TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 280, Number 2, December 1983

MULTI-INVARIANT SETS ON TORI

BY
DANIEL BEREND

ABSTRACT. Given a compact metric group G, we are interested in those semigroups Σ of continuous endomorphisms of G, possessing the following property: The only infinite, closed, Σ-invariant subset of G is G itself. Generalizing a one-dimensional result of Furstenberg, we give here a full characterization—for the case of finite-dimensional tori—of those commutative semigroups with the aforementioned property.

1. Introduction. Let Σ be a multiplicative semigroup of integers. Σ is *lacunary* if all the members of $\{\sigma \in \Sigma \mid \sigma > 0\}$ are powers of a single integer a. Otherwise, Σ is *nonlacunary*. With this terminology, Furstenberg proves in [**1**, p. 48] the following

THEOREM. *If Σ is a nonlacunary semigroup of integers and α is an irrational, then $\Sigma\alpha$ is dense modulo* 1.

This theorem is a generalization of a theorem of Hardy and Littlewood, which asserts that if r is a fixed positive integer and α is an irrational, then the set $\{n^r\alpha \mid n \in \mathbf{N}\}$ is dense modulo 1.

From the point of view of the theory of diophantine approximations, we are in a special case of the following general situation: Suppose G is a metric group and H is a closed subgroup, which is invariant under a given commutative semigroup S of continuous endomorphisms of G. We can form the subgroup H/S of G, consisting of all the elements of G which are carried to H by some endomorphism in S. Now it can be asked how closely, in a properly defined sense, can the elements of G be approximated by elements of H/S. The theorem relates to the case $G = \mathbf{R}$, $H = \mathbf{Z}$, and implies that if S is a nonlacunary semigroup, then for every irrational $\alpha \in \mathbf{R}$ and for every $\varepsilon > 0$ there is some $m/s \in \mathbf{Z}/S$ such that

$$(1.1) \qquad |\alpha - m/s| < \varepsilon/s.$$

Restricting ourselves to the problem of approximating irrational numbers, we may ask which sets S of positive integers have the property that every irrational α can be approximated as in (1.1) by rationals with denominators in S. The theorem supplies a complete answer in the case that S is a multiplicative semigroup. Such approximations are possible iff S is nonlacunary. (Actually, for lacunary S it is easy to find irrationals α for which (1.1) is impossible for sufficiently small $\varepsilon > 0$.)

Received by the editors May 24, 1982.

1980 *Mathematics Subject Classification*. Primary 10F10, 54H20; Secondary 28A65, 54H15.

Key words and phrases. Invariant set, finite-dimensional torus, semigroup of endomorphisms, ergodic endomorphism, minimal set.

The theorem has a dynamic aspect also. Given a continuous operator on a compact metric space, a basic problem is to describe the orbits of the points under the operator. Of course, instead of considering only one operator (or, more precisely, a one-parameter semigroup or group of operators), we may study the action generated by several operators. An important notion in this connection is that of a minimal system, i.e. a system in which the orbit of any point is dense in the space. A special, highly important case is that of semigroups of continuous endomorphisms of compact metric groups. In this case minimality is impossible; the unit of the group, for example, always has a trivial orbit.

In this language the theorem is concerned with orbits of points of the circle group $\mathbf{T}$ under a semigroup Σ of endomorphisms of $\mathbf{T}$. It asserts that, unless Σ is a one-parameter semigroup, the system is "almost minimal". That is, apart from the torsion elements (the rationals), which have easily describable finite orbits, each element gives rise to a dense orbit. The theorem is almost equivalent to the assertion that an infinite, closed set E in $\mathbf{T}$, which is invariant under a nonlacunary semigroup of endomorphisms of $\mathbf{T}$, is necessarily the whole of $\mathbf{T}$.

The theorem is proved in two stages:

(1) First, it is shown that if the set E has the additional property of containing the point 0 as a nonisolated point, then E is the whole group.

(2) Second, using results relating to the notion of disjointness, the case of arbitrary sets is established.

The main theme of this paper is a generalization of the theorem to finite-dimensional tori. We obtain necessary and sufficient conditions on a commutative semigroup Σ of endomorphisms of $\mathbf{T}^r$ to have the property that an infinite, closed, Σ-invariant subset of $\mathbf{T}^r$ is necessarily $\mathbf{T}^r$ itself. We might point out that these conditions are surprisingly mild and that, even in higher dimensions, "most" commutative semigroups (though not the one-parameter semigroups) satisfy them.

Theorem 2.1, which states these conditions, is formulated in §2. That section also contains a few notations and definitions we use in the sequel.

In §3 we prove the necessity of the conditions of the theorem. For every commutative Σ, which does not fulfill the conditions, we build an infinite, closed, Σ-invariant, proper subset of $\mathbf{T}^r$.

The two following sections are devoted to the proof of the sufficiency of the conditions. Similarly to the way of proof in the one-dimensional case, we first prove in §4 that a closed, Σ-invariant set, which contains 0 as a nonisolated point, is necessarily the whole group. This part, which is rather trivial in the one-dimensional case, is much more involved in the general case. In §5 we complete the proof, passing to arbitrary infinite, closed, Σ-invariant sets. The tools developed in [**1**] for the one-dimensional case are sufficiently general to enable us to complete the proof in our case as well.

In §6 the conditions of the theorem are discussed. We show that they are very weak and how they can be verified in special cases.

I wish to express my gratitude to H. Furstenberg for the encouragement and the helpful advice he gave me while working on the subject.

2. The main theorem. Let $\mathbf{T}^r$ denote the r-dimensional torus considered as an additive group: $\mathbf{T}^r = \mathbf{R}^r/\mathbf{Z}^r$. The points of $\mathbf{T}^r$ are regarded as column vectors $x = (x_1, x_2, \dots, x_r)^T$. We do not distinguish between a point $x \in \mathbf{T}^r$ and points of $\mathbf{R}^r$ lying above it. The continuous endomorphisms of $\mathbf{T}^r$ correspond to $r \times r$ integer matrices. σ denotes an endomorphism as well as the corresponding matrix. Lifting σ we get a linear transformation of $\mathbf{R}^r$, denoted also by σ. The action of an endomorphism σ on a point x is given by $\sigma(x) = \sigma x$, to be understood as the product modulo 1 of the matrix σ and the vector x.

