Ergod. Th. & Dynam. Sys. (1986), **6**, 449–473
Printed in Great Britain

Periodic points and invariant pseudomeasures for toral endomorphisms

WILLIAM A. VEECH
Department of Mathematics, Rice University, Houston, Texas 77251, *USA*

(*Received* 5 *October* 1984 *and revised* 5 *July* 1985)

Abstract. Extending a result of Livsic [**10**] it is proved that the coboundary equation $f(Tx)-f(x)=g(x)$ admits a C^∞ solution f for C^∞ g when T is an ergodic toral endomorphism and g sums to zero over every periodic orbit. The same statement is false with C^1 in place of C^∞, in contrast to the Livsic (hyperbolic) theorem. In one dimension the 'Lip α' case leads to questions relating to the generalized Riemann hypothesis.

1. *Introduction*

We begin by fixing some notation. If $N \geq 1$, $\mathbb{T}^N$ denotes the N-dimensional torus group, $\mathbb{T}^N = \mathbb{R}^n/\mathbb{Z}^N$. Setting $e(t) = \exp(2\pi i t)$, Fourier series on $\mathbb{T}^N$ are written $f \sim \sum_{n\in\mathbb{Z}^N} \hat{f}(n)e(n\cdot x)$, and $\mathbb{A} = \mathbb{A}(\mathbb{T}^N)$ is the space of absolutely convergent Fourier series with l^1-norm, $\|f\| = \sum_{n\in\mathbb{Z}^N} |\hat{f}(n)|$. $PM = PM(\mathbb{T}^N)$ is the dual space to $\mathbb{A}$, the space of *pseudomeasures* on $\mathbb{T}^N$, with the l^∞-norm $\|\mu\| = \sup_{n\in\mathbb{Z}^N} |\hat{\mu}(n)|$, where $\hat{\mu}(n) = \mu(e(n\cdot x))$.

Let there be given a continuous, non-singular endomorphism, T, of $\mathbb{T}^N$. T induces an isometry, $f \to f\circ T$, of $\mathbb{A}$ and a dual contractive mapping $\mu \to T\mu$ of PM. It makes sense therefore to speak of the space, $IPM(T)$, of *T-invariant pseudomeasures on* $\mathbb{T}^N$. $IPM(T)$ contains properly the space, $IM(T)$, of finite (complex-valued) T-invariant measures on $\mathbb{T}^N$.

Let $P(T)$ be the set of periodic points of the endomorphism T. If T is ergodic, $P(T)$ is a countable subgroup of $\mathbb{T}^N$, a union of finite subgroups. Associate to each $x \in P(T)$ the counting measure, σ_x, on the orbit of x, and denote by $\langle P(T)\rangle$ the $\mathbb{C}$-linear span of $\{\sigma_x | x \in P(T)\}$. The central result of the present work is

(1.1) THEOREM. *Let T be an ergodic endomorphism of $\mathbb{T}^N$. Then $\langle P(T)\rangle$ is weak-$*$ dense in $IPM(T)$.*

If T is an ergodic endomorphism of $\mathbb{T}^N$, it is known that $\langle P(T)\rangle$ is weak-$*$ dense in $IM(T)$ ([**11**]). Therefore, theorem 1.1 would be a consequence of a theorem on the density of $IM(T)$ in $IPM(T)$ and the theorem of Marcus. However, we are unable to take advantage of this implication, and our analysis leads directly to theorem 1.1. At present we know of no direct implication, in either direction, between Marcus' theorem and theorem 1.1. In this regard see the discussion in § 5.

The theorem to follow is a version for 'quasihyperbolic endomorphisms' ([**8**]) of a theorem of Livsic ([**9**], [**10**]).

(1.2) THEOREM. *Let T be an ergodic endomorphism of $\mathbb{T}^N$, and let $\alpha \geq 0$, $\beta > N$ be given. If $f \in C^{\alpha+\beta}(\mathbb{T}^N)$ satisfies $\sigma_x(f) = 0$ for all $x \in P(T)$, there exists $g \in C^{\alpha}(\mathbb{T}^N)$ such that*

$$g(Tx) - g(x) = f(x) \tag{1.3}$$

holds identically.

It is easy to see that if $f \in \mathbb{A}$, and if (1.3) admits an integrable solution g, then $\sigma_x(f) = 0$, $x \in P(T)$ ([**9**]). An immediate corollary to theorem 1.2 is

(1.4) COROLLARY. *Let $f \in C^{\infty}(\mathbb{T}^N)$. If T is an ergodic endomorphism of $\mathbb{T}^N$ such that $\sigma_x(f) = 0$ for all $x \in P(T)$, then (1.3) admits a solution $g \in C^{\infty}(\mathbb{T}^N)$.*

It is possible that the solution (1.3) enjoys more smoothness than is asserted by theorem 1.2. However, in the quasihyperbolic seting the Livsic theory does not go through without change. We have:

(1.5) PROPOSITION. *Let T be an ergodic endomorphism of $\mathbb{T}^N$, and suppose T is not hyperbolic. There exists $f \in C^1(\mathbb{T}^N)$ such that $\sigma_x(f) = 0$ for all $x \in P(T)$, but (1.3) admits no solution g of class C^1.*

If T is an endomorphism of $\mathbb{T}^N$, the dual endomorphism $A: \mathbb{Z}^N \to \mathbb{Z}^N$ may be identified with an $N \times N$ integral matrix, A. If T is non-singular and ergodic, then A is non-singular and has no root of unity among its eigenvalues. The theorem to follow may be of interest in its own right. It plays a critical role in the proof of theorem 1.1.

(1.6) THEOREM. *Let A be an $N \times N$ non-singular integer matrix, and suppose A has no root of unity among its eigenvalues. Let S be a set of rational primes having upper Dirichlet density 1 in the set of all rational primes. If $u, v \in \mathbb{Z}^N$, and if the congruence $A^l u \equiv v \pmod{p}$ admits a solution l for each finite set of $p \in S$, then there exists l_0 such that $A^{l_0} u = v$. Moreover, if l_0 is as above, and if $\{l_k\}$ is any sequence of integers such that*

$$\lim_{k \to \infty} A^{l_k} u \equiv v \pmod{p}$$

holds for all $p \in S$, then also

$$\lim_{k \to \infty} l_k \equiv l_0 \pmod{n}$$

for every integer $n > 0$.

The conclusion of the theorem is false for the unipotent matrix

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

if $u = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, and S is the set of odd primes. However, it is true for an

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

arbitrary non-singular integer matrix A that for all $u \in \mathbb{Z}^N$ the set $\mathbb{Z}^N \cap \{A^k u | k \in \mathbb{Z}\}$ is closed in the profinite topology of $\mathbb{Z}^N$ (theorem 3.14).

Theorem 1.6 is an easy consequence of a theorem of Chevalley [3]. The latter contains the statement that if R is a subring, of a specified sort, of an algebraic number field, and if U is the group of units of R, then the profinite (group) topology on U is the restriction to U of the profinite (ring) topology on R. A proof of Chevalley's theorem is included for the reader's convenience (we in fact learned of Chevalley's paper only after the present paper was typed).

§ 7 is devoted to the study of invariant distributions for endomorphisms of $\mathbb{T}^1$. Denote by Λ_α, $0 < \alpha < 1$, the space of Hölder functions on $\mathbb{R}$ of exponent α and period 1 ($\Lambda_\alpha = C^\alpha$).

(1.7) THEOREM. *Let p be a prime number. If $\alpha > \frac{1}{2}$, if $f \in \Lambda_\alpha$ is even, and if f satisfies*

$$\sum_{j=0}^{n-1} f\left(\frac{j}{n}\right) = 0 \qquad (n \geq 1, (n, p) = 1) \tag{1.8}$$

then there exists $g \in \Lambda_\alpha$ such that

$$g(px) - g(x) = f(x). \tag{1.9}$$

As any odd function satisfies (1.8), the assumption that f be even is necessary. If $p = 6$, the function $f(x) = \cos 2\pi 2\theta + \cos 2\pi 3\theta - 2\cos 2\pi 6\theta$ satisfies (1.8) but does not have the form (1.9) for any integrable function g.

As regards the assumption on α, if $\mu(\cdot)$ is the Möbius function, the even function

$$f(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \cos 2\pi nx \tag{1.10}$$

will be seen to be continuous and to satisfy (1.8) for all $n \geq 1$. Again (1.9) never admits an integrable solution.

It is possible the function defined by (1.10) enjoys more smoothness. While it cannot belong to Λ_α for $\alpha \geq \frac{1}{2}$ ($\alpha = \frac{1}{2}$ requires a special argument; $\alpha > \frac{1}{2}$ follows from $f \notin \mathbb{A}$), it is possible $f \in \Lambda_\alpha$ for some or all $\alpha < \frac{1}{2}$. Settling this question would be of interest because of

(1.11) PROPOSITION. *If f is defined by* (1.10), *and if $f \in \bigcap_{\alpha < \frac{1}{2}} \Lambda_\alpha$, then the (Generalized) Riemann Hypothesis is true for the cyclotomic fields.*

We do not know at present whether the converse to proposition 1.11 is also true. In this regard we mention that if $0 < \alpha < \frac{1}{2}$, if ψ_α is the αth 'Riesz potential' on $\mathbb{T}^1 \cong \mathbb{R}/\mathbb{Z}$, and if the series

$$\Psi_\alpha(x) = \sum_{\nu=1}^{\infty} \frac{\mu(\nu)}{\nu^\alpha} \psi_\alpha(\nu x) \tag{1.12}$$

converges in the $L^1(\mathbb{T}^1)$ sense, then $f \notin \Lambda_\beta$, $\beta > \alpha$, where f is defined by (1.10). In § 7 we will prove (1.12) converges in L^2 for $\alpha > \frac{1}{2}$ (for the purposes of the proof of theorem 1.7). However, the case of L^1 convergence for $0 < \alpha < \frac{1}{2}$ remains an intriguing mystery. The 'sum' of (1.12) is simply

$$\sum_{\nu=1}^{\infty} \frac{\mu(\nu)}{\nu^\alpha} \psi_\alpha(\nu x) = \frac{2}{(2\pi)^\alpha} \cos 2\pi \left(\frac{\alpha}{4} + x\right) \tag{1.13}$$

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

and (1.13) does hold in the distributional sense (at least in the dual of Λ_β for any $\beta > \text{Max}\,(0, \frac{1}{2}-\alpha)$).

The author is grateful to H. L. Montgomery for useful discussions in connection with this work and particularly for the reference to the work of Davenport [**4**], [**5**]. The latter is used to establish the continuity of the function (1.10). The identity (1.13) for $\alpha = 1$ (when $\psi_1(x) = -(x - [x] - \frac{1}{2})$) reduces to an identity established by Davenport. Davenport proved that the series (1.13) converges uniformly when $\alpha = 1$; in § 7 we will see it converges a.e. for $\frac{2}{3} < \alpha < 1$.

This research was supported by NSF-MCS-8219148

2. *Number fields*

In this section we apply some standard facts of algebraic number theory, especially the Dirichlet unit and Tchebotarev density theorems, to prove the Chevalley theorem mentioned in the introduction. References [**2**] and [**14**] are more than adequate.

