ACTA ARITHMETICA
LII (1989)

Density modulo 1 in local fields

by

DANIEL BEREND (Beer-Sheva)

1. Introduction. It follows from a result of Koksma that, if $(t_k)_{k=1}^{\infty}$ is sequence of real numbers satisfying some mild condition, for example $|t_i - t_j| \geqslant \delta$ for $i \neq j$, where δ is a certain positive number, then $(t_k \alpha)_{k=1}^{\infty}$ is dense modulo 1 for almost every $\alpha \in \boldsymbol{R}$ (cf. [8]).

Characterizing the set of exceptional α's is, however, usually a more formidable problem. One instance where this problem was solved is the following. Call non-zero numbers λ, μ *rationally independent* if $\lambda^m = \mu^n$ for integers m, n implies $m = n = 0$. A multiplicative semigroup is *multi-parameter* if it contains two rationally independent numbers. Using this terminology, we can state a result of Furstenberg [5, Th. IV.1] in the following form.

THEOREM A. *Let S be a multi-parameter semigroup of integers. Then $S\alpha$ is dense modulo* 1 *for any irrational* α.

Now let K be a real algebraic number field. Denote by K^* the multiplicative group of K. For $A \subseteq K$, let $\boldsymbol{Q}(A)$ be the subfield of K generated by A. A generalization of Theorem A is

THEOREM B [4, Th. 2.1]. *Let K be a real algebraic number field and S a multi-parameter subsemigroup of $K^* \cap [-1, 1]^C$ with $\boldsymbol{Q}(S) = K$. Then $S\alpha$ is dense modulo* 1 *for every $\alpha \notin K$. If, moreover, S is not contained in the semigroup of Pisot or Salem numbers of maximal degree in K, then $S\alpha$ is dense modulo* 1 *for every* $\alpha \neq 0$.

An analogue of Theorem B for multiplicative semigroups lying in the field $\boldsymbol{Q}_p$ of p-adic numbers was also obtained in [4].

Our main theme is examining to what extent the aforementioned results generalize to other local fields. Thus $\boldsymbol{R}$, for example, is replaced by $\boldsymbol{C}$; we are given a subsemigroup S of K^*, where K is a complex algebraic number field, and want to find out whether or not $S\alpha$ is dense modulo $\boldsymbol{Z}[i]$ for every $\alpha \neq 0$ (or, alternatively for every $\alpha \notin K$). Theorem 2.1 provides sufficient conditions for S to possess this property. Theorem 2.1′ is of a very similar nature; here $\boldsymbol{Z}[i]$ is replaced by an arbitrary lattice in $\boldsymbol{C}$, spanned by two numbers belonging to a certain complex quadratic extension of $\boldsymbol{Q}$. Theorem 2.2 is an analogue of Theorem 2.1′ for semigroups lying in finite extensions of $\boldsymbol{Q}_p$. It turns out, similarly to the special cases studied in [4], that the conditions in our theorems are quite mild, so that "most" semigroups have the property in question.

Section 3 deals with semigroups lying in local fields of finite characteristic. Different phenomena are encountered here, and already in the simplest cases semigroups satisfying the property in question must be quite large (see Proposition 3.1 *infra*).

In Section 4 we study the question to what extent the conditions on S, assumed in our theorems, are actually necessary. Some of these are shown to be so, but we also give examples of semigroups having the required property, yet not satisfying the conditions in question.

Section 5 is devoted to the proof of Theorem 2.2. The proofs of Theorems 2.1′ and 2.2 do not differ in principle, but the latter is technically more complicated, as extensions of an arbitrary degree have to be considered.

I am grateful to Andrew Pollington for many discussions related to the contents of this paper.

2. Semigroups whose dilations are dense modulo 1. A set $A \subseteq \boldsymbol{C}$ is *dense modulo* 1 (or, alternatively, *dense modulo* $\boldsymbol{Z}[i]$) if for every $z \in \boldsymbol{C}$ and $\varepsilon > 0$ there exist $a \in A$ and $g \in \boldsymbol{Z}[i]$ such that $|a-(g+z)| < \varepsilon$. We are looking for the conditions under which the properties to be defined now, and versions thereof in other settings, hold.

DEFINITION 2.1. Let K be a complex algebraic number field and S a subsemigroup of its multiplicative group K^* with $\boldsymbol{Q}(S) = K$. S is an *almost* DM_1 *semigroup* (resp. a DM_1 *semigroup*) if $S\alpha$ is dense modulo 1 for every $\alpha \notin K$ (resp. for every $\alpha \neq 0$). (DM_1 – Dense Modulo 1.)

Denote $\boldsymbol{C}_{\leqslant 1} = \{z \in \boldsymbol{C}\colon |z| \leqslant 1\}$. A complex number λ is called a *complex Pisot or Salem number* if λ is an algebraic integer, $\lambda \notin \boldsymbol{C}_{\leqslant 1}$, and all the other conjugates of λ, except for $\bar{\lambda}$, lie in $\boldsymbol{C}_{\leqslant 1}$ (compare with [10, p. 25, 34, 113]). Let K be a complex algebraic number field. Put $m = [K:\boldsymbol{Q}]$, and let $\theta_1, \theta_2, \ldots, \theta_m$ be the embeddings of K in $\boldsymbol{C}$, θ_1 being the identity and θ_2 – complex conjugation. We denote by $\mathrm{PS}(K)$ the subset of K consisting of all algebraic integers $\lambda \in K$ such that $\theta_i(\lambda) \in \boldsymbol{C}_{\leqslant 1}$ for $3 \leqslant i \leqslant m$. Thus, $\mathrm{PS}(K)$ contains all roots of unity lying in K and some, but not all, Pisot or Salem numbers belonging to the field.

LEMMA 2.1. $\mathrm{PS}(K)$ *is a multiplicative semigroup.*

The proof is straightforward (compare with [10, p. 33]).

For a multiplicative semigroup $S \subseteq K^*$ and $k \in \boldsymbol{N}$ denote by S^k the subsemigroup $\{s^k\colon s \in S\}$.

THEOREM 2.1. *Let K be a complex algebraic number field and $S \subseteq K^*$ a multiplicative semigroup with $\boldsymbol{Q}(S) = K$. Assume that:*

(i) *S is multi-parameter,*

(ii) *$S \nsubseteq \boldsymbol{C}_{\leqslant 1}$,*

(iii) *$\boldsymbol{Q}(S^l) \supseteq \boldsymbol{Q}(i)$ for every positive integer l.*

Then S is an almost DM_1 semigroup.

If, moreover,

(iv) *$S \nsubseteq \mathrm{PS}(K)$,*

then S is a DM_1 semigroup.

We now proceed to a more general setup. A set $\Lambda \subseteq \boldsymbol{C}$ is called a *lattice* if it is of the form

$$\Lambda = \{mu+nv\colon\ m, n \in \boldsymbol{Z}\}$$

where $u, v \in \boldsymbol{C}$ are linearly independent over $\boldsymbol{R}$. Given a subfield F of $\boldsymbol{C}$, Λ is an F*-lattice* if $u, v \in F$. A set $A \subseteq \boldsymbol{C}$ is *dense modulo* Λ if for every $z \in \boldsymbol{C}$ and $\varepsilon > 0$ there exist $a \in A$ and $g \in \Lambda$ with $|a-(g+z)| < \varepsilon$. Given a multiplicative subsemigroup S of K^* with $\boldsymbol{Q}(S) = K$, K being a complex algebraic number field, and a lattice Λ, S is an *almost* DM_Λ *semigroup* (resp. a DM_Λ *semigroup*) if $S\alpha$ is dense modulo Λ for every $\alpha \notin K$ (resp. for every $\alpha \neq 0$).