Let Σ denote a semigroup of endomorphisms of $\mathbf{T}^r$. To avoid trivialities, we assume throughout that the identity endomorphism I belongs to Σ, while the zero endomorphism 0 does not. A set $E \subseteq \mathbf{T}^r$ is Σ-*invariant* if $\sigma(E) \subseteq E$ for every $\sigma \in \Sigma$. A closed, Σ-invariant set M is *minimal* if there are no closed, nonvoid, Σ-invariant, proper subsets of M.

Studying the conditions, under which the property now to be defined is satisfied, is our main object of interest throughout the paper.

DEFINITION 2.1. The semigroup Σ satisfies the ID *property* if the only infinite, closed, Σ-invariant subset of $\mathbf{T}^r$ is $\mathbf{T}^r$ itself (ID—infinite invariant is dense).

We can also say, more briefly, that Σ is ID. As already indicated, the restriction to infinite sets in the definition is essential. In fact, considering the subgroups $\mathbf{T}^r[k]$ of torsion elements of order dividing k, k ranging over the positive integers, we obtain infinitely many fully invariant sets, i.e. sets which are invariant under all the endomorphisms of $\mathbf{T}^r$, and each of them is finite.

DEFINITION 2.2. Two endomorphisms σ, τ are *rationally dependent* if $\sigma^l = \tau^m$ for some nonzero integers l, m. Otherwise, they are *rationally independent*.

In a similar manner we define rational dependence and independence of pairs of nonzero complex numbers.

Our principal result can now be formulated.

THEOREM 2.1. *The commutative semigroup Σ of endomorphisms of $\mathbf{T}^r$ is an ID semigroup if and only if the following conditions are satisfied*:

(1) *There exists an endomorphism σ in Σ such that the characteristic polynomial of σ^n is irreducible over $\mathbf{Z}$ for every positive integer n.*

(2) *For every common eigenvector v of Σ there exists an endomorphism σ_v in Σ such that the corresponding eigenvalue λ_v of σ_v lies outside the unit disc in the complex plane.*

(3) *Σ contains a pair of rationally independent endomorphisms.*

Before proceeding to the proof of the theorem, one remark is in order. It will be shown in the course of the proof that if a commutative semigroup Σ satisfies the first condition of the theorem (or even a weaker one), then there exists a basis of $\mathbf{C}^r$ with respect to which all the linear transformations in Σ are in diagonal form (see Lemma 3.4). The vectors of this basis are the common eigenvectors of Σ, mentioned in the theorem in the second condition.

3. The necessity of the conditions. Throughout most of this section Σ will denote a commutative semigroup of endomorphisms of $\mathbf{T}^r$, which is known to satisfy the ID property. We shall prove a series of lemmas, which together imply that the three conditions in Theorem 2.1 are satisfied.

For an endomorphism σ we denote by f_σ its characteristic polynomial and by m_σ its minimal polynomial.

LEMMA 3.1. *m_σ is irreducible over $\mathbf{Z}$ for every $\sigma \in \Sigma$.*

PROOF. Suppose, to the contrary, that for some $\sigma \in \Sigma$ we have the nontrivial decomposition

$$m_\sigma = gh, \qquad (g, h \in \mathbf{Z}[x]). \tag{3.1}$$

Let

$$H = \{x \in \mathbf{T}^r \,|\, (g(\sigma))(x) = 0\}.$$

H is a closed subgroup of $\mathbf{T}^r$. Since $g(\sigma)$ is a polynomial in σ and Σ is commutative, $g(\sigma)$ commutes with every endomorphism in Σ. Hence H is Σ-invariant. By the nontriviality of the decomposition (3.1) we see that the rank of the matrix $g(\sigma)$ satisfies the inequalities $0 < \operatorname{rank}(g(\sigma)) < r$.

The left-hand side inequality shows that H is not the whole of $\mathbf{T}^r$, while the right-hand side shows that it is infinite.

Altogether, H is an infinite, closed, Σ-invariant, proper subset of $\mathbf{T}^r$, which is impossible since Σ is ID. The contradiction proves the lemma.

LEMMA 3.2. *There exists a basis of $\mathbf{C}^r$ with respect to which every $\sigma \in \Sigma$ is in diagonal form.*

PROOF. Suppose we are given a basis of $\mathbf{C}^r$ and a subsemigroup Σ' of Σ such that every $\sigma \in \Sigma'$ is in diagonal form with respect to that basis. (In the initial stage we have an arbitrary basis of $\mathbf{C}^r$ and the subsemigroup of Σ, consisting solely of the identity endomorphism.) For an endomorphism $\sigma \in \Sigma$ and an eigenvalue λ of σ let

$$V_{\sigma,\lambda} = \{v \in \mathbf{C}^r \,|\, \sigma(v) = \lambda v\}.$$

Having a basis with respect to which Σ' is in diagonal form means that $\mathbf{C}^r$ is the direct sum of all its subspaces of the form $\bigcap_{\sigma\in\Sigma'} V_{\sigma,\lambda(\sigma)}$ (most of which are null), where $\lambda\colon \Sigma' \to \mathbf{C}$ chooses for each $\sigma \in \Sigma'$ an eigenvalue of σ. If for every $\sigma \in \Sigma$ each such subspace is contained in one of the subspaces $V_{\sigma,\lambda}$, λ an eigenvalue of σ, then Σ itself is in diagonal form with respect to the present basis. Assume, therefore, this is not the case for some $\tau \in \Sigma$. Since Σ is commutative, every subspace of the form $\bigcap_{\sigma\in\Sigma'} V_{\sigma,\lambda(\sigma)}$ is Σ-invariant. Examine the restriction τ_1 of τ to some subspace of this form. Its minimal polynomial m_{τ_1} divides m_τ. In view of Lemma 3.1, m_τ is irreducible over $\mathbf{Z}$, and hence it has no multiple roots in $\mathbf{C}$. Consequently, m_{τ_1} also has no multiple roots. It follows that τ_1 is diagonalizable. Hence, in each subspace of the form $\bigcap_{\sigma\in\Sigma'} V_{\sigma,\lambda(\sigma)}$ we can find a basis, with respect to which the corresponding restriction of τ is in diagonal form. The union of all the bases obtained in this way forms a basis of $\mathbf{C}^r$, with respect to which the subsemigroup of Σ, generated by Σ' and τ, has diagonal form.