Let K be a fixed finite extension field of $\mathbb{Q}$, and denote by $\mathcal{M}_0 = \mathcal{M}_0(K)$ the set of non-trivial non-archimedean prime divisors of K. Each $P \in \mathcal{M}_0$ has the form $P = \{\phi^t | t > 0\}$ for some non-trivial discrete valuation, ϕ, of K. $\mathcal{S}$ will denote a fixed confinite subset of $\mathcal{M}_0$, and $\mathcal{O}(\mathcal{S})$ is the corresponding intersection of valuation rings,

$$\mathcal{O}(\mathcal{S}) = \bigcap_{P \in \mathcal{S}} \{\alpha \in K | \phi(\alpha) \leq 1, \phi \in P\}$$

$\mathcal{O}^*(\mathcal{S})$ is the group of units in $\mathcal{O}(\mathcal{S})$.

With notations as above the *Dirichlet unit theorem* implies there exist m, $s \geq 0$ and $\omega_0, \zeta_1, \ldots, \zeta_s \in \mathcal{O}^*(\mathcal{S})$ such that $\omega_0^m = 1$ and if we set $\zeta^a = \zeta_1^{a_1}\zeta_2^{a_2}\ldots\zeta_s^{a_s}$, $a \in \mathbb{Z}^s$, then the map

$$\psi(i, a) = \omega_0^i \zeta^a \qquad ((i, a) \in \mathbb{Z}_m \times \mathbb{Z}^s) \tag{2.1}$$

defines an isomorphism from $\mathbb{Z}_m \times \mathbb{Z}^s$ onto $\mathcal{O}^*(\mathcal{S})$.

The multiplicativity of valuations implies that if $\lambda \in \mathcal{O}^*(\mathcal{S})$, and if a polynomial $x^n - \lambda$ admits a root in K, then that root also lies in $\mathcal{O}^*(\mathcal{S})$. The lemma to follow is thus immediate from the Dirichlet unit theorem:

(2.2) LEMMA. *Let notations and assumptions be as above, and suppose $n > 0$ and $\lambda \in \mathcal{O}^*(\mathcal{S})$ are such that the polynomial $x^n - \lambda$ admits a root in K. If $\psi^{-1}\lambda = (j, a)$ in* (2.1), *then*:

(i) $a \equiv 0 \pmod{n}$; *and*

(ii) *the congruence $ni = j \pmod{m}$ admits a solution i.*

If $r > 0$ is an integer, K_r will denote a minimal splitting field for $x^r - 1$ over K (possibly $K_r = K$).

(2.3) LEMMA. *Let notation and assumptions be as above, and let $r > 0$. If $\lambda \in \mathcal{O}^*(\mathcal{S})$, and if the polynomial $Q(x) = x^r - \lambda$ has for each $P \in \mathcal{S}$ a root modulo the prime ideal at P, then $Q(x)$ splits completely in K_r.*

Proof. Let $\mathcal{S}_r \subseteq \mathcal{M}_0(K_r)$ be the set of extension to K_r of the elements of $\mathcal{S}$. $\mathcal{S}_r$ is cofinite in $\mathcal{M}_0(K_r)$, and for each $P^* \in \mathcal{S}_r$ $Q(x)$ splits completely modulo the prime ideal at P^* (i.e. in $\mathcal{O}(\mathcal{S}_r)$). This is because $Q(x)$ admits one root (modulo $P^* \cap \mathcal{O}(\mathcal{S})$)

and K_r contains the rth roots of unity. Now the Tchebotarev density theorem implies $Q(x)$ splits in K_r ([2, Exercise 6, pp. 361-362]).

(2.4) LEMMA. *Assumptions are as in lemma* 2.3 *with* $r = q^k$ *for some* $k > 0$ *and odd prime* q. *Then* $Q(x)$ *admits a root in* K.

Proof. The Galois group, G, of K_r over K is cyclic by the assumption on the form of r. Let σ be a generator. If $z \in K_r \cap K^c$, then $\sigma z \neq z$. By lemma 2.3 $Q(x)$ splits in K_r, and we denote the roots of $Q(x)$ by $\alpha_1, \ldots, \alpha_r$. Unless one of these roots lies in K, it is true that $\sigma\alpha_i \neq \alpha_i$, $1 \leq i \leq r$. In the latter event it is also true for all but a finite set of $P^* \in \mathcal{S}_r$ that $\sigma\alpha_i \neq \alpha_i$ modulo the prime ideal, $\pi(P^*)$, at P^* (in $\mathcal{O}(\mathcal{S}_r)$), $1 \leq i \leq r$. By the Tchebotarev density theorem there is an infinite set of $P^* \in \mathcal{S}_r$ such that $\sigma = ((K_r/K)/\pi(P^*))$, the Frobenius symbol. For such P^* if $P = P^*|_K$, then $Q(x)$ admits no root modulo $\pi(P)$ (in $\mathcal{O}(\mathcal{S})$). This is a contradiction, and the lemma obtains.

(2.5) LEMMA. *Assumptions are as in lemma* 2.3 *with* $r = 2^k$, $k > 0$. *Then* $Q(x)$ *admits a root in* $K_4 = K(\sqrt{-1})$.

Proof. Since $K_2 = K$, we may suppose by lemma 2.3 that $k \geq 2$. Now K_{2^k} has a cyclic Galois group over K_4, and the argument of the previous lemma applies.

(2.6) LEMMA. *Let notation and assumptions be as above, especially as in* (2.1). *If* $a^{(l)}$ *is a sequence in* $\mathbb{Z}^s$ *such that*

$$\lim_{l\to\infty} \zeta^{a^{(l)}} \equiv 1 \pmod{\pi(P)} \qquad (P \in \mathcal{S}) \tag{2.7}$$

then it is also true that

$$\lim_{l\to\infty} a^{(l)} \equiv 0 \pmod{r} \qquad (0 < r \in \mathbb{Z}). \tag{2.8}$$

Proof. It is sufficient to establish (2.8) when $r = q^k$, $k \geq 0$ and q prime. The case $k = 0$ being trivial, assume $k > 0$ and (2.8) holds for all $r = q^l$, $l < k$ and q prime.

Case 1. q *odd.* Discarding a finite number of $a^{(l)}$, if necessary, we may suppose $a^{(l)} = q^{k-1}\alpha^{(l)} + q^k\beta^{(l)}$ with $\alpha^{(l)}, \beta^{(l)} \in \mathbb{Z}^s$ and $0 \leq \alpha_j^{(l)} < q$, $1 \leq j \leq s$. We must prove $\alpha^{(l)} = 0$, or, what is the same, that $\alpha^{(l)} \equiv 0 \pmod{q}$ for large l. To this end we may pass to a subsequence, if necessary, and suppose $\alpha^{(l)} = \alpha$ is independent of l. If we prove $\alpha = 0$, we will be finished.

If $\alpha \neq 0$ above, then $\alpha \not\equiv 0 \pmod{q}$, and by lemma 2.2 the polynomial $Q(x) = x^{q^k} - \zeta^{q^{k-1}\alpha}$ admits no root in K. On the other hand if $\zeta^{a^{(l)}} = 1 \pmod{\pi(P)}$ for some P, l then also $\zeta^{q^{k-1}\alpha} \equiv \zeta^{-q^k\beta^{(l)}} \pmod{\pi(P)}$, and so $Q(x)$ admits a root modulo $\pi(P)$. This contradicts the assumption (2.7) and lemma 2.4, and so $\alpha = 0$, as claimed.

Case 2. $q = 2$. Proceed as in case 1 except for selecting $\alpha^{(l)} \bmod 4$, i.e. $0 \leq \alpha_j^{(l)} < 4$, $1 \leq j \leq s$, and writing $a^{(l)} = 2^{k-1}\alpha^{(l)} + 2^{k+1}\beta^{(l)}$, $\alpha^{(l)}, \beta^{(l)} \in \mathbb{Z}^s$. Again we suppose $\alpha^{(l)} = \alpha$, and we are to prove $\alpha \equiv 0 \pmod{2}$. If $\alpha \not\equiv 0 \pmod{2}$, then $Q(x) = x^{2^{k+1}} - \zeta^{2^{k-1}\alpha}$ admits no root in $K(\sqrt{-1})$. Indeed, if $Q_0(x)$ is a quadratic factor of $Q(x)$ in $K[x]$, $Q(x)$ has constant term of the form $\omega\zeta^{\alpha/2}$ with ω a root of unity. It follows readily that $\zeta^{\alpha/2} \in K$, whence $\alpha \equiv 0 \pmod{2}$ by lemma 2.2. Now the argument from case 1 applies (with lemma 2.5) to show $x^{2^{k+1}} - \zeta^{2^{k-1}\alpha}$ in fact does admit a root in $K(\sqrt{-1})$. This is a contradiction unless $\alpha \equiv 0 \pmod{2}$, and the lemma obtains.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

By the *profinite topology* on a group (resp. ring) is understood the least topology with respect to which each homomorphism to a finite group (resp. finite ring) with the discrete topology is continuous.

(2.9) THEOREM (Chevalley [3]). *Let K be an algebraic number field, and let $\mathcal{S}$ be a cofinite subset of $\mathcal{M}_0(K)$. If U is a profinite neighbourhood of 1 in the group $\mathcal{O}^*(\mathcal{S})$, there exist $\tau > 0$ and $P_1, \ldots, P_\tau \in \mathcal{S}$ such that U contains $\bigcap_{j=1}^{\tau} \{\lambda \in \mathcal{O}^*(\mathcal{S}) | \lambda \equiv 1 \pmod{\pi(P_j)}\}$. In particular, the profinite topology on the group $\mathcal{O}^*(\mathcal{S})$ is the trace on $\mathcal{O}^*(\mathcal{S})$ of the profinite topology on the ring $\mathcal{O}(\mathcal{S})$.*

Proof. Let notation be as in (2.1), and suppose $\{(j_l, a^{(l)})\} \subseteq \mathbb{Z}_m \times \mathbb{Z}^s$ is a sequence such that

$$\lim_{l\to\infty} \psi(j_l, a^{(l)}) \equiv 1 \pmod{\pi(P)} \qquad (P \in \mathcal{S}) \tag{2.10}$$

Now (2.10) implies also that (2.7) holds, with $a^{(l)}$ there replaced by $ma^{(l)}$. But then (2.8) applied to $ma^{(l)}$ implies (2.7) for $a^{(l)}$. Thus, it is also true that

$$\lim_{l\to\infty} \omega_0^{j_l} \equiv 1 \pmod{\pi(P)} \qquad (P \in \mathcal{S})$$

holds, which readily implies $m | j_l$ for large l. The theorem is proved.

(2.11) COROLLARY. *Let K be an algebraic number field, let $\lambda, \alpha, \beta \in K$ be non-zero, and let $\mathcal{S} \subseteq \mathcal{M}_0(K)$ be a cofinite set of prime divisors with respect to which $\lambda, \alpha, \beta \in \mathcal{O}^*(\mathcal{S})$. If the congruence*

$$\lambda^l \alpha \equiv \beta \pmod{\pi(P)} \tag{2.12}$$

admits a solution l for each finite set of $P \in \mathcal{S}$, then there exists l_0 such that

$$\lambda^{l_0} \alpha = \beta. \tag{2.13}$$

If in addition λ is not a root of unity, and if $\{l_k\}$ is a sequence in $\mathbb{Z}$ such that

$$\lim_{k\to\infty} \lambda^{l_k} \alpha \equiv \beta \pmod{\pi(P)} \qquad (P \in \mathcal{S})$$

then also

$$\lim_{k\to\infty} l_k \equiv l_0 \pmod{r} \qquad (0 < r \in \mathbb{Z}). \tag{2.14}$$

Proof. The trace on $\{\lambda^l | l \in \mathbb{Z}\}$ of the profinite topology on $\mathcal{O}^*(\mathcal{S}) \cong \mathbb{Z}_m \times \mathbb{Z}^s$ is the discrete topology if λ is a root of unity and the profinite topology on $\mathbb{Z}$ if λ is not a root of unity. In either case $\{\lambda^l | l \in \mathbb{Z}\}$ is also closed in the profinite topology, as is $\{\alpha\lambda^l | l \in \mathbb{Z}\}$. Now (2.13) and (2.14) follow.