THEOREM 2.1′. *Let K be a complex algebraic number field, $S \subseteq K^*$ a multiplicative semigroup with $\boldsymbol{Q}(S) = K$, D a positive integer and Λ a $\boldsymbol{Q}(\sqrt{-D})$-lattice. Assume that:*

(i) *S is multi-parameter,*

(ii) *$S \nsubseteq \boldsymbol{C}_{\leqslant 1}$,*

(iii) *$\boldsymbol{Q}(S^l) \supseteq \boldsymbol{Q}(\sqrt{-D})$ for every positive integer l.*

Then S is an almost DM_Λ semigroup.

If, moreover,

(iv) *$S \nsubseteq \mathrm{PS}(K)$,*

then S is a DM_Λ semigroup.

Now we shall state a p-adic analogue. Denote by $\boldsymbol{Q}_p$ the field of p-adic numbers and by $\boldsymbol{Z}_p$ its subring of p-adic integers. Let $E_{\mathfrak{P}}$ be a finite extension of $\boldsymbol{Q}_p$, and put $d = [E_{\mathfrak{P}}:\boldsymbol{Q}_p]$. $E_{\mathfrak{P}}$ can be realized as follows (cf. [11, Th. 5.4]). There exists a number field E with $[E:\boldsymbol{Q}] = d$, containing a prime ideal $\mathfrak{P}$ lying above the ideal $p\boldsymbol{Z}$, such that the completion of E under the $\mathfrak{P}$-adic valuation is $E_{\mathfrak{P}}$ (hence the notation $E_{\mathfrak{P}}$).

Denote by $\boldsymbol{Z}[1/a]$ the ring obtained from $\boldsymbol{Z}$ by adjoining $1/a$ to it. Any $\xi \in \boldsymbol{Q}_p$ can be uniquely decomposed in the form $\xi = [\xi]+\{\xi\}$, where $[\xi] \in \boldsymbol{Z}_p$ and $\{\xi\} \in \boldsymbol{Z}[1/p] \cap [0, 1)$. Denote by $\boldsymbol{T}$ the circle group: $\boldsymbol{T} = \boldsymbol{R}/\boldsymbol{Z}$. Let $\boldsymbol{Z}(p^\infty)$ be the subgroup of $\boldsymbol{T}$ consisting of all torsion elements whose order is a power of p. Since $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ is algebraically isomorphic to $\boldsymbol{Z}(p^\infty)$, we may view $\{\xi\}$ as an element of the latter. A set $A \subseteq \boldsymbol{Q}_p^d$ is *dense modulo* 1 if the set $\{(\{x_1\}, \{x_2\}, \ldots, \{x_d\})\colon (x_1, x_2, \ldots, x_d) \in A\}$ is dense in $\boldsymbol{T}^d$. More generally, let

$\omega_1, \omega_2, \ldots, \omega_d$ be an arbitrary fixed basis of $E_{\mathfrak{P}}$ over Q_p. Denote this (ordered) basis by Λ. Correspond to any $x \in E_{\mathfrak{P}}$ its vector of coordinates $(x_1, x_2, \ldots, x_d)$ with respect to the given basis. A set $A \subseteq E_{\mathfrak{P}}$ is *dense modulo* Λ if the set $\{(x_1, x_2, \ldots, x_d): x \in A\}$ is dense modulo 1. Let $K \subseteq E_{\mathfrak{P}}$ be a finite extension of Q. A semigroup $S \subseteq K^*$ with $Q(S) = K$ is an *almost* DM_Λ *semigroup* (resp. a DM_Λ *semigroup*) if $S\alpha$ is dense modulo Λ for every $\alpha \notin K$ (resp. for every $\alpha \neq 0$).

Denote by $|\cdot|_p$ the p-adic norm on Q_p, and also its extension to the algebraic closure $\bar{Q}_p$ of Q_p. Put $E_{\mathfrak{P}, \leq 1} = \{x \in E_{\mathfrak{P}}: |x|_p \leq 1\}$. A number $\lambda \in E_{\mathfrak{P}}$ is called a *Pisot–Salem–Chabauty number* if (i) λ is an algebraic integer over $Z[1/p]$, (ii) $\lambda \notin E_{\mathfrak{P}, \leq 1}$, (iii) all the conjugates of λ over Q in $\bar{Q}_p$, which are not conjugates of λ over Q_p, are of norm not exceeding 1, and (iv) for any embedding θ of $Q(\lambda)$ in C we have $|\theta(\lambda)| \leq 1$ (compare with [10, p. 65]). If $K \subseteq E_{\mathfrak{P}}$ is an extension of degree m of Q, let $\theta_1, \theta_2, \ldots, \theta_m$ be the embeddings of K in $\bar{Q}_p$, where $\theta_1, \theta_2, \ldots, \theta_d$ are the restrictions to K of embeddings of $E_{\mathfrak{P}}$ over Q_p in $\bar{Q}_p$, and $\theta'_1, \theta'_2, \ldots, \theta'_m$ – the embeddings of K in C. We denote by PSC(K) the subset of K consisting of all those numbers λ which are algebraic integers over $Z[1/p]$ and satisfy $|\theta_i(\lambda)|_p \leq 1$ for $d+1 \leq i \leq m$ and $|\theta'_i(\lambda)| \leq 1$ for $1 \leq i \leq m$.

THEOREM 2.2. *Let $\Lambda = \{\omega_1, \omega_2, \ldots, \omega_d\}$ be a basis of E over Q, $K \subseteq E_{\mathfrak{P}}$ a number field and $S \subseteq K^*$ a multiplicative semigroup with $Q(S) = K$. Assume that*

(i) *S is multi-parameter,*
(ii) *$S \nsubseteq E_{\mathfrak{P} \leq 1}$,*
(iii) *$Q(S^l) \supseteq E$ for every positive integer l.*

Then S is an almost DM_Λ semigroup.

If, moreover,
(iv) *$S \nsubseteq$ PSC(K),*

then S is a DM_Λ semigroup.

We shall prove this theorem in Section 5. The proof of Theorem 2.1′ is analogous (and simpler), and will thus be omitted.

3. Semigroups in local fields with finite characteristic. Do the results of the preceding section admit analogues in other local fields? We shall see in this section that the situation in local fields of finite characteristic is quite different.

Let F be a finite field, say $F = \mathrm{GF}(p^e)$. $F[x]$ denotes the ring of polynomials (in one indeterminate) over F, $F(x)$ – the field of rational functions, $F[[x]]$ – the ring $\{\sum_{k=0}^{\infty} a_k x^k: a_k \in F, k = 0, 1, \ldots\}$ and $F((x))$ – the field of formal power series, namely $\{\sum_{k=n}^{\infty} a_k x^k: n \in Z, a_k \in F, k = n, n+1, \ldots\}$.

The topology on $F((x))$ is given via the norm $\|\cdot\|$ defined by

$$\|f\| = c^n, \quad (f = \sum_{k=n}^{\infty} a_k x^k, a_n \neq 0)$$

where $0 < c < 1$.

Let $H = \{\sum_{k=-\infty}^{\infty} a_k x^k: a_k \in F, k = 0, \pm 1, \ldots\}$. Under formal addition of power series H forms an abelian group. We may view the additive groups of both $F((x))$ and $F((x^{-1}))$ as subgroups of H. Each set $D \subseteq Z$ gives rise to an endomorphism π_D of H defined by

$$\pi_D\left(\sum_{k=-\infty}^{\infty} a_k x^k\right) = \sum_{k \in D} a_k x^k.$$

Thus, for example, $\pi_N(F((x))) = xF[[x]]$ and $\pi_N(F((x^{-1}))) = xF[x]$.