This change of basis, made in order to enable the augmentation of the subsemigroup of Σ consisting of those transformations which are already in diagonal form, causes an increase in the number of the independent nontrivial subspaces of the form $\bigcap_{\sigma\in\Sigma'}V_{\sigma,\lambda(\sigma)}$. Hence the process must terminate after a finite number of steps. The basis we have at this stage satisfies the conditions of the lemma.

Let us now fix some basis $(v^{(1)}, v^{(2)},\dots,v^{(r)})$ of $\mathbf{C}^r$ satisfying the conditions of the lemma. For an endomorphism $\sigma \in \Sigma$ we denote by $\lambda_{1,\sigma}\lambda_{2,\sigma},\dots,\lambda_{r,\sigma}$ its eigenvalues corresponding to this basis. We want to show that σ is uniquely determined by $\lambda_{1,\sigma}$, that is $\lambda_{1,\sigma} = \lambda_{1,\tau}$ implies $\sigma = \tau$. In fact, the semigroup of endomorphisms generated by Σ and $\varphi = \sigma - \tau$ is still a commutative ID semigroup. Since $\lambda_{1,\varphi} = \lambda_{1,\sigma} - \lambda_{1,\tau} = 0$, the polynomial m_φ is divisible by x. Lemma 3.1 implies then that $m_\varphi = x$, which means that $\varphi = 0$, whence $\sigma = \tau$.

Consequently, instead of considering the semigroup Σ, we may just as well examine the set $\Lambda_1 = \{\lambda_{1,\sigma} | \sigma \in \Sigma\}$. Λ_1 is obviously a multiplicative semigroup of nonzero complex numbers, each element in which is an algebraic number of order not exceeding r over $\mathbf{Q}$. We need information concerning the field extension of $\mathbf{Q}$ obtained by adjoining the set Λ_1. Let us denote this field by K.

LEMMA 3.3. $[K:\mathbf{Q}] = r$.

PROOF. Every element of K has a concrete representation as a polynomial in elements of Λ_1 with rational coefficients. Hence every element of K is an eigenvalue of an $r \times r$ rational matrix. Thus K is an algebraic extension of $\mathbf{Q}$, every element in which is of a degree not exceeding r over $\mathbf{Q}$. Hence $[K:\mathbf{Q}] \leqslant r$.

Now suppose that $[K:\mathbf{Q}] = k < r$. Consider the ring of endomorphisms Σ' generated by Σ. Regarded as a multiplicative semigroup, Σ' (without the zero endomorphism) is commutative and satisfies the ID property. Σ' is obviously in diagonal form with respect to the basis $v^{(1)}, v^{(2)},\dots,v^{(r)}$. Hence each $\sigma \in \Sigma'$ is uniquely determined by $\lambda_{1,\sigma}$. Consequently, Σ' is isomorphic to some subring of the ring of integers of K. This implies that Σ', regarded as an additive group, is isomorphic to some subgroup of $\mathbf{Z}^k$. But then Σ' is isomorphic to $\mathbf{Z}^l$ for some $l \leqslant k$. Let $\sigma_1, \sigma_2,\dots,\sigma_l$ be a system of generators of Σ'. For an arbitrary one-dimensional closed subgroup H of $\mathbf{T}^r$, consider the subgroup $\Sigma_{i=1}^l\sigma_i(H)$. This subgroup is infinite, closed and Σ'-invariant, and it is at most l-dimensional. This contradicts the ID property of Σ', which proves the lemma.

Now we can prove the necessity of the first condition in Theorem 2.1.

PROPOSITION 3.1. *There exists some $\sigma \in \Sigma$ such that f_{σ^n} is irreducible over $\mathbf{Z}$ for every $n \in \mathbf{N}$.*

PROOF. Since the roots of f_{σ^n} are $\lambda_{1,\sigma}^n, \lambda_{2,\sigma}^n,\dots,\lambda_{r,\sigma}^n$, it is sufficient to prove the existence of an endomorphism σ in Σ such that $\mathbf{Q}(\lambda_{1,\sigma}^n) = K$ for every $n \in \mathbf{N}$. Suppose, to the contrary, that there exists no such endomorphism in Σ. Denoting by $F_1, F_2,\dots,F_l$ the proper subfields of K, we find that for every $\sigma \in \Sigma$ there exists a positive integer n such that $\lambda_{1,\sigma}^n \in F_i$ for some $1 \leqslant i \leqslant l$.

For an arbitrary subset A of K let

$$\sqrt{A} = \{\alpha \in K | \exists n \in \mathbf{N}, \alpha^n \in A\}, \qquad \Sigma_A = \{\sigma \in \Sigma | \lambda_{1,\sigma} \in A\}.$$

Our assumption that the proposition fails to be true means then that

$$\Sigma = \bigcup_{i=1}^{l} \Sigma_{\sqrt{F_i}}.$$

Let H be an arbitrary one-dimensional closed subgroup of $\mathbf{T}^r$. For a set Σ' of endomorphisms of $\mathbf{T}^r$ and a subset A of $\mathbf{T}^r$, we denote the set $\bigcup_{\sigma \in \Sigma'} \sigma(A)$ by $\Sigma' A$. In view of the foregoing decomposition of Σ it is clear that, in order to arrive at a contradiction to Σ being ID, it is sufficient to show that for each $1 \leqslant i \leqslant l$ the set $\Sigma_{\sqrt{F_i}} H$ is contained in a finite union of closed proper subgroups of $\mathbf{T}^r$. So let F be one of the fields F_i, $1 \leqslant i \leqslant l$. To show that $\Sigma_{\sqrt{F}} H$ is contained in a finite union of subgroups of $\mathbf{T}^r$, it is sufficient to show that $\sqrt{F}$ can be represented as

$$\sqrt{F} = \bigcup_{j=1}^{m} F\alpha_j, \qquad \alpha_j \in K, 1 \leqslant j \leqslant m. \tag{3.2}$$