Example. Let $\mathcal{S} = \mathcal{M}_0(K)$, $\mathcal{O} = \mathcal{O}(\mathcal{S})$ the full ring of integers in K. If $\lambda, \alpha, \beta \in \mathcal{O}$, are non-zero and if (2.12) admits a solution for each finite set of $P \in \mathcal{M}_0$, then (2.13) holds for some l_0. To see this enlarge the exceptional set of P so that $\lambda, \alpha, \beta \in \mathcal{O}^*(\mathcal{S})$, and apply the theorem.

In the case where $K = \mathbb{Q}$, $\lambda, \alpha, \beta \in \mathbb{Z}$ with $|\lambda| > 1$, if $\lambda^l \alpha = \beta \pmod{p}$ admits a solution for each finite set of primes p, then for some $l_0 \in \mathbb{Z}$, $\lambda^{l_0} \alpha = \beta$.

In the general case of $(\mathcal{S}, K)$ above, the set $\{\mathbb{Z} \cap \pi(P)\}$ determines a set of prime ideals in $\mathbb{Z}$. In order to apply the Tchebotarev density theorem as we have, it is only

necessary to suppose there is a set Σ of rational primes of upper Dirichlet density 1 in the set of all primes and that $\mathcal{S}$ contains all extensions to K of the p-adic valuation on $\mathbb{Z}$, $p \in \Sigma$. We omit the routine details.

3. *Orbits of integral matrices in the profinite topology*

In this section we prove theorem 1.6. Let A be an $N \times N$ integral matrix. We do not require that A be non-singular. If $u \in \mathbb{Z}^N$, define $\Lambda(u)$ to be the smallest subgroup of $\mathbb{Z}^N$ which contain the semiorbit $\{u, Au, A^2u, \ldots\}$. Let $\Omega(u)$ be the $\mathbb{Q}$-linear span of $\Lambda(u)$, and then define $\Lambda^*(u) = \Omega(u) \cap \mathbb{Z}^N$.

In this section we consider for given A as above the congruence

$$A^l u \equiv v \pmod{Q} \tag{3.1}$$

in which $u, v \in \mathbb{Z}^N$ and $0 < Q \in \mathbb{Z}$ are given and l is the unknown.

(3.2) PROPOSITION. *Let A and $u, v \in \mathbb{Z}^N$ be as above. If there is an infinite set of $Q > 0$ such that* (3.1) *admits a solution l, then $v \in \Lambda^*(u)$. If* (3.1) *admits a solution for <u>all</u> integers $Q > 0$, then $v \in \Lambda(u)$.*

Proof. By the basis theorem for abelian groups every subgroup of $\mathbb{Z}^N$ is closed in the profinite topology, and so in particular $\Lambda(u)$ is closed, implying the second assertion. As for the first assertion, the group $\mathbb{Z}^N/\Lambda^*(u)$ is torsion free by construction, and the image of v in $\mathbb{Z}^N/\Lambda^*(u)$ is divisible by each integer Q for which (3.1) admits a solution l. By the basis theorem for abelian groups v projects to 0, meaning $v \in \Lambda^*(u)$, as claimed.

Remark. If

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad u = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

then

$$\Lambda(u) = \left\{ \begin{pmatrix} 2a \\ b \end{pmatrix} \middle| \, a, b \in \mathbb{Z} \right\},$$

$\Lambda^*(u) = \mathbb{Z}^2$. If $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, then (3.1) admits a solution for every odd integer Q.

Remark. The subspaces $\Omega(A^k u) = A^k \Omega(u)$ stabilize for $k \geq N$, and therefore $\Lambda^*(A^k u) = \Lambda^*(A^{k+1} u)$, $k \geq N$. If there is an infinite set of Q such that (3.1) admits a solution $l \leq N$, then obviously $A^{l_0} u = v$ for some $l_0 \leq N$. Otherwise, in studying (3.1) we may replace u by $A^N u$ and so suppose $\Lambda^*(Au) = \Lambda^*(u)$. Thus, in what follows we suppose

$$\Lambda^*(u) = \mathbb{Z}^N, \qquad \Lambda^*(Au) = \Lambda^*(u). \tag{3.3}$$

In particular, it is true that

$$\det A \neq 0. \tag{3.4}$$

Case 1: *The eigenvalues of A are all roots of unity.* In this case we suppose (3.1) admits a solution l for *every integer* $Q \geq 1$. We divide into two subcases:

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

Case 1(a). Suppose A is unipotent. Because of (3.3), the minimal polynomial for A is $(x-1)^N$, and the vectors u, $(A-I)u$, $(A-I)^2u, \ldots, (A-I)^{N-1}u$, which span $\Lambda(u)$, comprise a basis for $\mathbb{R}^N$ with respect to which A has matrix

$$A_0 = \begin{pmatrix} 1 & & & & \\ 1 & & & 0 & \\ 0 & & & & \\ \vdots & & & & \\ 0 & \cdots & 1 & 1 & 0 \\ 0 & \cdots & 0 & 1 & 1 \end{pmatrix}.$$

Recalling the hypothesis of case 1 implies $v \in \Lambda(u)$, (3.1) is equivalent to the congruence

$$A_0^l e_1 \equiv v_0 \pmod{Q} \tag{3.5}$$

where e_n is the nth standard basis vector and $v_0 \in \mathbb{Z}^N$. Now

$$A_0^l e_1 = \begin{pmatrix} 1 \\ \binom{l}{1} \\ \vdots \\ \binom{l}{N-1} \end{pmatrix}. \tag{3.6}$$

Let r be the second coordinate of v_0. By (3.5), (3.6) it is true that if $(Q, N-1)!) = 1$, then

$$v_0 \equiv \begin{pmatrix} 1 \\ \binom{r}{1} \\ \vdots \\ \binom{r}{N-1} \end{pmatrix} \pmod{Q}.$$

Since Q may be arbitrarily large, $v_0 = A^r e_1$.

Case 1(b). A is not unipotent. In this case choose $m > 0$ so that A^m is unipotent, and notice then (under our hypothesis that (3.1) admits a solution for all Q) that there exists ν, $0 \leq \nu < m$, such that the congruence

$$A^{ml} A^{\nu} u \equiv v \pmod{Q}$$

admits a solution l for all Q. Now apply case 1(a).

Case 2: *At least one eigenvalue of A is not a root of unity.* In this case let K be a splitting field for the characteristic polynomial of A, and let $B \in \mathrm{GL}(N, K)$ be such that $B^{-1}AB = J$ is a Jordan form. There is a cofinite set $\mathscr{S}_0 \subseteq \mathscr{M}_0(K)$ such that $B = \mathrm{GL}(N, \mathscr{O}(\mathscr{S}_0))$.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

The block form of J induces a natural decomposition $K^N \cong \bigoplus_{j=1}^{r} K^{d_j}$, where J has r diagonal blocks, the jth block having dimension d_j and form

$$J_j = \begin{pmatrix} \lambda_j & 1 & 0 & \cdots & 0 \\ 0 & \lambda_j & 1 & \cdots & 0 \\ & & \ddots & & \vdots \\ & & & & 0 \\ & 0 & & & 1 \\ & & & & \lambda_j \end{pmatrix}.$$

It is possible $\lambda_i = \lambda_j$ for certain $i \neq j$.

If $\xi = B^{-1}u$, $\eta = B^{-1}v$, write ξ, η with respect to the decomposition above as $\xi = \sum_{j=1}^{r} \xi_j$, $\eta = \sum_{j=1}^{r} \eta_j$. By abuse of notation we view ξ_j, η_j as elements of $\mathcal{O}(\mathcal{S}_0)^{d_j}$.

Let p be a rational prime, and suppose the congruence

$$A^l u \equiv v \pmod{p} \tag{3.7}$$

admits a solution l. For the same l we have

$$J^l \xi \equiv \eta \pmod{p\mathcal{O}(\mathcal{S}_0)^N} \tag{3.8}$$

and also

$$J_j^l \xi_j \equiv \eta_j \pmod{p\mathcal{O}(\mathcal{S}_0)^{d_j}}. \tag{3.9}$$

Now choose j so that λ_j is not a root of unity. Because u is a cyclic vector the last (d_jth) component of ξ_j is non-zero, and if we denote this component by α and the corresponding component of η_j by β, then (3.9) implies

$$\lambda_j^l \alpha \equiv \beta \pmod{p\mathcal{O}(\mathcal{S}_0)}. \tag{3.10}$$

Suppose now that (3.7) admits a solution l for each finite set of primes p in a set, S, of rational primes of upper Dirichlet density 1, and let $\mathcal{S}_1$ be the set of extensions to K of the corresponding valuations. Set $\mathcal{S} = \mathcal{S}_0 \cap \mathcal{S}_1$, and note that by (3.10) the congruence

$$\lambda_j^l \alpha \equiv \beta \pmod{\pi(P)}$$

admits a solution l for each finite set of $P \in \mathcal{S}$. By corollary 2.11 and the remark at the end of § 2 there exists l_0 such that $\lambda_j^{l_0} \alpha = \beta$. Moreover, if l_k is a sequence such that

$$\lim_{k\to\infty} A^{l_k} u \equiv v \pmod{p} \qquad (p \in S) \tag{3.11}$$

then by (3.10)

$$\lim_{k\to\infty} \lambda_j^{l_k} \alpha \equiv \beta \pmod{\pi(P)} \qquad (P \in \mathcal{S}).$$

Since λ_j is not a root of unity, corollary 2.11 also implies

$$\lim_{k\to\infty} l_k \equiv l_0 \pmod{m} \tag{3.12}$$

holds for every integer $m > 0$. This now implies for every prime p that $A^{l_k - l_0} \equiv \mathrm{Id} \pmod{p}$ for large k, and so by (3.11)

$$A^{l_0} u \equiv v \pmod{p}. \tag{3.13}$$

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

Since p may be arbitrarily large, (3.13) implies $A^{l_0}u = v$. Since we have already proved (3.12) implies (3.13), theorem 1.6 is proved.

Using case 1, we also have:

(3.14) THEOREM. *Let A be an $N \times N$ integer matrix such that* $\det A \neq 0$, *and let $u \in \mathbb{Z}^N$. The set $\mathbb{Z}^N \cap \{A^l u | l \in \mathbb{Z}\}$ is closed in the profinite topology of $\mathbb{Z}^N$.*

Suitably restated, theorem 3.14 is also true if $\det A = 0$.

4. *Density of $\langle P(T) \rangle$ in $IPM(T)$*

In this section T will denote a fixed ergodic endomorphism of $\mathbb{T}^N$. The dual endomorphism is determined by an $N \times N$ integral matrix A, whose determinant will be denoted Δ, satisfying

$$\begin{aligned} &\Delta = \det A \neq 0 \\ &\text{No eigenvalue of } A \text{ is a root of 1} \end{aligned} \tag{4.1}$$

Represent $\mathbb{T}^N$ as $\mathbb{T}^N = \mathbb{R}^N/\mathbb{Z}^N$, and if $0 < Q \in \mathbb{Z}$, define $\Gamma(Q) = Q^{-1}\mathbb{Z}^N + \mathbb{Z}^N$; i.e. $\Gamma(Q)$ is the image in $\mathbb{T}^N$ of $Q^{-1}\mathbb{Z}^N$ under the canonical projection. In what follows δ_x denotes a point mass at x, and we recall the notation $e(t) = \exp 2\pi i t$. If $x \in \mathbb{T}^N$, $n \in \mathbb{Z}^N$, the relation between T and A is expressed by

$$e(n \cdot Tx) = e(An \cdot x). \tag{4.2}$$

Fix $n \in \mathbb{Z}^N$, and let $Q > 0$ satisfy $(Q, \Delta) = 1$. Define $\tau = \tau(Q) = \tau(Q, A, n)$ to be the least positive integer such that

$$A^\tau n = n \pmod{Q}. \tag{4.3}$$

τ exists because $(Q, \Delta) = 1$. In general, τ is less than the order of A in $\mathrm{GL}(N, \mathbb{Z}_Q)$.