Let $A \subseteq F((x^{-1}))$. A *is dense modulo* $F[x]$ if the set $\pi_{-N}(A)$ is dense in $x^{-1}F[[x^{-1}]]$. In other words, A is dense modulo $F[x]$ if for any $r \in N$ and $b_{-1}, b_{-2}, \ldots, b_{-r} \in F$ there exists a power series $\sum_{k=-r}^{\infty} a_k x^k \in A$ with $a_{-k} = b_{-k}$ for $1 \leq k \leq r$. A is *dense modulo* $F[[x^{-1}]]$ if the set $\pi_N(A)$, considered as a subset of $xF[[x]]$, is dense in it (or, equivalently, if for any $r \in N$ and $b_1, b_2, \ldots, b_r \in F$ there exists a power series $\sum_{k=-\infty}^{r} a_k x^k \in A$ with $a_k = b_k$ for $1 \leq k \leq r$).

We shall now see that these two notions of density modulo a subring of $F((x^{-1}))$ are analogous to those of density modulo 1 in R and in Q_p, respectively. In fact, in the first case the Dedekind domain Z is replaced by $F[x]$, the global field Q – by $F(x)$, and the local field R – by $F((x^{-1}))$. When Q is endowed with the spot $|\cdot|_\infty$, that is the equivalence class of the usual absolute value, its completion is R; the completion of $F(x)$ under the spot $|\cdot|_\infty$, defined by

$$|f|_\infty = c^{-(\deg f_1 - \deg f_2)}, \quad f = f_1/f_2, f_1, f_2 \in F[x]$$

where $0 < c < 1$, is $F((x^{-1}))$. (For more details regarding global and local fields, spots, etc., see, for example, [12].) To explain the second asserted analogy, let us interchange the indeterminates x^{-1} and x. Thus, a set $A \subseteq F((x))$ is dense modulo $F[[x]]$ if $\pi_{-N}(A)$ is dense in $x^{-1}F[[x^{-1}]]$. Again, Z is replaced by $F[x]$ and Q by $F(x)$, but this time Q is equipped with the p-adic spot $|\cdot|_p$ and $F(x)$ with the x-adic spot $|\cdot|_x$, defined as follows. If $f(x) = x^n f_1(x)/f_2(x)$, where $n \in Z$ and f_1, f_2 are polynomials neither of which is divisible by x, then $|f|_x = c^n$, where $0 < c < 1$. The completion of Q at $|\cdot|_p$ is Q_p; the completion of $F(x)$ at $|\cdot|_x$ is $F((x))$.

We note that one can easily define the notion of density modulo a more general lattice, as done in the cases of C and of $\mathfrak{P}$-adic fields. However, these generalizations are unnecessary for our purposes.

Let $K \subseteq F((x^{-1}))$ be a finite extension of $F(x)$. A multiplicative semigroup $S \subseteq K^*$ with $F(x)(S) = K$ is an *almost* $DM_{F[x]}$ *semigroup* (resp. a $DM_{F[x]}$ *semigroup*) if $S\alpha$ is dense modulo $F[x]$ for every $\alpha \notin K$ (resp. for every $\alpha \neq 0$). Almost $DM_{F[[x^{-1}]]}$ semigroups and $DM_{F[[x^{-1}]]}$ semigroups are analogously defined.

LEMMA 3.1. *Let S be a subsemigroup of K^* with $Q(S) = K$, where $K \subseteq F((x^{-1}))$ is a finite extension of $F(x)$. Then S is an almost $DM_{F[x]}$ semigroup (resp. a $DM_{F[x]}$ semigroup) iff it is an almost $DM_{F[[x^{-1}]]}$ semigroup (resp. a $DM_{F[[x^{-1}]]}$ semigroup).*

Employing the characterization of density of a set A modulo $F[x]$ and modulo $F[[x^{-1}]]$ in terms of the blocks of "digits" appearing in various elements of A, the lemma is easily proved.

The properties (i)–(iv) assumed in Theorems 2.1–2.2 admit analogues to the case at hand (for the definition and various properties of the analogues of Pisot numbers in formal power series fields see [1], [6], [7]). Similarly to the discussion in the next section, one can show that at least somewhat weaker conditions on S are necessary for it to be a $DM_{F[x]}$ semigroup (or almost such). To examine whether these conditions are necessary, we consider the simplest case, namely $K = F(x)$ and $S \subseteq F[x]$, corresponding to the one encountered in Theorem A. Our results in Section 2 would suggest that, provided S is multi-parameter, it is an almost $DM_{F[x]}$ semigroup. That this is not the case we see by

PROPOSITION 3.1. *If $S \subseteq F[x]$ is finitely generated, then it is not an almost $DM_{F[x]}$ semigroup.*

Before turning to the proof, we need some information concerning the action of polynomials on $F((x^{-1}))$. Let $P \in F[x]$ be a non-zero polynomial. P gives rise to an endomorphism on $F((x^{-1}))$, which we denote by P also, defined by

$$P(f(x)) = P(x)f(x), \quad f \in F((x^{-1})).$$

Since $F[x]$ is clearly a P-invariant set, P induces an endomorphism, again denoted by P, on the additive group of $x^{-1}F[[x^{-1}]]$. It is easy to see that P is surjective, whence it is measure preserving with respect to the Haar measure μ. (For the definition and properties of measure preserving transformations, both in general and in the special case of group endomorphisms, see, for example, [15]). Now suppose that P is actually a polynomial in x^{p^t} for a certain positive integer t, say $P(x) = Q(x^{p^t})$ for some $Q \in F[x]$. Set

$q = p^t$. Consider the set

$$(3.1) \qquad A = \Big\{\sum_{k=-\infty}^{-1} a_k x^k:\ a_{-jq} = 0,\ j = 1, 2, \ldots\Big\}.$$

Evidently, A forms a closed P-invariant subgroup of $x^{-1}F[[x^{-1}]]$ and $\mu(A) = 0$.

Proof of Proposition 3.1. Let S be the semigroup generated by the (non-zero) polynomials $P_1, P_2, \ldots, P_l \in F[x]$. Select a positive integer t, and define A as in (3.1). A is P_i^q-invariant for $1 \leqslant i \leqslant l$. Put

$$A_0 = \bigcup_{j_1, j_2, \ldots, j_l = 0}^{q-1} P_1^{-j_1} P_2^{-j_2} \ldots P_l^{-j_l}(A).$$

A_0 is a union of q^l closed sets of zero measure, and hence it possesses the same properties itself. Clearly, A_0 is P_i-invariant for $1 \leqslant i \leqslant l$. It follows in particular that $S\alpha$ is not dense modulo $F[x]$ for every $\alpha \in A_0$. Since A_0 is uncountable, this proves the proposition.

Remark 3.1. Taking in the proof larger and larger t's (not just $t = 1$, which suffices for the proof), we observe that, moreover, although the set of α's for which $S\alpha$ is not dense modulo $F[x]$ is "small" in terms of Haar measure (unless $S \subseteq F$), it is "large" in terms of Hausdorff dimension.

4. Examples. In this section we shall try to find out to what extent the conditions (i)–(iv) in Theorems 2.1–2.2 are necessary for the conclusions of those theorems to hold. For the sake of simplicity we shall emphasize the situation with respect to Theorem 2.1.