In fact, using the same arguments as the ones used in the proof of Lemma 3.3, we observe that, if $\Sigma'_{F\alpha_j}$ denotes the (additive) group generated by $\Sigma_{F\alpha_j}$, then $\Sigma'_{F\alpha_j} H$ is contained in a subgroup of $\mathbf{T}^r$, the dimension of which does not exceed $[F : \mathbf{Q}]$. Since the decomposition (3.2) of $\sqrt{F}$ leads to a corresponding decomposition of $\Sigma_{\sqrt{F}}$, namely $\Sigma_{\sqrt{F}} = \bigcup_{j=1}^{m} \Sigma_{F\alpha_j}$, the set $\Sigma_{\sqrt{F}} H$ is contained in a finite union of proper subgroups of $\mathbf{T}^r$.

Let R^* denote thc multiplicative group of invertible elements of a ring R with a unit element. F^* is a subgroup of $\sqrt{F}^*$, which is in turn a subgroup of K^*. To establish a decomposition of $\sqrt{F}$ as in (3.2) we only have to show that

$$\left[\sqrt{F}^* : F^*\right] < \infty. \tag{3.3}$$

Let α be an arbitrary element of $\sqrt{F}^*$. For some positive integer s we have

$$\alpha^s = a \in F^*. \tag{3.4}$$

Let us recall a few definitions and basic results concerning the groups of fractional ideals in F and in K, to be denoted by I_F and by I_K, respectively (see, for example, Narkiewicz [3]).

(1) Every fractional ideal $\mathfrak{A}$ can be uniquely decomposed into a product of integer powers of distinct prime ideals in the ring of integers of the field.

(2) There is a natural injection of I_F into I_K, whereby I_F may be thought of as a subset of I_K.

(3) In particular, we are interested in the decomposition

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_h^{e_h} \qquad (e_i \geqslant 1, 1 \leqslant i \leqslant h) \tag{3.5}$$

of every prime in I_F into a product of primes in I_K. Each $\mathfrak{P}_i$ is said to *lie above* $\mathfrak{p}$. Two ideals $\mathfrak{P}_1$, $\mathfrak{P}_2$, lying above distinct $\mathfrak{p}_1$, $\mathfrak{p}_2$, are themselves distinct. If in the decomposition (3.5) there is some $e_i > 1$, then $\mathfrak{p}$ is *ramified*. Only a finite number of primes in I_F are ramified.

(4) In the group I_F we distinguish a subgroup PI_F, consisting of all principal fractional ideals of F. The group I_F/PI_F, which is termed the *group of ideal classes*, is finite.

Returning to (3.4), we see that, in particular, the fractional ideals generated by α^s and by a are the same. That is, we have the following equality in I_K:

$$(3.6) \qquad (\alpha)^s = (a).$$

Now we decompose (α) and (a) into products of primes:

$$(3.7) \qquad (\alpha) = \mathfrak{P}_1^{k_1}\mathfrak{P}_2^{k_2}\cdots\mathfrak{P}_u^{k_u} \in I_K.$$

$$(3.8) \qquad (a) = \mathfrak{p}_1^{l_1}\mathfrak{p}_2^{l_2}\cdots\mathfrak{p}_v^{l_v} \in I_F.$$

Decomposing each $\mathfrak{p}_i$, $1 \leqslant i \leqslant v$, into a product of primes in I_K, and substituting (3.7) and (3.8) in (3.6), we are due to obtain an identity. Suppose that one of the primes $\mathfrak{p}_i$ decomposes, say, as in (3.5). Then that part of (3.7) which is composed of ideals lying above that $\mathfrak{p}_i$ is necessarily of the form $\mathfrak{A}^m$ where

$$\mathfrak{A} = \mathfrak{P}_1^{e_1/e}\mathfrak{P}_2^{e_2/e}\cdots\mathfrak{P}_h^{e_h/e}$$

with $e = \text{g.c.d.}(e_1, e_2, \ldots, e_h)$, and m is a positive integer. In particular, every unramified $\mathfrak{p}$, which appears on the right-hand side of (3.8), appears (decomposed perhaps) in an appropriate power in (3.7) also.

Hence there exist $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_w \in I_K$ (nontrivial roots of primes in I_F) and corresponding positive integers $n_1, n_2, \ldots, n_w$, such that

$$(\alpha) = \mathfrak{A}\mathfrak{A}_1^{m_1}\mathfrak{A}_2^{m_2}\cdots\mathfrak{A}_w^{m_w}, \qquad 0 \leqslant m_j < n_j,\ 1 \leqslant j \leqslant w,$$

for some $\mathfrak{A} \in I_F$. Let $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_t$ be a full system of elements of I_F, mutually noncongruent modulo PI_F. Then

$$(3.9) \qquad (\alpha) = (b)\mathfrak{B}_i\mathfrak{A}_1^{m_1}\cdots\mathfrak{A}_w^{m_w}, \qquad 0 \leqslant m_j < n_j,\ 1 \leqslant j \leqslant w,$$

for some $b \in F$ and $1 \leqslant i \leqslant t$.