With notation and assumptions fixed as above, define a complex valued measure, $\mu = \mu(Q) = \mu(Q, A, n)$, by

$$\mu = Q^{-N} \sum_{x \in \Gamma(Q)} \left(\sum_{l=0}^{\tau-1} e(-A^l n \cdot x) \right) \delta_x. \tag{4.4}$$

If $0 \leq k, l < \tau$, and if $A^k n \equiv A^l n \pmod{Q}$, the choice of τ implies $k = l$. This observation and the Schwarz inequality yield for the total variation norm of μ the inequality

$$\begin{aligned} \|\mu\|_{\mathrm{var}}^2 &\leq Q^{-N} \sum_{x \in \Gamma(Q)} \sum_{k,l=0}^{\tau-1} e(A^k n - A^l n) \cdot x) \\ &= \tau, \end{aligned}$$

whence

$$\|\mu\|_{\mathrm{var}} \leq \tau^{\frac{1}{2}}. \tag{4.5}$$

By contrast, a similar calculation reveals that $\hat{\mu}(m) = \mu(e(m \cdot x))$ satisfies

$$\hat{\mu}(m) = \begin{cases} 1 & m \equiv A^l n \pmod{Q} \text{ for some } 0 \leq l < \tau \\ 0 & \text{otherwise} \end{cases} \tag{4.6}$$

and in particular, the pseudomeasure norm of μ satisfies

$$\|\mu\| = 1. \tag{4.7}$$

Of course, $\mu \in \langle P(T) \rangle$.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

If $n \in \mathbb{Z}^N$, $-\infty \leq \nu(n) \leq -1$ is defined to be as small as possible with $A^k n \in \mathbb{Z}^N$ for all $k > \nu$. If $n \neq 0$, define $\lambda(n, A) \in IPM(T)$ to have Fourier series

$$\lambda(n, A) \sim \sum_{k > \nu(n)} e(A^k n \cdot x). \tag{4.8}$$

Now (4.6)-(4.8) combine with theorem 1.6 to yield

(4.9) THEOREM. *Let T be an ergodic endomorphism of $\mathbb{T}^N$, and let $n \in \mathbb{Z}^N$. If $p^{(k)}$ is the product of the first k rational primes prime to Δ, then in the notation of* (4.4) *and* (4.8),

$$\lim_{k \to \infty} \mu(p^{(k)}, A, n) = \lambda(n, A) \tag{4.10}$$

in the weak- topology of $PM(\mathbb{T}^N)$.*

It is evident that $IPM(T)$ is spanned (densely) by the elements $\lambda(n, A)$, $n \in \mathbb{Z}^N$, and therefore that theorem 4.9 implies theorem 1.1.

Remark. Let $\Delta = \det A$, and if $Q > 0$ define $Q_\Delta!$ to be the product of the integers $1 \leq l \leq Q$ such that $(l, \Delta) = 1$. Then it also follows that

$$\lim_{Q \to \infty} \mu(Q_\Delta!, A, n) = \lambda(n, A) \tag{4.11}$$

which is all that is necessary for the application.

It is possible there is a sequence $\{q_k\}$ of primes such that

$$\lim_{k \to \infty} \mu(q_k, A, n) = \lambda(n, A). \tag{4.12}$$

If so, the proof will perhaps involve more delicate number theory.

5. *Periodic points and coboundaries*

In this section we shall consider the coboundary equation

$$g \circ T - g = f \tag{5.1}$$

in which T is an ergodic endomorphism of $\mathbb{T}^N$, $f \in \mathbb{A}(\mathbb{T}^N)$ satisfies certain additional hypotheses, and g is unknown.

Given only that $f \in \mathbb{A}(\mathbb{T}^N)$, $\hat{f}(0) = 0$, it is always possible to solve (5.1) formally as follows. If $n \in \mathbb{Z}^N$, recall that $\nu(n)$ is $-\infty$ or the smallest integer such that $A^k n \in \mathbb{Z}^N$ for all $k > \nu(n)$. Now define g by $g(0) = 0$ and if $n \neq 0$

$$\hat{g}(n) = -\sum_{\nu(n) < k \leq 0} \hat{f}(A^k n) \qquad (n \neq 0). \tag{5.2}$$

The series (5.2) converges because $f \in \mathbb{A}$ and $A^k n \to \infty$ as $k \to \pm\infty$. Now define $g(x) \sim \sum_{n \in \mathbb{Z}^N} \hat{g}(n) e(n \cdot x)$, a formal Fourier series, and check directly that (5.1) holds formally. That is,

$$\begin{aligned} \hat{g}(A^{-1}n) - \hat{g}(n) &= \hat{f}(n), \quad n \in A\mathbb{Z}^N \\ -\hat{g}(n) &= \hat{f}(n), \quad n \notin A\mathbb{Z}^N. \end{aligned}$$

The form (5.2) for $\hat{g}$ is insufficient for providing good estimates. This is to be expected since thus far no assumption has been made on f, other than $f \in \mathbb{A}$. A

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

second form to try is

$$\hat{g}_1(n) = \sum_{k=1}^{\infty} \hat{f}(A^k n) \qquad (n \neq 0). \tag{5.3}$$

But here one computes that

$$\begin{aligned} \hat{g}_1(A^{-1}n) - \hat{g}_1(n) &= \hat{f}(n), \quad n \in A\mathbb{Z}^N \\ -\hat{g}_1(n) &= -\sum_{k=1}^{\infty} \hat{f}(A^k n), \quad n \notin A\mathbb{Z}^N. \end{aligned} \tag{5.4}$$

Moreover, $\hat{g}_1(n) = \hat{g}(n)$ (if and) only if

$$\sum_{\nu(n)<k<\infty} \hat{f}(A^k n) = 0. \tag{5.5}$$

Of course, in the notation of § 4, (5.5) is simply $\lambda(n, A)$ applied to f. Theorem 4.9 thus implies

(5.6) THEOREM. *Let T be an ergodic endomorphism of $\mathbb{T}^N$. If $f \in \mathbb{A}$ satisfies $\sum_{x \in O} f(x) = 0$ for every periodic orbit O of T, and if $\hat{g}(n)$ and $\hat{g}_1(n)$ are defined by* (5.2) *&* (5.3) *respectively, then $\hat{g} \equiv \hat{g}_1$.*

In what follows we suppose $\alpha > 0$, and we define $\mathbb{A}_\alpha$ to be the set of $f \in \mathbb{A}$ for which

$$\|f\|_\alpha = \sup_{n \in \mathbb{Z}^N} |\hat{f}(n)| \, \|n\|^\alpha < \infty \tag{5.7}$$

Denote by $\mathbb{A}_\alpha(T)$ the set of $f \in \mathbb{A}_\alpha$ which also satisfy the hypothesis of theorem 5.6. We shall prove

(5.8) PROPOSITION. *Let T be an ergodic endomorphism of $\mathbb{T}^N$, and let $f \in \mathbb{A}_\alpha(T)$ for some $\alpha > 0$. If $\hat{g}$ is defined by* (5.2) *(or* (5.3)*), then (whether or not $g \in \mathbb{A}$) $\|g\|_\beta < \infty$ for all $\beta < \alpha$.*

To begin the proof of the proposition we appeal to the real canonical form of the dual matrix A, to decompose $\mathbb{R}^N$ into a direct sum $\mathbb{R}^N \cong V_1 \oplus V_2 \oplus V_3$ with the following properties, in terms of fixed constants $C < \infty$, $\rho > 1$, $d \leq N$:

(o) $AV_j = V_j$, $1 \leq j \leq 3$
(i) $\|A^l v\| \geq C\rho^l \|v\|$, $v \in V_1$, $l \geq 0$
(ii) $\|A^l v\| \geq C\rho^{-l} \|v\|$, $v \in V_3$, $l \leq 0$
(iii) $\|A^l v\| \geq C(|l|+1)^{-d} \|v\|$, $v \in V_2$, $l \in \mathbb{Z}$.

It is convenient to use the norm on $\mathbb{R}^N$ which is the sum of the norms on V_j. Thus, if $v = v_1 + v_2 + v_3$, $v_j \in V_j$, then $\|v\| \geq \|v_j\|$, $1 \leq j \leq 3$.

If $n \in \mathbb{Z}^N$, write $n = v_1(n) + v_2(n) + v_3(n)$ with $v_j(n) \in V_j$, $1 \leq j \leq 3$. We shall distinguish three cases, numbered by the least j such that $\|v_j(n)\| = \mathrm{Max}_{1 \leq i \leq 3} \|v_i(n)\|$. Cases 1 and 3 are similar. Thus we shall treat only case 3 and case 2.

Case 3. We use the form (5.2) for $\hat{g}(n)$. By assumption $\|v_3(n)\| \geq \frac{1}{3}\|n\|$, and therefore by (ii)

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

$$
\begin{aligned}
|\hat{g}(n)| &= \left| \sum_{\nu(n)<k\le 0} \hat{f}(A^k n) \right| \\
&\le \|f\|_\alpha \textstyle\sum_{\nu(n)<k\le 0} \|A^k n\|^{-\alpha} \\
&\le \|f\|_\alpha \sum_{\nu(n)<k\le 0} \|A^k v_3(n)\|^{-\alpha} \\
&\le \|f\|_\alpha C^{-\alpha} \|v_3(n)\|^{-\alpha} \sum_{\nu(n)<k\le 0} \rho^{k\alpha} \\
&\le \|f\|_\alpha 3^\alpha C^{-\alpha} \frac{\rho^\alpha}{\rho^\alpha - 1} \|n\|^{-\alpha}.
\end{aligned}
$$

Case 2. Since T is ergodic, lemma 3 of Katznelson [6] implies for each $n \in \mathbb{Z}^N$, $n \neq 0$, that

$$\|v_1(n)\| \ge \gamma \|n\|^{-N} \tag{5.9}$$

for some constant $\gamma > 0$.

Choose an integer l_0 by

$$l_0 = \left[\frac{(N+1)\log \|n\|}{\log \rho} \right] + 1$$

and notice $\rho^{l_0} \ge \|n\|^{N+1}$. We have for $l \ge l_0$

$$
\begin{aligned}
\|A^l n\| &\ge \|A^l v_1(n)\| \\
&\ge C\rho^l \|v_1(n)\| \\
&\ge C\gamma \rho^{l-l_0} \rho^{l_0} \|n\|^{-N} \\
&\ge C\gamma \rho^{l-l_0} \|n\|.
\end{aligned} \tag{5.10}
$$

Using (iii) above it is also true for all $l \ge 0$ that

$$
\begin{aligned}
\|A^l n\| &\ge \|A^l v_2(n)\| \\
&\ge C(1+l)^{-d} \|v_2(n)\| \\
&\ge \frac{C}{3}(1+l)^{-d} \|n\|.
\end{aligned} \tag{5.11}
$$

Now let $\hat{g}(n) = \hat{g}_1(n)$ be defined by the series (5.3). We use (5.11) to bound terms in the range $1 \le k \le l_0$ and (5.10) for terms in the range $k > l_0$. We find

$$\|\hat{g}(n)\| \le 3^\alpha C^{-\alpha} l_0 (1+l_0)^{d\alpha} \|n\|^{-\alpha} + C^{-\alpha} \gamma^{-\alpha} \frac{\rho^\alpha}{\rho^\alpha - 1} \|n\|^{-\alpha}.$$

By the choice of l_0 there is a constant $D = D(\alpha, N)$ such that

$$\|\hat{g}(n)\| \le D(\log \|n\|)^{N\alpha+1} \|n\|^{-\alpha}$$

in case 2, and proposition 5.8 follows.