Condition (i): Let us recall first why this condition is necessary in Theorem B (for more details see [4]). It was proved by de Mathan [9] and Pollington [13] that, given a *lacunary sequence* $(t_k)_{k=1}^{\infty}$ of positive numbers, i.e., a sequence satisfying $t_{k+1}/t_k \geqslant q > 1$ for each k, there exists a set of Hausdorff dimension 1 of α's for which 0 is not a limit point modulo 1 of the sequence $(t_k\alpha)_{k=1}^{\infty}$. From this one can infer that the condition for S to be multi-parameter is necessary in Theorem B. Now call a sequence $(z_k)_{k=1}^{\infty}$ in C *lacunary* if $|z_{k+1}/z_k| \geqslant q > 1$ for each k. It is readily observed that, provided q is sufficiently large, there exist uncountably many dilations of $(z_k)_{k=1}^{\infty}$ which are not dense modulo 1. We get accordingly

EXAMPLE 4.1. The semigroup $S = \{(10+i)^n:\ n \in \boldsymbol{Z}\} \subseteq \boldsymbol{Q}(i)^*$ satisfies conditions (ii)–(iv) of Theorem 2.1, but is not even an almost DM_1 semigroup.

Thus, condition (i) is not superfluous in Theorem 2.1. However, we are unable to show it is necessary. In fact, in [14] Pollington could only show that, if z is an arbitrary complex number, then the set of α's for which the sequence $(z^n\alpha)_{n=1}^{\infty}$ is not uniformly distributed modulo 1 is "large". (Moreover, to prove that the condition in question is necessary, one would have to show that sets of the form $\{\omega^k\zeta^n: k, n \in \boldsymbol{Z}\}$, ω being a root of unity and ζ an arbitrary algebraic number, have non-trivial dilations which are not dense modulo 1.) In the p-adic case an analogue of the result of de Mathan [9] and Pollington [13] is not available even for lacunary sequences in $\boldsymbol{Q}_2$.

Condition (ii): This condition is obviously necessary in both Theorems 2.1′ and 2.2.

Condition (iii): This condition is not necessary already in Theorem 2.1. Furthermore, neither of the weaker conditions

(iii′) $S^l \nsubseteq \boldsymbol{R}$ for every positive integer l,

and

(iii″) $\boldsymbol{Q}(S) \supseteq \boldsymbol{Q}(i)$,

is necessary.

EXAMPLE 4.2. Let ω be a primitive cubic root of unity and $S = \boldsymbol{Q}^* \cup \boldsymbol{Q}^*\omega \cup \boldsymbol{Q}^*\omega^2$. Then $S^3 \subseteq \boldsymbol{R}$ and $\boldsymbol{Q}(S) = \boldsymbol{Q}(i\sqrt{3}) \nsupseteq \boldsymbol{Q}(i)$, so that S satisfies neither (iii′) nor (iii″), yet S is a DM_1 semigroup.

On the other hand, the condition in question cannot be omitted nor even be relaxed to (iii″).

EXAMPLE 4.3. The semigroup $S = \boldsymbol{Q}^* \cup \boldsymbol{Q}^* i$ satisfies conditions (i), (ii) and (iv) of Theorem 2.1, and also (iii″), yet it is not even an almost DM_1 semigroup.

We do not know whether or not (iii) may be replaced by (iii′).

Condition (iv): With respect to this condition we have

PROPOSITION 4.1. *Condition* (iv) *is necessary in Theorems* 2.1–2.2.

The key role in the proof is played by the following two lemmas, of which only the latter will be proved.

LEMMA 4.1. *Let K be a complex algebraic number field. Then for every $\varepsilon > 0$ there exist infinitely many $\gamma \in K$ such that* $\mathrm{Re}(\mathrm{PS}(K)\gamma) \subseteq (-\varepsilon, \varepsilon) \pmod 1$ (*where* $\mathrm{Re}(A)$ *denotes the projection on* $\boldsymbol{R}$ *of a set* $A \subseteq \boldsymbol{C}$).

LEMMA 4.2. *Let $E_{\mathfrak{P}}$ be an extension of degree d of $\boldsymbol{Q}_p$ and $K \subseteq E_{\mathfrak{P}}$ an algebraic number field with $\boldsymbol{Q}_p(K) = E_{\mathfrak{P}}$. Suppose that $\eta_1 = 1, \eta_2, \ldots, \eta_d$ is a basis of $E_{\mathfrak{P}}$ over $\boldsymbol{Q}_p$ satisfying $\mathrm{tr}_{E_{\mathfrak{P}}/\boldsymbol{Q}_p}(\eta_i) = 0$ for $2 \leqslant i \leqslant d$. Let $\pi_1\colon E_{\mathfrak{P}} \to \boldsymbol{Q}_p$ be the homomorphism taking any $x \in E_{\mathfrak{P}}$ to the coefficient of η_1 in the representation of x with respect to the given basis. Then there exist infinitely many $\gamma \in K$ such that $\pi_1(\mathrm{PSC}(K)\gamma) \subseteq (-\varepsilon, \varepsilon) \pmod{\boldsymbol{Z}_p}$.*

Proof. Take $x \in \mathrm{PSC}(K)$ with $|x|_p > 1$. (We do not need to show there exist such x's, as otherwise $\mathrm{PSC}(K)$ is finite so that the lemma is trivial.) Let $\theta_1, \theta_2, \ldots, \theta_m$ and $\theta'_1, \theta'_2, \ldots, \theta'_m$ be as before Theorem 2.2. Take an increasing sequence $(n_k)_{k=1}^{\infty}$ such that for each $d+1 \leqslant i \leqslant m$ the sequence $(\theta_i(x^{n_k}))_{k=1}^{\infty}$ converges in the normal closure of $E_{\mathfrak{P}}/\boldsymbol{Q}_p$ and for each $1 \leqslant i \leqslant m$ the sequence $(\theta'_i(x^{n_k}))_{k=1}^{\infty}$ converges in $\boldsymbol{C}$. Set $\beta = x^{n_{k+1}} - x^{n_k}$ for some k. We can make all the numbers $|\theta_i(\beta)|_p$, $d+1 \leqslant i \leqslant m$, and $|\theta'_i(\beta)|$, $1 \leqslant i \leqslant m$, arbitrarily small by choosing k sufficiently large. Let $\alpha \in \mathrm{PSC}(K)$. Expand $\alpha\beta$ with respect to the given basis of $E_{\mathfrak{P}}$ over $\boldsymbol{Q}_p$:

$$\alpha\beta = a_1\eta_1 + a_2\eta_2 + \ldots + a_d\eta_d, \qquad (a_1, a_2, \ldots, a_d \in \boldsymbol{Q}_p).$$

We shall show that $\{da_1\}$ is restricted to a small neighbourhood of 0 in $\boldsymbol{T}$ independently of α. In fact, according to our assumptions concerning the η_i's we have

$$\mathrm{tr}_{E_{\mathfrak{P}}/\boldsymbol{Q}_p}(\alpha\beta) = da_1.$$

On the other hand

$$\mathrm{tr}_{E_{\mathfrak{P}}/\boldsymbol{Q}_p}(\alpha\beta) = \sum_{i=1}^{d} \theta_i(\alpha\beta) = \mathrm{tr}_{K/\boldsymbol{Q}}(\alpha\beta) - \sum_{i=d+1}^{m} \theta_i(\alpha)\theta_i(\beta). \tag{4.1}$$

The first term on the right-hand side of (4.1) is an ordinary rational number. Writing

$$\mathrm{tr}_{K/\boldsymbol{Q}}(\alpha\beta) = \sum_{i=1}^{m} \theta'_i(\alpha)\theta'_i(\beta)$$

we observe that, considered as a real number, it can be made arbitrarily close to 0 by selecting k sufficiently large. The second term on the right-hand side of (4.1) belongs to $\boldsymbol{Q}_p$ and, since it can be also made arbitrarily close to 0 by taking k large enough, it may be assumed in particular to lie in $\boldsymbol{Z}_p$. Putting $\gamma = d\beta$ we now see that, in the expansion of $\alpha\gamma$ with respect to the given basis, the coefficient of η_1 taken modulo $\boldsymbol{Z}_p$ can be confined to an arbitrarily small neighbourhood of 0, independently of α. This completes the proof.