Consider the subgroup of $\sqrt{F}^*$ consisting of those $\alpha \in \sqrt{F}^*$ such that $(\alpha) = (b)$ for some $b \in F^*$. Denoting by $\mathcal{O}_K$ the ring of integers of K, we readily see that this group is just $\mathcal{O}_K^*F^* \cap \sqrt{F}^*$. Now

$$(3.10) \qquad \left[\sqrt{F}^* : F^*\right] = \left[\sqrt{F}^* : \mathcal{O}_K^*F^* \cap \sqrt{F}^*\right]\cdot\left[\mathcal{O}_K^*F^* \cap \sqrt{F}^* : F^*\right].$$

The first factor on the right-hand side of (3.10) is finite by (3.9). Hence, to establish (3.3) it remains to show that

$$(3.11) \qquad \left[\mathcal{O}_K^*F^* \cap \sqrt{F}^* : F^*\right] < \infty.$$

We obviously have $\mathcal{O}_K^*F^* \cap \sqrt{F}^* = (\mathcal{O}_K^* \cap \sqrt{F}^*)F^*$. This implies

$$\mathcal{O}_K^*F^* \cap \sqrt{F}^*/F^* \cong \mathcal{O}_K^* \cap \sqrt{F}^*/\mathcal{O}_K^* \cap F^*.$$

Consequently, (3.11) is equivalent to

$$(3.12) \qquad \left[\mathcal{O}_K^* \cap \sqrt{F}^* : \mathcal{O}_K^* \cap F^*\right] < \infty.$$

Let Ω_K denote the finite group of roots of unity lying in K. By Dirichlet's unit theorem there exist units $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m \in \mathcal{O}_K^*$ such that every $\eta \in \mathcal{O}_K^*$ can be uniquely represented in the form

$$(3.13) \qquad \eta = \xi\cdot\varepsilon_1^{i_1}\varepsilon_2^{i_2}\cdots\varepsilon_m^{i_m},$$

where $\xi \in \Omega_K$ and $i_1, i_2, \ldots, i_m$ are integers. Let H denote the subgroup of $\mathcal{O}_K^*$ consisting of those $\eta \in \mathcal{O}_K^*$ with $\xi = 1$ in their decomposition. We have

$$(3.14)\quad \left[\mathcal{O}_K^* \cap \sqrt{F^*} : \mathcal{O}_K^* \cap F^*\right] \leqslant \left[\mathcal{O}_K^* \cap \sqrt{F^*} : H \cap F^*\right]$$
$$= \left[\mathcal{O}_K^* \cap \sqrt{F^*} : H \cap \sqrt{F^*}\right] \cdot \left[H \cap \sqrt{F^*} : H \cap F^*\right]$$
$$\leqslant \left[\mathcal{O}_K^* : H\right] \cdot \left[H \cap \sqrt{F^*} : H \cap F^*\right] = |\Omega_K| \cdot \left[H \cap \sqrt{F^*} : H \cap F^*\right].$$

Dirichlet's theorem establishes an isomorphism, given through (3.13), between H and $\mathbf{Z}^m$, carrying the two subgroups $H \cap \sqrt{F^*}$ and $H \cap F^*$ of H into the subgroups Γ_1 and Γ_2 of $\mathbf{Z}^m$, respectively. Of course $\Gamma_1 \supseteq \Gamma_2$. Since from (3.13) it is clear that every element of Γ_1 has some nonzero multiple lying in Γ_2, both groups are of the same rank. Since every subgroup of $\mathbf{Z}^m$ is isomorphic to $\mathbf{Z}^n$ for some $0 \leqslant n \leqslant m$, and since a subgroup of rank n of $\mathbf{Z}^n$ is of finite index in $\mathbf{Z}^n$, we obtain

$$\left[H \cap \sqrt{F^*} : H \cap F^*\right] = [\Gamma_1 : \Gamma_2] < \infty.$$

Thus, applying (3.14), we see that (3.12) is indeed true, which completes the proof of the proposition.

For a polynomial f over $\mathbf{Q}$ we denote by $\mathbf{Q}(f)$ the splitting field of f over $\mathbf{Q}$. We use the same notation for an automorphism of $\mathbf{Q}(f)$ and for its natural extension to $\mathbf{Q}(f)^n$, n being any positive integer. Now we can formulate the following lemma, which helps us to visualize Σ more clearly. Since the lemma will be used in §4 also, we do not assume that Σ is an ID semigroup.

LEMMA 3.4. *Let Σ be a commutative semigroup of endomorphisms of $\mathbf{T}^r$. Assume there is some σ in Σ with f_σ irreducible over $\mathbf{Z}$. Then*:

(1) *The roots $\lambda_{1,\sigma}, \lambda_{2,\sigma}, \ldots, \lambda_{r,\sigma}$ of f_σ are mutually distinct.*

(2) *There exists some basis $v^{(1)}, v^{(2)}, \ldots, v^{(r)}$ of $\mathbf{C}^r$ such that*:

(a) *Σ is in diagonal form with respect to this basis.*

(b) *$v^{(i)} \in \mathbf{Q}(\lambda_{i,\sigma})^r$ for all $1 \leqslant i \leqslant r$.*

(c) *If ψ is any element of the Galois group of the extension $\mathbf{Q}(f_\sigma)/\mathbf{Q}$ then $\psi(v^{(i)}) = v^{(j)}$ iff $\psi(\lambda_{i,\sigma}) = \lambda_{j,\sigma}$.*

(3) *Every endomorphism τ in Σ can be uniquely expressed in the form $\tau = \sum_{i=0}^{r-1} a_i \sigma^i$ with $a_i \in \mathbf{Q}$ for all $0 \leqslant i \leqslant r - 1$.*

PROOF. The first part follows from the irreducibility of f_σ.

To construct a basis with the required properties we proceed as follows. The homogeneous system of linear equations over $\mathbf{Q}(\lambda_{1,\sigma})$,

$$(3.15)\qquad (\sigma - \lambda_{1,\sigma})v = 0,$$

is known to have a nontrivial solution v in $\mathbf{C}^r$. Hence it also has a nontrivial solution $v^{(1)}$ in $\mathbf{Q}(\lambda_{1,\sigma})^r$.

Let the elements of the Galois group of the extension $\mathbf{Q}(f_\sigma)/\mathbf{Q}$ act on the system of equalities obtained from (3.15) after replacing v with $v^{(1)}$. We obtain solutions $v^{(2)}, \ldots, v^{(r)}$ of the systems produced by (3.15) when substituting $\lambda_{2,\sigma}, \ldots, \lambda_{r,\sigma}$, respectively, for $\lambda_{1,\sigma}$. Evidently, the resulting vectors $v^{(1)}, v^{(2)}, \ldots, v^{(r)}$ satisfy (2)(b) and they are eigenvectors of σ, corresponding to the eigenvalues $\lambda_{1,\sigma}, \lambda_{2,\sigma}, \dots, \lambda_{r,\sigma}$, respectively. Hence, they form a basis of $\mathbf{C}^r$. It is now clear that they satisfy (2)(c) also.