(5.12) THEOREM. *Let T be an ergodic endomorphism of $\mathbb{T}^N$. If $f \in \mathbb{A}_\alpha(T)$ for some $\alpha > N/2$, then there exists $g \in L^2(\mathbb{T}^N)$ such that*

$$g \circ T - g = f \tag{5.13}$$

holds a.e.

Proof. Apply theorem 5.6 and proposition 5.8 to see that the formal solution (5.2) satisfies $\sum_{n \in \mathbb{Z}^N} |\hat{g}(n)|^2 < \infty$.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

If $\alpha > 0$, let $C^\alpha = C^\alpha(\mathbb{T}^N)$ be the set of functions which have continuous partial derivatives of order $\leq [\alpha]$ and whose partial derivatives of order $[\alpha]$ are Hölder continuous with exponent $\alpha - [\alpha]$. One has $C^\alpha \subseteq \mathbb{A}$ if $\alpha > N/2$ ([13]). Also, define L^2_β, $\beta \geq 0$, to be the set of $f \in L^2(\mathbb{T}^N)$ which satisfy $\sum_n \|n\|^{2\beta} |\hat{f}(n)|^2 < \infty$. By the Sobolov theorem, if $\beta > N/2$, $\alpha \geq 0$, then $L^2_{\alpha+\beta} \subseteq C^\alpha$.

(5.14) COROLLARY. *Let T be an ergodic endomorphism of $\mathbb{T}^N$, and let $\gamma = \alpha + \beta$, where $\beta > N$ and $\alpha \geq 0$. If $f \in C^\gamma$ is such that $\sigma_x(f) = 0$ for all $x \in P(T)$, there exists $g \in C^\alpha$ such that* (5.13) *holds (identically).*

Proof. Let $N < \beta' < \beta$, and let g be the Fourier coefficients defined by (5.2). By proposition 5.8, $|\hat{g}(n)| = O(\|n\|^{-\beta'-\alpha})$, and therefore $g \in L^2_{(\beta'/2)+\alpha}$. By the Sobolov theorem $g \in C^\alpha$.

(5.15) COROLLARY. *With notation and assumptions as in theorem* 5.12 *and corollary* 5.14, *if $f \in C^\infty$ is such that $\sigma_x(f) = 0$ for all $x \in P(T)$, there exists $g \in C^\infty$ such that* (5.13) *holds identically.*

If $0 \leq \alpha \leq \infty$, then C^α carries the natural structure of a Banach space ($\alpha < \infty$) or a Frechet space ($\alpha = \infty$). The dual of C^α will be denoted by M^α, and $IM^\alpha(T)$ has the obvious meaning for a given endomorphism T. One has $\langle P(T) \rangle \subseteq IM^\alpha(T)$, and so for every α there is a question of density relative to any topology between the weak-* and strong topologies on M^α.

In what follows T is an ergodic endomorphism, $B_\alpha(T)$ is the set of $f = g \circ T - g$ such that $g \in C^\alpha$, and $E_\alpha(T)$ is the set of $f \in C^\alpha$ such that $\sigma_x(f) = 0$ for all $x \in P(T)$. Of course, $B_\alpha \subseteq C_\alpha$ for all α. The following lemma involves a standard application of the Hahn Banach theorem:

(5.16) LEMMA. *If $B_\alpha(T)$ is dense in $E_\alpha(T)$ (for the topology of C^α), then $\langle P(T) \rangle$ is weak-* dense in IM^α.*

(5.17) THEOREM. *Let T be an ergodic endomorphism of $\mathbb{T}^N$. Then $\langle P(T) \rangle$ is dense in IM^∞, the space of T-invariant Schwartz distributions, for the strong topology.*

Proof. $\langle P(T) \rangle$ is weak-* dense in IM^∞ by corollary 5.15 and lemma 5.16. Since C^∞ is reflexive, density in the strong topology is a consequence of the Banach-Mazur theorem.

If $\alpha = 0$, and if T is an ergodic endomorphism of $\mathbb{T}^N$, then according to Marcus [11], $\langle P(T) \rangle$ is weak-* dense in $IM^0(T)$, the space of finite invariant Borel measures on $\mathbb{T}^N$.

Question. Let $0 < \alpha < \infty$, and let T be an ergodic endomorphism of $\mathbb{T}^N$. Is $\langle P(T) \rangle$ weak-* dense in $IM^\alpha(T)$?

In the case that T is *hyperbolic*, Livsic [9] proves $B_1(T) = E_1(T)$, and therefore $\langle P(T) \rangle$ is weak-* dense in $IM^1(T)$. In § 6 we will demonstrate that $B_1(T) \neq E_1(T)$ for *every* ergodic endomorphism which is not hyperbolic.

With much stronger hypotheses on T (that its dual matrix is diagonalizable over $\mathbb{R}$) Livšic [9] proves $f \in B_\alpha(T)$ as soon as $f \in E_\alpha(T)$ and the partial derivatives of f up to order $[\alpha]$ belong to $\mathbb{A}$.

Finally, we note that if $\gamma = \alpha + \beta$ with $\beta > N$ and $\alpha \geq 0$, and if T is an ergodic endomorphism of $\mathbb{T}^N$, then by corollary 5.14

$$E_{\alpha+\beta}(T) \subseteq B_\alpha(T) \qquad (\alpha \geq 0, \beta > N). \tag{5.18}$$

We have:

(5.19) THEOREM. *Let T be an ergodic endomorphism of $\mathbb{T}^N$, and let $\gamma = \alpha + \beta$, where $\alpha \geq 0$ and $\beta > N$. The weak-* closure of $\langle P(T)\rangle$ in IM^γ contains IM^α.*

Proof. Apply a variant of lemma 5.16 to (5.18).

Remark. With regard to the hypotheses of lemma 5.16 it should be noted that because $E_\infty(T) = B_\infty(T)$, it would suffice to prove $E_\infty(T)$ is dense in $E_\alpha(T)$.

Remark. If $\alpha > N/2$, then because $C^\alpha \hookrightarrow \mathbb{A}$ is a continuous inclusion, it follows that (4.10) holds in the strong topology on M^α. This raises the question of characterizing the closed linear span of $\{\lambda(n, A) | n \in \mathbb{Z}^N, n \neq 0\}$ in the weak-* or strong topologies of M^α. Riesz (or Bessel) potentials may be useful for this purpose, at least for non-integral α. (The auxiliary functions in § 7 are Riesz potentials with $N = 1$.)

6. *Proof of proposition* 1.5

If T is an hyperbolic endomorphism of $\mathbb{T}^N$, and if $f \in C^1(\mathbb{T}^N)$ satisfies $\sigma_x(f) = 0$ for all $x \in P(T)$, then according to Livsic [**9**] there exists $g \in C^1(\mathbb{T}^N)$ such that $g \circ T - g = f$. In this section we shall apply the closed graph theorem to demonstrate that Livsic's statement is false for any ergodic endomorphism whose dual matrix admits an eigenvalue of modulus 1.

In what follows T is a fixed ergodic endomorphism of $\mathbb{T}^N$, and A is its dual matrix. It is assumed of A that at least one eigenvalue has absolute value 1. Since A has no root of unity among its eigenvalues, the real canonical form for A implies there exists an inner product $\langle\ ,\ \rangle$ on $\mathbb{R}^N$, a $Q > 0$, and a $2Q$-dimensional subspace, W, of $\mathbb{R}^N$ such that (i) $AW = W = A^* W$, where $*$ denotes adjoint relative to $\langle\ ,\ \rangle$, and (ii) there is a 2×2 (irrational) rotation matrix, R_θ, and a basis for W, relative to which A has matrix

$$\begin{pmatrix} R_\theta & I_2 & 0 & \cdots & 0 \\ 0 & R_\theta & I_2 & \cdots & 0 \\ & & \ddots & & \vdots \\ & 0 & & \ddots & I_2 \\ & & & & R_\theta \end{pmatrix} \tag{6.1}$$

and A^* has matrix α^t. Note that α has dimension $2Q$. Elements of W will be written as Q-tuples of two-dimensional vectors. In particular, $V \subseteq W$ denotes the set of Q-tuples $(v, 0, \ldots, 0)$. α acts as an isometry on V.

Below, c denotes a positive constant which depends only upon N, $\langle\ ,\ \rangle$, and A. $\|\cdot\|$ is the norm associated to $\langle\ ,\ \rangle$, and $\rho > 1$ is the operator norm of A relative to $\|\cdot\|$.

Let $V \subseteq W$ be as above, and define $l(v) = l$ for $v \in V$, $\|v\| > \rho$, by

$$l = \left[\frac{\log \|v\|}{\log \rho}\right]. \tag{6.2}$$

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

Clearly

$$\rho^k \le \|v\| \qquad (0 \le k \le l). \tag{6.3}$$

If $v \in V$, there exists $n(v) \in \mathbb{Z}^N$ such that $\|v - n(v)\| < c$. We have the inequalities

$$\begin{aligned} \|A^k n(v)\| &\le \|A^k v\| + \|A^k(n(v) - v)\| \\ &\le \|v\| + c\rho^k \end{aligned}$$

and therefore by (6.3) (with a new c)

$$\|A^k n(v)\| \le c\|v\| \quad (0 \le k \le l(v)). \tag{6.4}$$

With notation as above, define a trigonometric polynomial, $G_v(x)$, by

$$G_v(x) = \sum_{k=0}^{l(v)-1} e(A^k n(v) \cdot x). \tag{6.5}$$

If $\|\cdot\|^1$ is the C^1 norm on $C^1(\mathbb{T}^N)$, then $G_v \circ T - G_v = e(A^l n(v) \cdot x) - e(n(v) \cdot x)$ satisfies by (6.4)

$$\|G_v \circ T - G_v\|^1 \le c\|v\|. \tag{6.6}$$

Let $L \in \mathbb{R}^N$ be viewed as a vector field on $\mathbb{T}^N$. The L^2 norm of LG_v is given, by abuse of notation, by

$$\|LG_v\|_2^2 = \sum_{k=0}^{l-1} (LA^k n(v))^2. \tag{6.7}$$

Choose $L \in \mathbb{R}^N$ to satisfy $L \cdot M = \langle v/\|v\|, M\rangle$, $M \in \mathbb{R}^N$. If $w(v)$ is the orthogonal projection (for $\langle \cdot, \cdot \rangle$) of $n(v)$ on W, then

$$LA^k n(v) = \left\langle \frac{v}{\|v\|}, A^k n(v) \right\rangle = \left\langle \frac{v}{\|v\|}, A^k w(v) \right\rangle = \left\langle \frac{v}{\|v\|}, \alpha^k w(v) \right\rangle = \frac{v}{\|v\|} \alpha^k w(v),$$

the last relative to the chosen basis for W. If $w(v) = (w_1(v), \ldots, w_Q(v))$, then

$$\frac{v}{\|v\|} \alpha^k w(v) = \sum_{j=0}^{Q-1} \binom{k}{j} \frac{v}{\|v\|} R_\theta^{k-j} w_{j+1}(v). \tag{6.8}$$

Now $\|v - w_1(v)\| \le c$ and $\|w_j(v)\| \le c$, $2 \le j \le Q$, and so

$$\begin{aligned} \frac{v}{\|v\|} \alpha^k w(v) &\ge \frac{v}{\|v\|} R_\theta^k v - ck^{Q-1} \\ &= \|v\| \cos 2\pi k\theta - ck^{Q-1}. \end{aligned}$$

In the range $0 \le k \le l(v)$ it follows that

$$LA^k n(v) \ge \|v\| \cos 2\pi k\theta - c(\log \|v\|)^{Q-1}. \tag{6.9}$$

Now let $R < \infty$ such that $R > 2c\,(\log R)^{Q-1}$, so that by (6.9)

$$LA^k n(v) \ge \|v\|(\cos 2\pi k\theta - \tfrac{1}{2}) \qquad (\|v\| > R,\ k \le l(r)). \tag{6.10}$$

As $\|v\| \to \infty$ implies $l(v) \to \infty$, (6.10) and (6.7), together with the Kronecker–Weyl theorem, imply

$$\begin{aligned} \|LG_v\|_2^2 &\ge cl\|v\|^2 \\ &\ge c \log \|v\| \cdot \|v\|^2. \end{aligned}$$

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

From this we conclude

$$\|G_v\|^1 \geq c(\log \|v\|)^{\frac{1}{2}}\|v\| \tag{6.11}$$

holds for large $\|v\|$, $v \in V$.