Proof of Proposition 4.1. We shall deal only with the p-adic case. Let us show first that we can pass from the given basis $\omega_1, \omega_2, \ldots, \omega_d$ to a basis $\eta_1, \eta_2, \ldots, \eta_d$ satisfying the conditions of Lemma 4.2 by means of a rational transition matrix. In fact, we may certainly assume that $\omega_1 = 1$, and then, setting

$$\eta_i = \omega_i - \frac{1}{d}\mathrm{tr}_{E/\boldsymbol{Q}}(\omega_i), \qquad i = 2, 3, \ldots, d$$

we arrive at a basis $\eta_1, \eta_2, \ldots, \eta_d$ possessing the required properties. Let

$R = (r_{ij})_{i,j=1}^{d} \in M_d(\mathbf{Q})$ be the transition matrix between the two bases, namely

$$\omega_i = r_{i1}\eta_1 + r_{i2}\eta_2 + \ldots + r_{id}\eta_d, \quad i = 1, 2, \ldots, d.$$

Denote by $(x_1, x_2, \ldots, x_d)$ (resp. $(x_1', x_2', \ldots, x_d')$) the vector of coordinates of $x \in E_{\mathfrak{P}}$ with respect to the basis $\omega_1, \omega_2, \ldots, \omega_d$ (resp. $\eta_1, \eta_2, \ldots, \eta_d$). We have $(x_1', x_2', \ldots, x_d') = (x_1, x_2, \ldots, x_d)R$ for every $x \in E_{\mathfrak{P}}$. For $\varepsilon > 0$ put

$$A_\varepsilon = \{x \in E_{\mathfrak{P}}: x_1' \in (-\varepsilon, \varepsilon) \pmod{\mathbf{Z}_p}\}.$$

In view of Lemma 4.2, for any $\varepsilon > 0$ there exist infinitely many numbers $\gamma \in E_{\mathfrak{P}}$ for which $\mathrm{PSC}(K)\gamma \subseteq A$. It suffices therefore to show that, if ε is sufficiently small, then the set

$$B_\varepsilon = \{(x_1, x_2, \ldots, x_d): x \in A_\varepsilon\} \subseteq \mathbf{Q}_p^d$$

is not dense modulo 1. Select a positive integer q such that $qR \in M_d(\mathbf{Z})$. Let $\pi: \mathbf{Q}_p \to \mathbf{T}$ denote the homomorphism given by $\pi(\xi) = \{\xi\}$ for $\xi \in \mathbf{Q}_p$. According to our assumptions, if $\varepsilon < 1/2q$, then the set $B_\varepsilon \cdot qR$ is not dense modulo 1, and consequently $\pi(B_\varepsilon)\cdot qR$ is not dense in the d-dimensional torus $\mathbf{T}^d$. Since qR forms a continuous epimorphism of $\mathbf{T}^d$, $\pi(B_\varepsilon)$ is not dense in $\mathbf{T}^d$ either. This proves the proposition.

5. Proof of Theorem 2.2. Let S be a semigroup satisfying conditions (i)–(iii). We have to show that if $S\alpha$ is not dense modulo Λ for some $\alpha \neq 0$, then $S \subseteq \mathrm{PSC}(K)$ and $\alpha \in K$. We shall concentrate on the features of the proof which are particular to our case, only briefly sketching those already appearing in [4].

Let $\varphi: E_{\mathfrak{P}} \to \mathbf{Q}_p^d$ denote the mapping taking each $x \in E_{\mathfrak{P}}$ to its vector of coordinates with respect to the basis $\omega_1, \omega_2, \ldots, \omega_d$. φ forms an isomorphism between the two $\mathbf{Q}_p$-vector spaces. Hence the mapping $\psi: E_{\mathfrak{P}} \to M_d(\mathbf{Q}_p)$ given by

$$(\psi(a))(\varphi(x)) = \varphi(ax), \quad a, x \in E_{\mathfrak{P}}$$

is well-defined. We may write $\psi(a) = (\psi_{i,j}(a))_{i,j=1}^{d}$, $a \in E_{\mathfrak{P}}$, for suitable $\mathbf{Q}_p$-linear transformations $\psi_{i,j}: E_{\mathfrak{P}} \to \mathbf{Q}_p$.

Given any positive integer q, the mappings φ and ψ admit q-fold extensions φ_q and ψ_q, defined as follows. If $u = (u_1, u_2, \ldots, u_q)^t \in E_{\mathfrak{P}}^q$, where $u_i = \sum_{j=1}^{d} u_{ij}\omega_j$ for $1 \leqslant i \leqslant q$, then

$$\varphi_q(u) = (u_{11}, u_{21}, \ldots, u_{q1}, \ldots, u_{1d}, u_{2d}, \ldots, u_{qd})^t \in \mathbf{Q}_p^{dq}.$$

φ_q forms an isomorphism between the $\mathbf{Q}_p$-vector spaces $E_{\mathfrak{P}}^q$ and $\mathbf{Q}_p^{dq}$. The mapping ψ_q is defined via

$$(\psi_q(A))(\varphi_q(u)) = \varphi_q(Au), \quad A \in M_q(E_{\mathfrak{P}}),\ u \in \mathbf{Q}_p^q,$$

and is readily verified to form a $\mathbf{Q}_p$-isomorphism between $M_q(E_{\mathfrak{P}})$ and a certain $\mathbf{Q}_p$-subalgebra of $M_{dq}(\mathbf{Q}_p)$. Extending the mappings $\psi_{i,j}$, $1 \leqslant i, j \leqslant d$, to $M_q(E_{\mathfrak{P}})$ by letting them act on matrices entrywise, we get

$$\psi_q(A) = \begin{bmatrix} \psi_{1,1}(A) & \ldots & \psi_{1,d}(A) \\ \ldots & \ldots & \ldots \\ \psi_{d,1}(A) & \ldots & \psi_{d,d}(A) \end{bmatrix}, \quad A \in M_q(E_{\mathfrak{P}}).$$

Restricting ψ_q to $M_q(E)$ we obtain a $\mathbf{Q}$-isomorphism between $M_q(E)$ and a $\mathbf{Q}$-subalgebra of $M_{dq}(\mathbf{Q})$. We shall subsequently denote φ_q and ψ_q by φ and ψ, respectively.

If $a \in E_{\mathfrak{P}}$ then the minimal polynomial of the matrix $\psi(a)$ coincides with the minimal polynomial of a over $\mathbf{Q}_p$. Consequently, the eigenvalues of $\psi(a)$ are a and all its conjugates over $\mathbf{Q}_p$ in the normal closure of the extension $E_{\mathfrak{P}}/\mathbf{Q}_p$. Fix an arbitrary $a \in E_{\mathfrak{P}}$ of degree d over $\mathbf{Q}_p$, and let $v \in E_p^d$ be the eigenvector of $\psi(a)$ corresponding to the eigenvalue a. Evidently, $\psi(b)v = bv$ for every $b \in E_{\mathfrak{P}}$. The conjugates $v^{(1)} = v, v^{(2)}, \ldots, v^{(d)}$ of v over $\mathbf{Q}_p$ are all the eigenvectors of $\psi(a)$. Moreover, they form common eigenvectors of the whole algebra $\psi(E_{\mathfrak{P}})$. Requiring to begin with that $a \in E$, we may ensure that $v^{(1)} \in E^d$. In the following, given a vector y we shall denote by $y_1, y_2, \ldots$ its components. It may be assumed that $v_1^{(1)} = 1$.