Since σ is in diagonal form with respect to the chosen basis, (2)(a) is a consequence of (3), whence it remains to prove only the latter part.

Let us determine the algebra of all matrices X over some subfield L of $\mathbf{C}$ commuting with σ, to be denoted by $C_L(\sigma)$. Since the condition of commuting $\sigma X = X\sigma$ is given by a homogeneous system of linear equations over $\mathbf{Q}$, $\dim(C_L(\sigma))$ is independent of the choice of L. Hence $\dim(C_{\mathbf{Q}}(\sigma)) = \dim(C_{\mathbf{C}}(\sigma))$. Let $\tilde{\sigma}$ be the diagonal matrix representing σ with respect to the basis $v^{(1)}, v^{(2)}, \dots, v^{(r)}$. It is easy to verify that $\dim(C_{\mathbf{C}}(\sigma)) = \dim(C_{\mathbf{C}}(\tilde{\sigma}))$. Now the elements on the main diagonal of $\tilde{\sigma}$ are $\lambda_{1,\sigma}, \lambda_{2,\sigma}, \dots, \lambda_{r,\sigma}$. Since they are mutually distinct, $C_{\mathbf{C}}(\tilde{\sigma})$ is just the r-dimensional algebra of all diagonal matrices. Hence $C_{\mathbf{Q}}(\sigma)$ is also r-dimensional.

The algebra $P_{\mathbf{Q}}(\sigma)$, consisting of all polynomials in σ with rational coefficients, is obviously contained in $C_{\mathbf{Q}}(\sigma)$. Since all the eigenvalues of σ are distinct we have $m_\sigma = f_\sigma$. Hence $P_{\mathbf{Q}}(\sigma)$ is also r-dimensional. Consequently $C_{\mathbf{Q}}(\sigma) = P_{\mathbf{Q}}(\sigma)$, and the last part of the lemma follows.

Now we fix a basis $v^{(1)}, v^{(2)}, \dots, v^{(r)}$ satisfying the conditions of the lemma. We return to the proof that an ID semigroup Σ satisfies the conditions in Theorem 2.1. The necessity of the second condition is seen in the following

Lemma 3.5. *For every* $1 \leqslant i \leqslant r$ *there exists an endomorphism* σ_i *in* Σ *such that* $|\lambda_{i,\sigma_i}| > 1$.

Proof. Suppose, to the contrary, that, for example, $|\lambda_{1,\sigma}| \leqslant 1$ for all $\sigma \in \Sigma$. To arrive at a contradiction, we shall build an infinite, closed, Σ-invariant, proper subset of $\mathbf{T}^r$. Let us select an endomorphism $\tau \in \Sigma$ with f_τ irreducible. We distinguish between two cases.

Case I. $\lambda_{1,\tau}$ is real.

In this case we see, using Lemma 3.4, that $\lambda_{1,\sigma}$ is real for all $\sigma \in \Sigma$ and that the vector $v^{(1)}$ is real as well. It is clear that, for sufficiently small $a > 0$, the projection of the line segment

$$\mathfrak{L}_a = \{ t v^{(1)} \mid t \in \mathbf{R}, |t| \leqslant a \} \subseteq \mathbf{R}^r$$

on $\mathbf{T}^r$ may serve as the required set.

Case II. $\lambda_{1,\tau}$ is nonreal.

In this case $\overline{\lambda_{1,\tau}}$ also is an eigenvalue of τ, say $\lambda_{2,\tau} = \overline{\lambda_{1,\tau}}$, where the bar denotes complex conjugation. By Lemma 3.4 we have $v^{(2)} = \overline{v^{(1)}}$ and $\lambda_{2,\sigma} = \overline{\lambda_{1,\sigma}}$ for all $\sigma \in \Sigma$. As a set with the required properties we may choose the projection of an ellipse (its interior included) of the form

$$\mathfrak{E}_a = \{ z v^{(1)} + \bar{z} v^{(2)} \mid z \in C, |z| \leqslant a \} \subseteq \mathbf{R}^r$$

on $\mathbf{T}^r$ for some sufficiently small $a > 0$. This completes the proof.

Now we turn to the proof of the necessity of the third condition in Theorem 2.1. First, we show that it is impossible for a one-parameter semigroup, or group, to satisfy the ID property. For a matrix σ we denote by $S(\sigma)$ the semigroup consisting of all the nonnegative powers of σ and by $G(\sigma)$ the group consisting of all integral powers of σ.

LEMMA 3.6. *Let σ be an endomorphism of $\mathbf{T}^r$. Then*:

(1) *$S(\sigma)$ does not satisfy the ID property.*

(2) *If σ is an automorphism then $G(\sigma)$ is not ID as well.*

PROOF. We have to consider only the case in which f_σ is irreducible. We treat separately the case in which σ is an automorphism and the case in which it is not, building in each an infinite, closed, proper subset of $\mathbf{T}^r$, which is invariant under the relevant semigroup.

Case I. σ is not an automorphism.

In view of Lemma 3.5 we may assume that $|\lambda_{i,\sigma}|> 1$ for all $1 \leqslant i \leqslant r$.