Continuing with T as above, define $E^1(T)$ to be the set of $f \in C^1(\mathbb{T}^N)$ such that $\sigma_x(f) = 0$ for all $x \in P(T)$. C_0^1 denotes the set of $g \in C^1(\mathbb{T}^N)$ such that $\hat{g}(0) = 0$. The operator $\Phi g = g \circ T - g$ is continuous, linear and injective from C_0^1 into $E^1(T)$. If Φ is surjective, then because C_0^1 and $E^1(T)$ are closed in $C^1(\mathbb{T}^N)$, the closed graph theorem implies the existence of $\gamma > 0$ such that $\|\Phi g\|^1 \geq \gamma \|g\|^1$, $g \in C_0^1$. But by (6.6) and (6.11) no such γ can exist.

7. *Distributions on* $\mathbb{T}^1$

In this section we shall be concerned with infinite series whose terms are measures on $\mathbb{T}^1$ and whose sums, when they exist, are distributions on $\mathbb{T}^1$. The object is to determine the least value of α such that the series converge in the space of distributions of order α.

Functions on $\mathbb{T}^1$ will be viewed interchangeably as functions on $\mathbb{R}$ with period 1. If B is a space of integrable functions on $\mathbb{T}^1$, B^0 will denote the set of $f \in B$ such that $\hat{f}(0) = 0$. If $n \geq 1$, ω_n denotes the measure on $\mathbb{T}^1$ corresponding to $(1/n)\sum_{j=0}^{n-1} \delta_{j/n}$ on $\mathbb{R}$. If $q > 1$, and if $(q, n) = 1$, then $\omega_n \in IM(T_q)$, where $T_q x = qx \pmod 1$.

The series to be considered in this section have the form

$$\sum_{\substack{\nu=1 \\ (\nu,q)=1}}^{\infty} \mu(\nu)\omega_{n\nu} = \eta(n, q). \tag{7.1}$$

Here $\eta = \eta(n, q)$ depends upon fixed $n, q \geq 1$ and the Möbius function $\mu(\cdot)$.

It is possible to assign Fourier coefficients to η. First, declare $\hat{\eta}(0) = 0$. Also, because $\hat{\omega}_l(k) = 1$ or 0 as $l|k$ or not, declare $\hat{\eta}(k) = 0$ unless $n|k$. Finally, if $n|k$, say $k = nl$, $l \neq 0$, compute term by term in (7.1) and sum to find

$$\hat{\eta}(k) = \sum_{\substack{\nu|l \\ (\nu,q)=1}} \mu(\nu). \tag{7.2}$$

Because $\sum_{d|r} \mu(d) = 1$ or 0 as $r = 1$ or $r > 1$, the sum (7.3) is 1 if every prime which divides $l = k/n$ also divides q, and otherwise it is 0. If $\Gamma(n, q)$ is the set of $k = nl$ for which the sum is 1, then we have the formal identity

$$\sum_{\substack{\nu=1 \\ (\nu,n)=1}}^{\infty} \mu(\nu)\omega_{n\nu} = \sum_{k \in \Gamma(n,q)} e(kx). \tag{7.3}$$

While the series on the right in (7.3) converges in the weak-* topology of $(\mathbb{A}^0)^*$ (and $\mathbb{A}^*$), the series on the left is more delicate.[1] For if Ω_N is the Nth partial sum on the left, and if $N_q!$ is the product of those integers ν such that $1 \leq \nu \leq N$ and

[1] A rearrangement of (7.1) has a subsequence of partial sums converging weak-* in $(\mathbb{A}^0)^*$. This is all that is necessary for the applicaion to theorem 7.6. In our view theorem 7.5 is intrinsically more interesting.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

$(\nu, q) = 1$, then

$$\hat{\Omega}_N(N_q!) = \sum_{\substack{\nu=1 \\ (\nu,q)=1}}^{N} \mu(\nu). \tag{7.4}$$

The right side of (7.4) is well known to be unbounded in N, and therefore $\{\Omega_N\}$ is unbounded in $(\mathbb{A}^0)^*$. Thus, the left side of (7.3) does not converge weak-$*$ in $(\mathbb{A}^0)^*$. Indeed, by the Banach-Steinhaus theorem, there exists $f \in \mathbb{A}^0$ such that $\limsup_{N\to\infty} \Omega_N(f) = \infty$.

If $\alpha > 0$, define Λ_α to be the space of Hölder functions of exponent α on $\mathbb{T}^1$, identified, as above, with the corresponding space of periodic Hölder functions on $\mathbb{R}$. We shall prove

(7.5) THEOREM. *If $\alpha > \frac{1}{2}$, the series* (7.1) *converges in norm in $(\Lambda_\alpha^0)^*$, and the identity* (7.3) *is true.*

Suppose now $q = p$ is prime. In this case $\Gamma(n, p) = \{\pm np^k\}$, and if $(n, p) = 1$, the right side of (7.3) is simply $\lambda(n, p) + \lambda(-n, p)$, where $\lambda(\pm n, p)$ is the pseudomeasure of § 4, associated to $\pm n$ and the 1×1 matrix $A = \{p\}$.

(7.6) THEOREM. *Let $p > 1$ be prime. If $\alpha > \frac{1}{2}$, and if $f \in \Lambda_\alpha^0$ is an even function such that $\omega_m(f) = 0$ whenever $(m, p) = 1$, there exists $g \in \Lambda_\alpha^0$ such that*

$$g(T_p x) - g(x) = f(x) \qquad (x \in \mathbb{R}). \tag{7.7}$$

Proof. Theorem 7.5 and the hypotheses on f imply $\lambda(n, p)(f) = 0$ for all n such that $(n, p) = 1$. (Note that $\lambda(n, p)(f) = \lambda(-n, p)(f)$ because f is even.) It follows (as in [**9**]) that $\sigma_x(f) = 0$ for *all* $x \in P(T_p)$, and therefore by the Livsic argument [**9**] the solution $g \in \Lambda_\alpha^0$ to (7.7) also exists.

Example. We define $f \in L^2$ to have Fourier cosine series

$$f(x) = \sum_{\nu=1}^{\infty} \frac{\mu(\nu)}{\nu} \cos 2\pi\nu x \tag{7.8}$$

According to Davenport [**5**] the functions $P_m(x) = \sum_{\nu=1}^{m} \mu(\nu) \cos 2\pi\nu x$ satisfy the estimate $\|P_m\|_\infty = O(m(\log m)^{-h})$ for any given $h > 0$. If we choose $h > 1$, then summation by parts in (7.8) leads to the conclusions that the series converges uniformly and $f \in C(\mathbb{T}^1)$. We compute that for any $k \geq 1$

$$\omega_k(f) = \sum_{\substack{\nu=1 \\ k|\nu}}^{\infty} \frac{\mu(l)}{l} = \frac{\mu(k)}{k} \sum_{\substack{l=1 \\ (l,k)=1}}^{\infty} \frac{\mu(l)}{l} = 0, \tag{7.9}$$

the last equality by the prime number theorem.

If p is a prime, if n is square free, and if $(n, p) = 1$, then $\lambda(n, p)(f) = ((p-1)/p)(\mu(n)/n) \neq 0$, and it follows (7.7) admits no integrable solution. Of course, $f \notin \Lambda_\alpha$ for any $\alpha > \frac{1}{2}$. In § 8 we make the observation that if $f \in \bigcap_{\alpha<\frac{1}{2}} \Lambda_\alpha$, the Generalized Riemann Hypothesis for cyclotomic fields is true. We do not know if the converse is true.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

In order to prove theorem 7.5 we introduce the functions ψ_β, $\beta>0$, defined by their Fourier series as

$$\psi_\beta(x)=(2\pi)^{-\beta}\sum_k{}'\frac{e\left(-\frac{\beta}{4}\operatorname{sgn}(k)\right)e(kx)}{|k|^\beta} \tag{7.10}$$

where $'$ denotes omission of the $k=0$ term. If $0<\beta<\alpha$, then $\psi_\beta\in L^p_{\mathrm{loc}}$ for $p<1/(1-\beta)$, and if convolution is understood to be on the group $\mathbb{T}^1$, then

$$\psi_\beta * \Lambda^0_{\alpha-\beta}=\Lambda^0_\alpha \qquad (0<\beta\le\alpha). \tag{7.11}$$

For these and other properties of ψ_β see [**16**, Vol. 1, Ch. II, Sec. 13 and Vol. II, Ch. XII, Secs. 8–9]. We record for later reference that if ϕ_β, $\beta>0$, is defined to be periodic with period 1 satisfying

$$\phi_\beta(x)=\begin{cases}0 & -\frac{1}{2}<x\le 0\\ x^{\beta-1} & 0<x\le\frac{1}{2}\end{cases} \tag{7.12}$$

then

$$\phi_\beta-\psi_\beta\in L^\infty(\mathbb{R}). \tag{7.13}$$

If $\|\cdot\|$ denotes distance to nearest integer, then (7.12) & (7.13) imply there is a constant $C(\beta)<\infty$ such that

$$|\psi_\beta(x)|\le C(\beta)\|x\|^{\beta-1}. \tag{7.14}$$

We remark that $-\psi_1(x)=\{x\}-\frac{1}{2}$, where $\{\cdot\}$ denotes fractional part. The lemma to follow is thus an extension of [**7**, Satz 484] from $\beta=1$ to $\beta>\frac{1}{2}$:

(7.15) Lemma. *Suppose $\beta>\frac{1}{2}$. If $a, b\ge 1$ are integers, then*

$$\int_0^1\psi_\beta(ax)\overline{\psi_\beta(bx)}\,dx=\frac{2\zeta(2\beta)(a,b)^{2\beta}}{(2\pi)^{2\beta}(ab)^\beta}. \tag{7.16}$$

Proof. ψ_β is real, but the conjugate in the integral makes for ease of calculation in the Parseval relation. If $\{a,b\}=\operatorname{lcm}(a,b)=ab/(a,b)$, the values of k, k' which are paired for the Parseval relation satisfy $ka=k'b$ or, what is the same, $k=\tau\{a,b\}/a$ and $k'=\tau\{a,b\}/b$. As then $\operatorname{sgn} ka=\operatorname{sgn}\tau=\operatorname{sgn} k'b$, (7.10) implies the integral (7.16) has the value

$$(2\pi)^{-2\beta}\sum_{\tau=-\infty}^{\infty}{}'\frac{(ab)^\beta}{(\{a,b\}|\tau|)^{2\beta}}=\frac{2\zeta(2\beta)}{(2\pi)^{2\beta}}\frac{(a,b)^{2\beta}}{(ab)^\beta}. \tag{7.17}$$

The lemma is proved.

