X'_3, $L'.L'.L' = L'_{S'}.L'_{S'} \geq 5$, and since (X'_3, L') is not in the list of [A-S; 0.2], it follows by [A-S; Thrm. A] that $K_{X'} \otimes L'^2$ is spanned by global sections.

Consider the following short exact sequence:

$$0 \to K_{X'_i} \otimes L'^{(i-2)} \to K_{X'_i} \otimes L'^{(i-1)} \to K_{X'_{i-1}} \otimes L'^{(i-2)} \to 0$$

Using the sequence for $i = 4$, and the Kodaira vanishing theorem on the associated long exact sequence, it follows that $K_{X'_4} \otimes L'^3$ is spanned by global sections. So, using the same exact sequence for for $i = n$, and by the induction assumption for $i = n-1$, it follows that $K_{X'} \otimes L'^{(n-1)}$ is spanned by global sections. By lemma (1.2), therefore $p_n^*(M) \otimes L'$ is spanned. Since $p_n^*(M)$ is locally trivial, L' must be locally spanned.

□

(1.4) **Theorem**: *Let* (X, L) *be as in* (1.0). *Assume moreover that* L *is very ample, then* L' *is locally very ample.*

Proof: By the main theorem in [S-VdV] we know that $K_{X'} \otimes L'^{(n-1)}$ is very ample. By Lemma (1.2) $K_{X'} \otimes L'^{(n-2)} \cong p_n^*(M)$. Hence $p_n^*(M) \otimes L'$ is very ample or L' is locally very ample.

□

The following example shows that on weakening the condition $\kappa(A) \geq 0$, in (0.1), to the condition $\kappa(S) \geq 0$, lemma (1.2) is false.

(1.5) **Example**: Let S be a smooth elliptic surface of non-negative Kodaira dimension such that any morphism of S onto a curve factors through the projection $p: S \to C$, defining the elliptic surface (this is the

case for minimal models of all but very special class of elliptic surfaces). Let H be a very ample line bundle on S, and let $V = H \oplus H \oplus H$. Let L denote the tautological bundle of the fourfold $X = P(V)$. Then L is very ample, and if $A_i \in |L|$, then $A_1 \cap A_2$ is a smooth elliptic surface of non-negative Kodaira dimension. In fact S is birational to $A_1 \cap A_2$, and so $\kappa(S) = \kappa(A_1 \cap A_2)$. Now we can easily see that the only reduction of (X,L) is (X,L). Furthermore, any morphism from X to a curve must factor through the composition of X to S and S to C, since the fibres of $X \to S$ are P^2, that must go to points under a map to a curve. Now let us consider $K_X \otimes L^{(4-2)}$ restricted the fibre P^2 of $X \to S$. By adjunction, and on noting that $L_{P^2} = \vartheta_{P^2}(1)$, we see that $(K_X \otimes L^{4-2})_{P^2} = \vartheta_{P^2}(-1)$. Hence it *cannot* be a pullback from the base curve C.

Acknowledgement: The author would like to thank A. Sommese for many useful discussions.

REFERENCES

[A-S] M. Andreatta and A. J. Sommese: On the adjunction mapping for singular projective varieties (preprint).

[D] H. D'Souza; Threefolds whose hyperplane sections are elliptic surfaces: Pacific Journal of Mathematics, 134 (1) 57 - 78.

[Fu] T. Fujita; On the Lefschetz hyperplane section principle. J. Math. Soc. Japan, 32 (1) 1980.

[Ha] R. Hartshorne; Algebraic Geometry, Springer Verlag, 1977, GTM # 52.

[S] A. Sommese; On the Adjunction Theoretic Structure of Projective Varieties, Proc. of the Complex Analysis and Algebraic Geometry Conference (ed. H. Grauert), Gottingen, 1985, Springer Lecture Notes, **1195** (1986), 175-213.

[S-VdV] A. Sommese and Van de Ven; On the adjunction mapping, Math. Ann. Vol. in Honor of F. Hirzebruch (1987).

Harry D'Souza
Department of Mathematics
University of Michigan, Flint
Flint, MI 48502-2186

Received June 6, 1989

Mailing Addresses

1.	A.O. Bahya	Ecole Normale Supérieure Takaddoum Avenue Oued Akreuch BP: 51 18, Rabat (Maroc)
2.	B. Choczewski	Department of Mathematics Academy of Mining and Metallurgy 30-059 Kraków, Poland
3.	H. D'Souza	Department of Mathematics Univeristy of Michigan at Flint Flint, MI 48502-2186, U.S.A.
4.	G. Grätzer	Department of Mathematics University of Manitoba Winnipeg, Manitoba R3T 2N2
5.	M. Kuczma	Department of Mathematics Silesian University 40-007 Katowice, Poland
6.	H. Lakser	Department of Mathematics University of Manitoba Winnipeg, Manitoba R3T 2N2
7.	H. Osada	Department of Mathematics Rikkyo University Nishi-Ikebukuro, Tokyo 171, Japan
8.	K. Ota	Department of Mathematics Tsuda College Kodaira, Tokyo 187, Japan
9.	N. Terai	Department of Mathematics School of Science and Engineering Waseda University, Okubo Shinjuku, Tokyo 160, Japan