Choose some nonzero integral point e in $\mathbf{R}^r$, say $e = (1,0,\dots,0)^T$. We assert that the projection on $\mathbf{T}^r$ of the set

$$\mathcal{O}_\sigma^-(e) = \{\sigma^{-n}(e) \mid n \geqslant 0\} \subseteq \mathbf{R}^r,$$

which is the orbit of e in $\mathbf{R}^r$ under the linear transformation σ^{-1}, has the needed properties. In fact, it is obviously an $S(\sigma)$-invariant, proper subset of $\mathbf{T}^r$. Now, decompose e in $\mathbf{C}^r$ into a sum of eigenvectors of σ:

$$e = \alpha_1 v^{(1)} + \alpha_2 v^{(2)} + \cdots + \alpha_r v^{(r)}. \tag{3.16}$$

For every $n \geqslant 0$ we have

$$\sigma^{-n}(e) = \lambda_{1,\sigma}^{-n}\alpha_1 v^{(1)} + \lambda_{2,\sigma}^{-n}\alpha_2 v^{(2)} + \cdots + \lambda_{r,\sigma}^{-n}\alpha_r v^{(r)}.$$

Hence $\sigma^{-n}(e) \underset{n\to\infty}{\to} 0$. Since $e \in \mathbf{R}^r$ projects into $0 \in \mathbf{T}^r$, this implies that our set is closed. Its infinity follows from the fact that $\sigma^{-n}(e) \neq 0$ for all n.

Case II. σ is an automorphism.

In view of Lemma 3.5 we may assume that σ has no eigenvalues on the unit circle. Suppose, for example, that $|\lambda_{i,\sigma}|< 1$ for $1 \leqslant i \leqslant k$, while $|\lambda_{i,\sigma}|> 1$ for $k < i \leqslant r$, where $1 \leqslant k < r$.

Select again the point $e \in \mathbf{R}^r$, used in the previous case, and perform the decomposition (3.16). Choose the point

$$v = e - \left(\alpha_1 v^{(1)} + \cdots + \alpha_k v^{(k)}\right) = \alpha_{k+1} v^{(k+1)} + \cdots + \alpha_r v^{(r)}. \tag{3.17}$$

The first representation of v shows that $\sigma^n(v) \underset{n\to\infty}{\to} 0 \pmod 1$, while the second shows that $\sigma^{-n}(v) \underset{n\to\infty}{\to} 0$. Hence the closure of the projection of the two-sided orbit of v under σ,

$$\mathcal{O}_\sigma(v) = \{\sigma^n(v) \mid n \in \mathbf{Z}\} \subseteq \mathbf{R}^r,$$

on $\mathbf{T}^r$ is just that projection together with the point 0. This set is, therefore, a closed, proper subset of $\mathbf{T}^r$, which is evidently also $G(\sigma)$-invariant.

It remains to prove that our set is infinite. For this it is obviously sufficient to show that $\sigma^n(v) \notin \mathbf{Z}^r$ for every $n \in \mathbf{Z}$. First, we deal with the point v. The numbers $\alpha_1, \alpha_2, \dots, \alpha_r$, used in (3.17) to define v, are uniquely determined by the nonhomogeneous system of linear equations (3.16). Since the coefficients of that system belong to $\mathbf{Q}(f_\sigma)$, we have $\alpha_i \in \mathbf{Q}(f_\sigma)$ for every $1 \leqslant i \leqslant r$. Let ψ be an automorphism of the extension $\mathbf{Q}(f_\sigma)/\mathbf{Q}$, which carries, say, $v^{(k+1)}$ to $v^{(1)}$. By (3.17) we have $\psi(v) \neq v$, whence $v \notin \mathbf{Q}^r$. Since $\sigma^n(e) \neq 0$ for all n, the same reasoning applies to show that $\sigma^n(v) \notin \mathbf{Q}^r$ for all n. This completes the proof.

Now we can complete the proof of the necessity of the third condition in Theorem 2.1.

PROPOSITION 3.2. *Σ contains a pair of rationally independent endomorphisms.*

PROOF. Choose an endomorphism $\sigma \in \Sigma$ with f_{σ^n} irreducible for all $n > 0$. We want to find an endomorphism $\tau \in \Sigma$, rationally independent of σ.

Denote by $D_R(\sigma)$ the set of matrices over the ring R, which commute with σ and are rationally dependent of it. From Lemma 3.4 it follows that $D_{\mathbf{Q}}(\sigma)$ is a commutative semigroup of matrices. To prove the proposition it is sufficient to show that its subsemigroup $D_{\mathbf{Z}}(\sigma)$ is not ID.

The main idea is to show that $D_{\mathbf{Z}}(\sigma)$ is not much larger than the multiplicative semigroup, or group, generated by σ, which was shown in Lemma 3.6 not to satisfy the ID property. More precisely, we claim that $D_{\mathbf{Z}}(\sigma)$ may be represented in the form

$$D_{\mathbf{Z}}(\sigma) = \bigcup_{i=1}^{s} G(\sigma)\cdot\sigma_i \tag{3.18}$$

if σ is an automorphism, and in the form

$$D_{\mathbf{Z}}(\sigma) = \bigcup_{i=1}^{s} S(\sigma)\cdot\sigma_i \tag{3.19}$$

if σ is not an automorphism, for a suitable finite set of endomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_s$ in $D_{\mathbf{Z}}(\sigma)$.

Suppose that such a decomposition has been accomplished. Let E be an infinite, closed, $G(\sigma)$-invariant (or $S(\sigma)$-invariant), proper subset of $\mathbf{T}^r$. The set $E_1 = \bigcup_{i=1}^{s}\sigma_i(E)$ is obviously infinite, closed and $D_{\mathbf{Z}}(\sigma)$-invariant. To show that E_1 is a proper subset of $\mathbf{T}^r$ we notice that, since f_{σ^n} is irreducible over $\mathbf{Z}$ for every positive n, f_σ has no roots of unity among its eigenvalues. (Actually, this is not exactly so if $r = 1$, in which case $\sigma = 1$ and $\sigma = -1$ are roots of unity, although they satisfy the irreducibility condition. Here we have to choose $\sigma \neq \pm 1$, which is, of course, possible.) Hence σ is *ergodic*, i.e., every closed, $S(\sigma)$-invariant, proper subset of $\mathbf{T}^r$ is nowhere dense [**1**, pp. 26–27]. This implies that E_1 is a proper subset of $\mathbf{T}^r$. Hence, $D_{\mathbf{Z}}(\sigma)$ does not satisfy the ID property.