(7.18) Lemma. *Let $\beta>0$. If $t\notin\mathbb{Q}$, then for all $0<n$, $\nu\in\mathbb{Z}$*

$$\int_0^1\psi_\beta(x-t)\omega_{n\nu}(dx)=\frac{1}{(n\nu)^\beta}\psi_\beta(-n\nu t). \tag{7.19}$$

Proof. The integral may be evaluated using (7.10). The resulting series again has the form (7.10) with x replaced by $-n\nu t$, after one notices that $\operatorname{sgn}(n\nu\tau)=\operatorname{sgn}\tau$ for all $\tau\ne 0$. Thus, (7.19) holds.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

Now let $0<q, n$ be fixed, and set up a new function Ψ_β *formally* as

$$\Psi_\beta(t)=\frac{1}{n^\beta}\sum_{\substack{\nu=1\\(\nu,q)=1}}^{\infty}\frac{\mu(\nu)}{\nu^\beta}\psi_\beta(-\nu nt). \tag{7.20}$$

(7.21) PROPOSITION. *Let $0<\beta<\alpha$, and suppose the series* (7.20) *converges in $L^1[0,1]$. Then the series* (7.1) *converges in the norm of* $(\Lambda_\alpha^0)^*$.

Proof. There exists a constant $C(\alpha,\beta)<\infty$ such that each $f\in\Lambda_\alpha^0$ has the form $f=\psi_\beta * g$ for a unique $g\in\Lambda_{\alpha-\beta}^0$ with $\|g\|^{(\alpha-\beta)}\le C(\ ,\ )\|f\|^{(\alpha)}$, where $\|f\|^{(\gamma)}$ is the Hölder norm. By (7.19) & (7.20) and the assumed L^1 convergence of (7.20)

$$\sum_{\substack{\nu=1\\(\nu,q)=1}}^{\infty}\mu(\nu)\omega_{n\nu}(f)=\frac{1}{n^\beta}\sum_{\substack{\nu=1\\(\nu,q)=1}}^{\infty}\frac{\mu(\nu)}{\nu^\beta}\int_0^1\psi_\beta(-\nu nt)g(t)\,dt$$

$$=\int_0^1\Psi_\beta(t)g(t)\,dt \tag{7.22}$$

If ε_N is the L^1 norm of the Nth tail of the series (7.20), the Nth tail of the second series in (7.22) has absolute value at most

$$\varepsilon_N\|g\|_\infty\le\varepsilon_N\|g\|^{(\alpha-\beta)}\le C(\alpha,\beta)\varepsilon_N\|f\|^{(\alpha)}.$$

Thus, the series (7.1) converges in $(\Lambda_\alpha^0)^*$, as claimed.

Remark. If $q=p$ is *prime*, and if (7.1) converges in $(\Lambda_\alpha^0)^*$, the formal calculation leading to (7.5) is valid. If (7.20) converges in L^1, one finds similarly

$$\sum_{\substack{\nu=1\\(\nu,p)=1}}^{\infty}\frac{\mu(\nu)}{\nu^\beta}\psi_\beta(-n\nu t)=\frac{2}{(2\pi)^\beta}\sum_{k=0}^{\infty}\frac{\cos 2\pi\left(\frac{\beta}{4}+np^kt\right)}{p^{k\beta}}$$

in the L^1 sense. If $q=1$, we have

$$\sum_{\nu=1}^{\infty}\frac{\mu(\nu)}{\nu^\beta}\psi_\beta(-n\nu t)=\frac{2}{(2\pi)^\beta}\cos 2\pi\left(\frac{\beta}{4}+nt\right).$$

In the case $\beta=1$ and $n=1$, $\psi_1(-\nu t)=-(\{\nu t\}-\frac{1}{2})$, and one has

$$\sum_{\nu=1}^{\infty}\frac{\mu(\nu)}{\nu}(\{\nu t\}-\tfrac{1}{2})=-\frac{\sin 2\pi t}{\pi} \tag{7.23}$$

The formula (7.23) is due to Davenport ([**4**], [**5**]) who proved the series on the left converges uniformly in t.

(7.24) THEOREM. *If $\beta>\frac{1}{2}$, the series* (7.20) *converges in the L^2 norm.*

Proof. Because $t\to nt \pmod 1$ is an isometry on L^2, it is sufficient to deal with the case $n=1$, $\beta>\frac{1}{2}$. If $N\ge 1$, define $S_N(t)$ by

$$S_N(t)=\sum_{\substack{\nu=1\\(\nu,q)=1}}^{N-1}\frac{\mu(\nu)}{\nu^\beta}\psi_\beta(\nu t).$$

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

Using (7.16) we compute for $N \le M$

$$\|S_{M+1} - S_N\|_2^2 = \gamma(\beta) \sum_{\substack{a,b=N \\ (q,ab)=1}}^{M} \frac{\mu(a)\mu(b)}{(ab)^{2\beta}} (a,b)^{\beta}. \tag{7.25}$$

If $1 \le d \le M$ and $(d, q) = 1$, the pairs a, b in (7.25) which have $(a, b) = d$ have the form $a = dQ$, $b = dR$ with $(Q, R) = 1 = (d, QR)$ and $N/d \le Q, R \le M/d$. It follows therefore that

$$\|S_{M+1} - S_N\|_2^2 = \gamma(\beta) \sum_{\substack{d=1 \\ (d,q)=1}}^{M} \frac{1}{d^{2\beta}} \sum_{\substack{N/d \le R,Q \le M/d \\ (R,Q)=1=(q,RQ)}} \frac{\mu(Rd)\mu(Qd)}{Q^{2\beta}R^{2\beta}} \tag{7.26}$$

If $1 \le d \le N$, the inner sum is $O((d/N)^{2(2\beta-1)})$. The contribution of the terms in which $1 \le d \le N$ is therefore $O(\sum_{d=1}^{N} d^{-2\beta}(d/N)^{2(2\beta-1)}) = O(N^{1-2\beta})$. If $d > N$, the inner sum in (7.26) is $O(\zeta^2(2\beta))$, and so the terms in which $d > N$ contribute $O(\sum_{N+1}^{\infty} d^{-2\beta}) = O(N^{1-2\beta})$. It follows the series (7.20) converges in L^2, as claimed.

We remark that if the series (7.20) converges in L^1 for all $\beta > 0$, and $q = 1$, then the function f in (7.8) belongs to none of the spaces Λ_β, $\beta > 0$. For if $f \in \Lambda_\beta$, then (7.3) applied to f says $0 \equiv \mu(n)/n$ (because $\Gamma(n, 1) = \{\pm n\}$) which is absurd.

While the series (7.23) does converge uniformly in t, the summands of the series (7.20) are unbounded when $\beta < 1$. However, we do have

(7.27) THEOREM. *If $\beta > \frac{2}{3}$, the series* (7.20) *converges a.e. in t.*

Proof. The proof is a modification of an argument which goes back to Weyl ([**15**, p. 346]). With notation as above we have that $\|\Psi_\beta - S_N\|_2^2 = O(N^{1-2\beta})$ for $\beta > \frac{1}{2}$, and therefore if $\beta > \frac{2}{3}$, S_{N^3} converges a.e. to Ψ_β. It remains to estimate for $N^3 \le r < (N+1)^3$ the contribution to S_r of the sum $S_r - S_{N^3}$. We shall prove it is $O(N^{2-3\beta+\varepsilon})$ for any $\varepsilon > 0$ and a.e. t such that $S_{N^3}(t) \to \Psi_\beta(t)$.

Fix $\varepsilon > 0$ small enough that $2 - 3\beta + 4\varepsilon(1-\beta) < 0$. It is true for a.e. t that

$$\lim_{N\to\infty} S_{N^3}(t) = \Psi_\beta(t) \tag{7.28}$$

$$\|at\| \ge c|a|^{-1-\varepsilon} \qquad (a \in \mathbb{Z} - \{0\})$$

where $c = c(t, \varepsilon) > 0$ and $\|\cdot\|$ is distance to nearest integer. In what follows we suppose t satisfies (7.28).

Let $0 \le k \le \log_3 N^2$. We divide $[N^3, (N+1)^3)$ into equal intervals of length $[(3N^2 + 3N + 1)/3^k]$ with one of smaller length left over. The number of intervals in this decomposition is $O(3^k + (3^{2k}/N^2))$. Let I be one of these intervals ('stage k'), and suppose $a, b \in I$ with $a \ne b$. By (7.28)

$$\|(a-b)t\| \ge c\left[\frac{3N^2+3N+1}{3^k}\right]^{-1-\varepsilon} \tag{7.29}$$

If a satisfies

$$\|at\| \le c\left[\frac{3N^2+3N+1}{3^{k-1}}\right]^{-1-\varepsilon}, \tag{7.30}$$

then by (7.29) & (7.30)

$$\|bt\| \ge c(AB-1)\left[\frac{3N^2+3N+1}{3^{k-1}}\right]^{-1-\varepsilon}, \tag{7.31}$$

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

where

$$A=\left[\frac{3N^2+3N+1}{3^k}\right]^{-1-\varepsilon}\geq\left(\frac{3N^2+3N+1}{3^k}\right)^{-1-\varepsilon},$$

$$B=\left[\frac{3N^2+3N+1}{3^{k-1}}\right]^{1+\varepsilon}\geq\left(\frac{3N^2+3N+1}{3^k}-1\right)^{1+\varepsilon}$$

Since $3^k\leq N^2$ by definition, $AB>(3-\frac{1}{3})^{1+\varepsilon}>\frac{7}{3}$, and $AB-1>\frac{4}{3}$. Now (7.31)implies (7.30) is false if a is replaced by b or any other element from I. We conclude that for any k satisfying $0\leq k\leq\log_3 N^2$ there are at most $O(3^k+(3^{2k}/N^2)$ solutions to (7.30) in the interval $[N^3,(N+1)^3)$. We note that there is at most 1 solution to (7.30) with $k=0$ and this solution satisfies $\|at\|\geq c(N+1)^{-3(1+\varepsilon)}$.