Set $\underline{K} = \bigcap_{k=1}^{\infty} \mathbf{Q}(S^k)$. Select a positive integer l such that $\mathbf{Q}(S^l) = \underline{K}$, and put $\underline{S} = S^l$. Let $r = [\underline{K} : E]$. In the sequel, φ and ψ will usually stand for φ_r and ψ_r, respectively.

According to [3, Lemma 4.2] and by the choice of $\underline{S}$ we can find an $s_0 \in \underline{S}$ such that $\mathbf{Q}(s_0^n) = \underline{K}$ for every positive integer n. Let $f = x^r + c_{r-1}x^{r-1} + \ldots + c_0$ be the minimal polynomial of s_0 over E. Denote by τ the companion matrix of f:

$$\tau = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ -c_0 & -c_1 & -c_2 & \ldots & -c_{r-1} \end{bmatrix},$$

The vector $u = (1, s_0, s_0^2, \ldots, s_0^{r-1})^t$ forms an eigenvector of τ corresponding to the eigenvalue s_0. Its conjugates $u^{(1)} = u, u^{(2)}, \ldots, u^{(r)}$ over E are all the eigenvectors of τ, and the corresponding eigenvalues are all the conjugates of s_0 over E. Set $\sigma_0 = \psi(\tau)$.

Let $\varrho: \underline{K} \to M_r(E)$ denote the (unique) $\underline{K}$-isomorphism from $\underline{K}$ into $M_r(E)$ carrying s_0 to τ. The minimal polynomial of $\sigma_0 = \psi(\varrho(s_0))$ clearly coincides with the minimal polynomial of s_0 over $\mathbf{Q}$, whence it is also the characteristic polynomial of σ_0. It follows that the eigenvalues of σ_0 are s_0 and all its conjugates over $\mathbf{Q}$. We claim that the eigenvector of σ_0 corresponding to the eigenvalue s_0 is the vector w given by:

$$w = (v_1 u_1, v_1 u_2, \ldots, v_1 u_r, \ldots, v_d u_1, v_d u_2, \ldots, v_d u_r)^t.$$

That is, we have to show that

$$\sigma_0(w) = s_0 w. \tag{5.1}$$

In fact, let $1 \leqslant m \leqslant d$ and $1 \leqslant k \leqslant r$. Write $\tau = (\tau_{gh})_{g,h=1}^{r}$. Then

$$(\sigma_0(w))_{(m-1)r+k} = \sum_{i=1}^{d} \sum_{j=1}^{r} \psi_{m,i}(\tau_{kj})\, v_i u_j.$$

Since $\psi(\tau_{kj}) v = \tau_{kj} v$ for $1 \leqslant j \leqslant r$ we get

$$(\sigma_0(w))_{(m-1)r+k} = \sum_{j=1}^{r} \Big(\sum_{i=1}^{d} \psi_{m,i}(\tau_{kj}) v_i\Big) u_j = \sum_{j=1}^{r} (\psi(\tau_{kj}) v)_m u_j$$

$$= \sum_{j=1}^{r} \tau_{kj} v_m u_j = v_m (\tau u)_k = v_m \cdot s_0 u_k = s_0 w_{(m-1)r+k}$$

which implies (5.1).

Choose an $s_1 \in \underline{S}$ such that the subsemigroup $\underline{S}$ of $\underline{S}$, generated by s_0 and s_1, also satisfies conditions (i)–(iii) of the theorem. From our assumption it follows in particular that $\underline{S}\alpha$ is not dense modulo Λ. Let $\sigma_1 = \psi(\varrho(s_1))$. Denote by Σ the multiplicative subsemigroup of $M_{dr}(\mathbf{Q})$ generated by σ_0 and σ_1. Let $p_1, p_2, \ldots, p_h$ be all the primes dividing the denominator of some entry of either σ_0 or σ_1. We may assume that $p_1 = p$. Put $a = p_1 p_2 \ldots p_h$.

We now describe a certain compact abelian group which will play an important role in the proof (for a more detailed survey see [2, Sec. II.1]). Consider first (the additive group of) $\mathbf{R} \times \mathbf{Q}_{p_1} \times \ldots \times \mathbf{Q}_{p_h}$. Putting for convenience $p_0 = \infty$ and $\mathbf{Q}_\infty = \mathbf{R}$, we can write this group as $\prod_{j=0}^{h} \mathbf{Q}_{p_j}$. The set

$$H = \{(b, -b, \ldots, -b) \colon b \in \mathbf{Z}[1/a]\}$$

forms a discrete subgroup of $\prod_{j=0}^{h} \mathbf{Q}_{p_j}$. We denote by Ω_a the quotient group $\prod_{j=0}^{h} \mathbf{Q}_{p_j}/H$ and by π the projection of $\prod_{j=0}^{h} \mathbf{Q}_{p_j}$ on Ω_a. For any positive integer q, the q-fold product of π, mapping $\prod_{j=0}^{h} \mathbf{Q}_{p_j}^{q}$ onto Ω_a^q, is also denoted by π. One can show that Ω_a is compact.

Let us describe the rings of (continuous) endomorphisms of Ω_a and of

Ω_a^q. Any $c \in \mathbf{Z}[1/a]$ gives rise to an endomorphism θ_c of $\prod_{j=0}^{h} \mathbf{Q}_{p_j}$ defined by

$$\theta_c(x_0, x_1, \ldots, x_h) = (cx_0, cx_1, \ldots, cx_h), \quad (x_0, x_1, \ldots, x_h) \in \prod_{j=0}^{h} \mathbf{Q}_{p_j}.$$

Obviously, θ_c leaves H invariant, and therefore induces an endomorphism of Ω_a. It can be shown that all the endomorphisms of Ω_a are of this form. Thus the ring of endomorphisms of Ω_a^q is (isomorphic to) $M_q(\mathbf{Z}[1/a])$; the action of $C \in M_q(\mathbf{Z}[1/a])$ on $\prod_{j=0}^{h} \mathbf{Q}_{p_j}^{q}$ is given by

$$C(x_0, x_1, \ldots, x_h) = (Cx_0, Cx_1, \ldots, Cx_h), \quad (x_0, x_1, \ldots, x_h) \in \prod_{j=0}^{h} \mathbf{Q}_{p_j}^{q}.$$

We define a homomorphism $\pi_1\colon \Omega_a \to \mathbf{T}$ as follows. Given $y \in \Omega_a$, we pick a point $x = (x_0, x_1, \ldots, x_h) \in \prod_{j=0}^{h} \mathbf{Q}_{p_j}$ with $\pi(x) = y$ and put $\pi_1(y) = \sum_{j=0}^{h} \{x_j\}$. It is easy to check that π_1 is well-defined.