Returning to (7.13) we see that there are at most $O(3^k+3^{2k}/N^2)$ solutions $a\in[N^3,(N+1)^3)$ to

$$|\psi_\beta(at)|\geq C(\beta)c^{\beta-1}\left[\frac{3N^2+3N+1}{3^{k-1}}\right]^{(1+\varepsilon)(1-\beta)}$$

and that $|\psi_\beta(at)|\leq C(\beta)c^{\beta-1}(N+1)^{3(1+\varepsilon)(1-\beta)}$ for all a. Values of $a\in[N^3,(N+1)^3)$ which are unaccounted for by (7.30) for some $k\leq\log_3 N^2$ are $O(N^2)$ in number and contribute individually $O(N^{-3\beta})$ to any sum $S_r-S_{N^3}$, $N^3\leq r\leq(N+1)^3$. Recall the summands are $(\mu(a)/a^\beta)\psi_\beta(at)=O(N^{-3\beta}\psi_\beta(at))$, for $N^3\leq a\leq(N+1)^3$.) It follows that if $N^3\leq r\leq(N+1)^3$, then $S_r(t)-S_{N^3}(t)$ is dominated by

$$O\left(\frac{N^2}{N^{3\beta}}\right)+O\left(\frac{N^{3(1+\varepsilon)(1-\beta)}}{N^{3\beta}}\right)+\sum_{k=0}^{[\log_3 N^2]}O\left(\left(3^k+\frac{3^{2k}}{N^2}\right)\left(\frac{3N^2+3N+1}{3^{k-1}}\right)^{(1+\varepsilon)(1-\beta)}\right)$$

$$=O(N^{2-3\beta})+O\left(N^{2(1+\varepsilon)(1-\beta)-3\beta}\sum_{k=0}^{[\log_3 N^2]}\left(3^{k(\beta+\varepsilon(1-\beta))}+\frac{3^{k(1+\beta+\varepsilon(1-\beta))}}{N^2}\right)\right)$$

$$=O(N^{2-3\beta}+N^{2(1+\varepsilon)(1-\beta)-3\beta}N^{2(\beta+\varepsilon(1-\beta))})$$

$$=O(N^{2-3\beta}+N^{2-3\beta+4\varepsilon(1-\beta)}).$$

The last term is $O(1)$ by the choice of ε, and the theorem is proved.

8. *Hölder continuity and the Riemann Hypothesis for L-series*

In this section we consider the series

$$F(x)=\sum_{\nu=1}^{\infty}\frac{\mu(\nu)}{\nu}e(\nu x), \tag{8.1}$$

whose real and imaginary parts are the series (7.8) and its conjugate, respectively. The argument in § 7 shows the series (8.1) converges uniformly. Moreover, Privalov's Theorem ([1]) implies for $0<\alpha<1$ that $f\in\Lambda_\alpha$ if, and only if, $F\in\Lambda_\alpha$.

To describe a connection between (8.1) and L-series, let $q\geq 1$, and let χ be a Dirichlet character mod q. The Gauss sum, $\tau_a(\chi)$, is defined for $a\in\mathbb{Z}$ by

$$\tau_a(\chi)=\sum_{j=0}^{q-1}\chi(j)e\left(\frac{aj}{q}\right). \tag{8.2}$$

Now χ is represented by its Fourier series on $(\mathbb{Z}/q\mathbb{Z})$:

$$\chi(n)=\frac{1}{q}\sum_{a=0}^{q-1}\tau_{-a}(\chi)e\left(\frac{an}{q}\right). \tag{8.3}$$

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

Recall that $L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)/n^s$ and

$$L^{-1}(s,\chi))=\sum_{n=1}^{\infty}\frac{\mu(n)\chi(n)}{n^s}\qquad(\mathrm{Re}\,s\geq 1), \tag{8.4}$$

the series converging for $\mathrm{Re}\,s=1$ (by the prime number theorem for arithmetic progressions). Now (8.3) and (8.1) imply

$$L^{-1}(1,\chi)=\frac{1}{q}\sum_{a=0}^{q-1}\tau_{-a}(\chi)F\left(\frac{a}{q}\right) \tag{8.5}$$

(8.6) PROPOSITION. *Let F be defined by* (8.1). *If α is such that $0<\alpha<\frac{1}{2}$ and $F\in\Lambda_\alpha$, then for all $q\geq 1$ and Dirichlet characters χ* mod q *the L-series $L(s,\chi)$ has no zero s with* $\mathrm{Re}\,s>1-\alpha$.

Proof. The assumption $F\in\Lambda_\alpha$ implies the series (8.1) converges uniformly at a rate $O(N^{-\alpha}\log N)$. Using (8.4) & (8.5) it follows for any $\gamma\in(0,\alpha)$ that

$$\left|\sum_{n=1}^{N}\frac{\mu(n)\chi(n)}{n}-L^{-1}(1,\chi)\right|=O(N^{-\gamma}). \tag{8.7}$$

Now fix β real with $\beta>1-\alpha$. If we prove (8.4) converges for $s=\beta$, then $L^{-1}(s,\chi)$ will be analytic for $\mathrm{Re}\,s>\beta$. To this end choose γ so that $0<\gamma<\alpha$ and $\gamma+\beta>1$. Summing by parts we have

$$\begin{aligned}\sum_{n=1}^{N}\frac{\mu(n)\chi(n)}{n^\beta}&=\sum_{n=1}^{N}\left(\sum_{k=1}^{n}\frac{\mu(k)\chi(k)}{k}-L^{-1}(1,\chi)\right)(n^{1-\beta}-(n+1)^{1-\beta})\\&\quad+\left(\sum_{k=1}^{N}\frac{\mu(k)\chi(k)}{k}-L^{-1}(1,\chi)\right)(N+1)^{1-\beta}.\end{aligned} \tag{8.8}$$

The summands of the series on the right are $O(n^{-(\beta+\gamma)})$ while the extra term is $O(N^{1-(\beta+\gamma)})$. Thus, (8.4) converges for $s=\beta$, and the proposition obtains.

Define $F(s,x)$ for $\mathrm{Re}\,s>1$, $x\in\mathbb{R}$ by the series

$$F(s,x)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}e(nx) \tag{8.9}$$

By Davenport's estimate the series converges even for $\mathrm{Re}\,s=1$, uniformly in x, and a significant improvement in Davenport's estimate would imply the same for $\mathrm{Re}\,s>\frac{1}{2}$. We do not know if such an improvement is possible, but we will make one conditional remark about (8.9).

If $\frac{1}{2}<\beta<1$, and if $F(\beta,\cdot)$ is continuous, set $\alpha=1-\beta$, and notice that, but for a constant factor,

$$\psi_\alpha * F(\beta,\cdot)=F(1,\cdot)=F(\cdot), \tag{8.10}$$

so that $F\in\Lambda_\alpha$. In what follows we shall observe that conditioned on the Riemann Hypothesis for L-series, the series (8.9) converges for each rational x, as soon as $\mathrm{Re}\,s>\frac{1}{2}$.

If $q\geq 1$, define $e_q(y)=e(y/q)$. We denote by $\Gamma(q)$ the set of Dirichlet characters mod q. We have $|\Gamma(q)|=\phi(q)$.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

Now suppose $x = b/q$ with $(b, q) = 1$. We sum formally in (8.9):

$$F\left(s, \frac{b}{q}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} e_q(nb)$$

$$= \sum_{d|q} \sum_{\substack{l=1 \\ (l, q/d)=1}}^{\infty} \frac{\mu(dl)}{d^s l^s} e_{q/d}(lb) \tag{8.11}$$

If $(l, d) > 1$, then $\mu(ld) = 0$, and otherwise $\mu(ld) = \mu(l)\mu(d)$. Thus we may replace $(l, q/d) = 1$ by $(l, q) = 1$ in the series on the right to find

$$F\left(s, \frac{b}{q}\right) = \sum_{d|q} \frac{\mu(d)}{d^s} \sum_{\substack{l=1 \\ (l,q)=1}}^{\infty} \frac{\mu(l)}{l^s} e_{q/d}(lb) \tag{8.12}$$

Working with the inner sum in (8.12) we find

$$\sum_{\substack{l=1 \\ (l,q)=1}}^{\infty} \frac{\mu(l)}{l^s} e_{q/d}(lb) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q-1} \sum_{l \equiv a(q)}^{\infty} \frac{\mu(l)}{l^s} e_{q/d}(ab)$$

$$= \sum_{\substack{a=1 \\ (a,q)=1}}^{q-1} \frac{1}{\phi(q)} \sum_{\chi \in \Gamma(q)} \sum_{l=1}^{\infty} \frac{\mu(l)\chi(l)\bar{\chi}(a)}{l^s} e_{q/d}(ab)$$

$$= \sum_{\substack{a=1 \\ (a,q)=1}}^{q-1} \frac{1}{\phi(q)} \sum_{\chi \in \Gamma(q)} \frac{\bar{\chi}(a) e_q(abd)}{L(s, \chi)}$$

$$= \frac{1}{\phi(q)} \sum_{\chi \in \Gamma(q)} \frac{\tau_{bd}(\bar{\chi})}{L(s, \chi)}. \tag{8.13}$$

Substitution in (8.12) yields formally

$$F\left(s, \frac{b}{q}\right) = \frac{1}{\phi(q)} \sum_{\chi \in \Gamma(q)} \frac{1}{L(s, \chi)} \left(\sum_{d|q} \frac{\mu(d)\tau_{bd}(\bar{\chi})}{d^s} \right). \tag{8.14}$$

Assuming the Riemann Hypothesis for L-series, the right side of (8.14) is analytic in s for Re $s > \frac{1}{2}$ and moreover the series which were summed in (8.13) are actually convergent. It follows that (8.14) is valid. We have proved:

(8.15) PROPOSITION. *If the Riemann Hypothesis for L-series is correct, the series* (8.9) *is convergent, with sum given by* (8.14), *for each rational x and complex s with* Re $s > \frac{1}{2}$.

Remark. If $q = p$ is prime, then (8.14) reduces to

$$F\left(s, \frac{b}{p}\right) = \left(\frac{1}{p-1} \sum_{\chi \in \Gamma(p)} \frac{\tau_b(\bar{\chi})}{L(s, \chi)} \right) - \frac{1}{p^s L(s, \chi_0)},$$

where χ_0 is the principal character.

RREFERENCES

[1] N. Bary. *A Treatise on Trigonometric Series*, Vol. II. Oxford, Pergamon Press, 1964.

[2] J. W. S. Cassels & A. Frohlich, Eds. *Algebraic Number Theory*. Washington, D.C., Thompson Book Co., 1967.

[3] C. Chevalley. Deux theoremes d'Arithmetique. *J. Math. Soc. of Japan*, **3** (1951), 36-44.

https://doi.org/10.1017/S0143385700003606 Published online by Cambridge University Press

[4] H. Davenport. On some infinite series involving arithmetical functions. *The Quarterly Journal of Mathematics*, **8** (1937), 8-13.
[5] H. Davenport. On some infinite series involving arithmetical functions, (II). *The Quarterly Journal of Mathematics*, **8** (1937), 313-320.
[6] Y. Katznelson. Ergodic automorphisms on $\mathbb{T}^n$ are Bernoulli shifts. *Israel J. Math.* **10** (1971), 186-195.
[7] E. Landau. *Handbuch über die Lehre von der Verteilung der Prinzahlen.* Leipzig, Teubner, 1909.
[8] D. Lind, Dynamical properties of quasihyperbolic toral automorphisms. *Ergod. Th. & Dynam. Sys.* **2** (1982), 49-86.
[9] A. N. Livšic. Homology properties of Y systems. *Math. Notes*, **10** (1971), 758-763.
[10] A. N. Livšic. Cohomology of dynamical systems. *Math. U.S.S.R. Izvestija*, **6** (1972), 1278-1301.
[11] B. Marcus. A note on periodic points for ergodic toral automorphisms. *Monatsh. Math.* **89** (1980), 121-129.
[12] E. M. Stein. *Singular Integrals and Differentiability Properties of Functions.* Princeton, Princeton University Press, 1970.
[13] E. M. Stein & G. Weiss. *Introduction to Fourier Analysis on Euclidean Space.* Princeton, Princeton University Press, 1971.
[14] E. Weiss. *Algebraic Number Theory.* New York, McGraw-Hill, 1963.
[15] H. Weyl. Über die Gleichverteilung von Zahlen mod Eins. *Math. Ann.* **77** (1916), 313-352.
[16] A. Zygmund. *Trigonometric Series*, Vols. I, II. Cambridge, Cambridge University Press, 1959.