Set $t = (0, \varphi(\alpha u), 0, \ldots, 0) \in \prod_{j=0}^{h} \mathbf{Q}_{p_j}^{dr}$. For any $s \in \underline{S}$ we have

$$\psi(\varrho(s))(t) = (0, \varphi(s\alpha u), 0, \ldots, 0).$$

Recall that $\underline{S}\alpha$ is not dense modulo Λ, so that in particular the set $\overline{\pi_1 \pi(\Sigma t)}$ is not dense in $\mathbf{T}^{dr}$. Hence $\pi(\Sigma t)$ is not dense in Ω_a^{dr}. Put $B = \overline{\pi(\Sigma t)}$.

We claim that B may be assumed to be infinite. In fact, if $r > 1$, then certainly $\alpha u \notin E^r$, and hence $\varphi(\alpha u) \notin \mathbf{Q}^{dr}$, so that B must be infinite as in [4]. Assume therefore that $r = 1$. Employing similar reasoning we may assume also that $\alpha \in E$ and that $S \subseteq E$. Take an $s \in S$ with $|s|_p > 1$. The sequence $(s^n\alpha)_{n=1}^{\infty}$ is unbounded in $E_{\mathfrak{P}}$, and consequently the sequence $(\varphi(s^n\alpha))_{n=1}^{\infty}$ is unbounded in $\mathbf{Q}_p^d$. It follows that the set $\{\pi_1 \pi\varphi(s^n\alpha) \colon n \in \mathbf{N}\} \subseteq \mathbf{T}$ contains points of arbitrarily high order and is therefore infinite, whence B is certainly also infinite.

The semigroup Σ may be viewed as a semigroup of endomorphisms of Ω_a^{dr}. One can verify that Σ consists of epimorphisms, and consequently the set B' of all accumulation points of B is Σ-invariant. Let $M \subseteq B'$ be a Σ-minimal set. Select a point $x \in M$ and a sequence $(x_n)_{n=1}^{\infty}$ of distinct points in $\pi(\Sigma t)$ converging to x. Set $y_n = x_n - x$ for $n \in \mathbf{N}$. We can find a sequence $(\bar{y}_n)_{n=1}^{\infty}$ converging to 0 in $\prod_{j=0}^{h} \mathbf{Q}_{p_j}^{dr}$ such that $\pi(\bar{y}_n) = y_n$ for each n.

Denote by L the normal closure of the extension $\underline{K}/\mathbf{Q}$. Let $w^{(1)} = w$, $w^{(2)}, \ldots, w^{(dr)}$ be all the conjugates of w in L^{dr}. These vectors form a basis of

L^{dr} and each of them is an eigenvector of σ_0, and therefore a common eigenvector of Σ. For $0 \leqslant j \leqslant h$ denote by L_j the splitting field of f over $\boldsymbol{Q}_{p_j}$ and let $w^{1,j}, w^{2,j}, \ldots, w^{dr,j}$ be a basis of L_j^{dr} corresponding to the given basis of L^{dr}. We may assume that $w^{1,1}, w^{2,1}, \ldots, w^{d,1}$ are all the conjugates of $w^{1,1}$ over $\boldsymbol{Q}_{p_1}$.

Let $\lambda_{ij\sigma} \in L_j$ denote the eigenvalue of an endomorphism $\sigma \in \Sigma$ corresponding to the eigenvector $w^{i,j}$, $1 \leqslant i \leqslant dr$, $0 \leqslant j \leqslant h$. Put

$$C_j = \{1 \leqslant i \leqslant dr\colon |\lambda_{ij\sigma}|_{p_j} \leqslant 1 \ \forall \sigma \in \Sigma\},$$

$$V_{\leqslant 1,j} = \mathrm{sp}\,\{w^{i,j}\colon i \in C_j\} \subseteq L_j^{dr}, \qquad V_{>1,j} = \mathrm{sp}\,\{w^{i,j}\colon i \notin C_j\} \subseteq L_j^{dr}$$

for $0 \leqslant j \leqslant h$, and

$$V_{\leqslant 1} = \prod_{j=0}^{h} V_{\leqslant 1,j}, \qquad V_{>1} = \prod_{j=0}^{h} V_{>1,j}.$$

If $\bar{y}_n \notin V_{\leqslant 1}$ for infinitely many indices n, then the discussion in [4] follows verbatim to our case to prove that $B = \Omega_a^{dr}$, yielding a contradiction. We may assume accordingly that, say, $\bar{y}_1, \bar{y}_2 \in V_{\leqslant 1}$. Thus there exist distinct endomorphisms $\tau_1, \tau_2 \in \Sigma$ such that $\pi(\tau_1(t)) - x$ and $\pi(\tau_2(t)) - x$ have inverse images in $\prod_{j=0}^{h} \boldsymbol{Q}_{p_j}^{dr}$ lying in $V_{\leqslant 1}$, and in particular we have

$$\tau_2(t) - \tau_1(t) \in V_{\leqslant 1} + \mathrm{Ker}(\pi).$$

Set $\lambda_k = \lambda_{11\tau_k}$. Then

$$(5.2)\quad (0, \varphi((\lambda_2 - \lambda_1)\alpha u), 0, \ldots, 0) = \Big(\sum_{i \in C_0} \beta_{i0} w^{i,0}, \sum_{i \in C_1} \beta_{i1} w^{i,1}, \ldots, \sum_{i \in C_h} \beta_{ih} w^{i,h}\Big) + (\boldsymbol{b}, -\boldsymbol{b}, \ldots, -\boldsymbol{b})$$

for $\beta_{ij} \in L_j$ and $\boldsymbol{b} \in \boldsymbol{Z}[1/a]^{dr}$.

To exploit (5.2) we first need to show that for any $z \in E_{\mathfrak{P}}$ we have

$$(5.3)\qquad \varphi(zu) = \sum_{i=1}^{d} \gamma_i w^{i,1}$$

for appropriately chosen $\gamma_i \in L_1$, $1 \leqslant i \leqslant d$. In fact, write

$$\varphi(zu) = \sum_{i=1}^{dr} \gamma_i w^{i,1}.$$

For every non-negative integer n we then have

$$(5.4)\qquad \varphi(s_0^n zu) = \varphi(\tau^n(zu)) = \psi(\tau)^n \varphi(zu) = \sum_{i=1}^{dr} s_{0i}^n \gamma_i w^{i,1}$$

where s_{0i} is the conjugate of s_0 over $\boldsymbol{Q}$ corresponding to the conjugate $w^{i,1}$ of $w^{1,1}$. Now the sequence $(\varphi(s_0^n zu))_{n=1}^{\infty}$ satisfies the linear recurrence determined by the minimal polynomial of s_0 over $\boldsymbol{Q}_p$, and consequently

$$(5.5)\qquad \varphi(s_0^n zu) = \sum_{i=1}^{d} s_{0i}^n z^{(i)}, \quad n = 0, 1, 2, \ldots$$

for suitable vectors $z^{(1)}, \ldots, z^{(d)} \in L_1^{dr}$. The choice of s_0 ensures that $s_{0i}/s_{0i'}$ is not a root of unity for any $i \neq i'$. Comparing (5.4) and (5.5) we conclude therefore that $\gamma_i = 0$ for $d+1 \leqslant i \leqslant dr$, which yields (5.3).

From (5.2) we can now infer, similarly to [4], that

$$(5.6)\qquad C_j = \begin{cases} \{1, 2, \ldots, dr\}, & j = 0, 2, 3, \ldots, h, \\ \{d+1, d+2, \ldots, dr\}, & j = 1 \end{cases}$$

and that $\varphi((\lambda_2 - \lambda_1)\alpha u) \in L^{dr}$. (5.6) clearly implies that $\underline{S} \subseteq \mathrm{PSC}(\underline{K})$.

We want to show now that $\alpha \in \underline{K}$. According to (5.3) we can write

$$(5.7)\qquad \varphi(u) = \sum_{i=1}^{d} \delta_i w^{i,1}$$

for certain $\delta_1, \delta_2, \ldots, \delta_d$ in L_1. Let $\theta_1, \theta_2, \ldots, \theta_d$ be the embeddings of $E_{\mathfrak{P}}$ in L_1, enumerated in such a way that $\theta_i(w^{1,1}) = w^{i,1}$. Obviously, $\varphi(zu) = z\varphi(u)$ for $z \in \boldsymbol{Q}_p$. It follows therefore from (5.4), since $\{1, s_0, s_0^2, \ldots\}$ span $E_{\mathfrak{P}}$ over $\boldsymbol{Q}_p$, that

$$\varphi(zu) = \sum_{i=1}^{d} \delta_i \theta_i(z) w^{i,1}, \qquad z \in E_{\mathfrak{P}}.$$

From (5.2) we then obtain

$$(5.8)\qquad \sum_{i=1}^{d} \delta_i \theta_i((\lambda_2 - \lambda_1)\alpha) w^{i,1} - \sum_{i=d+1}^{dr} \beta_{i1} w^{i,1} = -\boldsymbol{b}.$$

Viewing (5.8) as a linear system of dr equations over L in the unknowns $\delta_1\theta_1((\lambda_2 - \lambda_1)\alpha), \ldots, \delta_d\theta_d((\lambda_2 - \lambda_1)\alpha), \beta_{d+1,1}, \ldots, \beta_{dr,1}$, we observe that each of these must lie in L. Consider any $\theta \in \mathrm{Gal}(L/\boldsymbol{Q})$ belonging to the fixed group of $\underline{K}$. Letting θ act on both sides of (5.8), we see that θ leaves fixed the vector $w^{1,1}$, and hence also its coefficient. From this we infer that $\delta_1(\lambda_2 - \lambda_1)\alpha \in \underline{K}$. Rearranging the vectors $v^{(1)}, v^{(2)}, \ldots, v^{(d)}$ if necessary, we may assume that $v^{(i)} = \theta_i(v^{(1)})$ for $1 \leqslant i \leqslant d$. It is now easy to deduce from (5.7) that

$$(5.9)\qquad \varphi(1) = \sum_{i=1}^{d} \delta_i v^{(i)}.$$

Since the vectors $\omega_1, \omega_2, \ldots, \omega_d$ form a basis of E over $\boldsymbol{Q}$, $\varphi(1) \in \boldsymbol{Q}^d$.

Similarly to the way we concluded from (5.8) that $\delta_1(\lambda_2-\lambda_1)\alpha \in \underline{K}$, we conclude from (5.9) that $\delta_1 \in \underline{K}$. This implies that $\alpha \in \underline{K}$.

As in [4] we can now prove that $\underline{K} = K$. Let $s \in S$. Repeating all our construction with $\underline{S}$ replaced by the semigroup generated by $\underline{S}$ and s, we observe that the latter semigroup is also contained in $\mathrm{PSC}(K)$. Thus $S \subseteq \mathrm{PSC}(K)$.

The proof is thereby completed.

References

[1] P. T. Bateman and A. L. Duquette, *The analogue of the Pisot–Vijayaraghavan numbers in fields of formal power series*, Illinois J. Math. 6 (1962), 594–606.

[2] D. Berend, *Multi-invariant sets on compact abelian groups*, Trans. Amer. Math. Soc. 286 (1984), 505–535.

[3] —, *Minimal sets on tori*, Ergod. Th. and Dynam. Sys. 4 (1984), 499–507.

[4] —, *Dense* (mod 1) *dilated semigroups of algebraic numbers*, J. Number Theory 26 (1987), 246–256.

[5] H. Furstenberg, *Disjointness in ergodic theory, minimal sets and a problem in diophantine approximations*, Math. Systems Theory 1 (1967), 1–49.

[6] M. Grandet-Hugot, *Une propriété des "nombres de Pisot" dans un corps de séries formelles*, C. R. Acad. Sci. Paris Sér. A 265 (1967), 39–41; errata, *ibid.*, p. 551.

[7] —, *Éléments algébriques remarquables dans un corps de séries formelles*, Acta Arith. 14 (1968), 177–184.

[8] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York 1974.

[9] B. de Mathan, *Numbers contravening a condition in density modulo* 1, Acta Math. Acad. Sci. Hungar. 36 (1980), 237–241.

[10] Y. Meyer, *Algebraic Numbers and Harmonic Analysis*, North-Holland Publishing Company, Amsterdam–London 1972.

[11] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warsaw 1974.

[12] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, Berlin 1963.

[13] A. D. Pollington, *On the density of sequence* $\{n_k\xi\}$, Illinois J. Math. 23 (1979), 511–515.

[14] —, *The Hausdorff dimension of certain sets related to sequences which are not dense* mod 1, Quart. J. Math. Oxford 31 (1980), 351–361.

[15] P. Walters, *An Introduction to Ergodic Theory*, Springer-Verlag, New York 1982.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
BEN-GURION UNIVERSITY OF THE NEGEV
Beer-Sheva 84 105, Israel

Received on 14.7.1987
and in revised form on 13.1.1988 (1735)

ACTA ARITHMETICA
LII (1989)

On Mellin–Ramanujan expansions

by

DIETER KLUSCH (Rendsburg)

1. Introduction. Ramanujan's trigonometrical sums are given by

$$c_q(n) = \sum_{\substack{1 \leq h \leq q \\ (h,q)=1}} e^{-2\pi i n h/q} = \sum_{d \mid (n,q)} d\mu\left(\frac{q}{d}\right) \quad (q, n \in \mathbf{N}), \tag{1.1}$$

where $\mu(\cdot)$ is Möbius' μ-function. For fixed n the sequence $(c_q)_{q \geq 1}$ satisfies certain orthogonal relations. Thus in analogy to the Fourier theory of real functions the theory of Fourier–Ramanujan expansions

$$f(n) \sim \sum_{q \geq 1} a_q(f)\, c_q(n) \quad (n \in \mathbf{N}) \tag{1.2}$$

for arithmetical functions $f\colon \mathbf{N} \to \mathbf{C}$ (including the cases when f is multiplicative or additive) has been established by many authors [5], [6], [10], [12], [14]. The connection with the theory of Mellin integral transforms was studied by the author [7].

First special point-wise convergent expansions of the converse form

$$f(q) = \sum_{n \geq 1} a_n(f)\, c_q(n) \quad (q \in \mathbf{N}) \tag{1.3}$$

for arithmetical $f\colon \mathbf{N} \to \mathbf{C}$ are due to S. Ramanujan [9] and M. M. Crum ([4]; [11], pp. 10–12), e.g.

$$\sum_{d \mid q} \mu\left(\frac{q}{d}\right) d^{1-s} = \frac{1}{\zeta(s)} \sum_{n \geq 1} n^{-s} c_q(n) \tag{1.4}$$

($\operatorname{Re} s > 1$, $\zeta(s)$ being Riemann's zeta-function).

In contrast to (1.2) general criterions on the existence of the coefficients $a_n(f)$ in (1.3) even for special classes of f seem not to be known.

In the present paper we solve this open problem for the class of Dirichlet convolutions $g\colon \mathbf{N} \to \mathbf{C}$ defined for $q \in \mathbf{N}$ and $\operatorname{Re}\alpha \geq 0$ by

$$g_\alpha(q) = \sum_{d \mid q} \mu\left(\frac{q}{d}\right) d^{1-\alpha} w(d), \tag{1.5}$$