Thus, it remains only to establish the possibility of representing $D_{\mathbf{Z}}(\sigma)$ as in (3.18) or (3.19). Let τ be any element of $D_{\mathbf{Z}}(\sigma)$. Suppose

$$\tau^l = \sigma^m \tag{3.20}$$

for some nonzero integers l, m. In particular we have

$$\lambda_{1,\tau}^{l} = \lambda_{1,\sigma}^{m}. \tag{3.21}$$

The solutions $\lambda_{1,\tau} \in K$ of (3.21) are in correspondence with the solutions $\tau \in D_{\mathbf{Q}}(\sigma)$ of (3.20). Hence we only have to find the solutions of (3.21). We distinguish between two cases.

Case I. σ is an automorphism.

In this case the numbers $\lambda_{1,\sigma}$ and $\lambda_{1,\tau}$ belong to $\mathcal{O}_K^*$. Using Dirichlet's unit theorem we decompose $\lambda_{1,\sigma}$:

$$\lambda_{1,\sigma} = \xi \cdot \varepsilon_1^{k_1} \varepsilon_2^{k_2} \cdots \varepsilon_u^{k_u} \qquad (\xi \in \Omega_K,\, k_i \in \mathbf{Z},\, 1 \leqslant i \leqslant u).$$

Now $\lambda_{1,\tau}$ solves (3.21) for some l, m iff it is of the form

$$\lambda_{1,\tau} = \xi' \cdot \varepsilon_1^{tk_1} \varepsilon_2^{tk_2} \cdots \varepsilon_u^{tk_u}$$

where ξ' is any element of Ω_K and $t \in \frac{1}{k}\mathbf{Z}$, k being the g.c.d. of $k_1, k_2, \ldots, k_u$. Hence

$$[D_{\mathbf{Q}}(\sigma) : G(\sigma)] = k \cdot |\Omega_K| < \infty.$$

Consequently, we obtain $[D_{\mathbf{Z}}(\sigma) : G(\sigma)] < \infty$, proving the feasibility of a decomposition of the form (3.18).

Case II. σ is not an automorphism.

From (3.21) we obtain, by passing to I_K, that $(\lambda_{1,\tau})^l = (\lambda_{1,\sigma})^m$. Let us decompose $(\lambda_{1,\sigma})$ into a product of primes in I_K:

$$(\lambda_{1,\sigma}) = \mathfrak{p}_1^{k_1} \mathfrak{p}_2^{k_2} \cdots \mathfrak{p}_v^{k_v}.$$

It is immediately seen that $(\lambda_{1,\tau})$ is necessarily of the form

$$(3.22) \qquad (\lambda_{1,\tau}) = \mathfrak{p}_1^{tk_1} \mathfrak{p}_2^{tk_2} \cdots \mathfrak{p}_v^{tk_v}$$

with $t \in \frac{1}{k}\mathbf{Z}$, k being the g.c.d. of $k_1, k_2, \ldots, k_v$.

Now, the set of numbers t, for which the ideal $\mathfrak{p}_1^{tk_1} \mathfrak{p}_2^{tk_2} \cdots \mathfrak{p}_v^{tk_v}$ is actually generated by a solution $\lambda_{1,\tau}$ of (3.21), forms a subgroup of $\frac{1}{k}\mathbf{Z}$ containing $\mathbf{Z}$, say, $\frac{1}{k'}\mathbf{Z}$. For any $t \in \frac{1}{k'}\mathbf{Z}$ there are exactly $|\Omega_K|$ solutions $\lambda_{1,\tau}$ of (3.21) generating the ideal $\mathfrak{p}_1^{tk_1} \mathfrak{p}_2^{tk_2} \cdots \mathfrak{p}_v^{tk_v}$. In fact, if $\lambda_{1,\tau}$ satisfies both of these conditions, then the set of all elements satisfying them is just $\Omega_K \lambda_{1,\tau}$. Hence $[D_{\mathbf{Q}}(\sigma) : G(\sigma)] = k' |\Omega_K|$.

For every $\tau \in D_{\mathbf{Z}}(\sigma)$ the number t corresponding to τ in (3.22) is nonnegative. Hence it is evident that if out of every coset of $D_{\mathbf{Q}}(\sigma)$ modulo $G(\sigma)$ we select that endomorphism $\tau \in D_{\mathbf{Z}}(\sigma)$, if there exists any, for which t is the minimum possible, then we obtain a finite set of endomorphisms, for which the decomposition (3.19) holds. This proves the proposition.

Thus, the conditions stated in Theorem 2.1 have been shown to be necessary for Σ to be an ID semigroup, so we turn to prove their sufficiency.

4. Sufficiency—sets with 0 **as a nonisolated point.** Throughout this section Σ denotes a commutative semigroup satisfying the conditions stated in Theorem 2.1. E is a closed, Σ-invariant subset of $\mathbf{T}^r$ which contains 0 as a nonisolated point. Our aim is to show that E is necessarily $\mathbf{T}^r$ itself, which will prove that Σ satisfies what might be called a restricted ID property.

Lifting E to $\mathbf{R}^r \subseteq \mathbf{C}^r$ we obtain there a set, also denoted by E. We fix a basis $v^{(1)}$, $v^{(2)}, \ldots, v^{(r)}$ of $\mathbf{C}^r$ having the properties stated in Lemma 3.4. The matrix U, built by the column vectors $v^{(1)}$, $v^{(2)}, \ldots, v^{(r)}$, is the connecting link between the representations of vectors and of transformations relative to the standard basis of $\mathbf{C}^r$ and relative to the new one. The semigroup obtained from Σ by diagonalization is denoted by $\tilde{\Sigma}$; the matrices corresponding to $\sigma, \tau \in \Sigma$—by $\tilde{\sigma}, \tilde{\tau} \in \tilde{\Sigma}$. The set of vectors of coefficients of all the points of E with respect to the new basis is denoted by $\tilde{E}$. Evidently, $\tilde{E}$ is a closed, $\tilde{\Sigma}$-invariant subset of $\mathbf{C}^r$ containing 0 as a nonisolated point. We note, for subsequent use, that a point in $\mathbf{C}^r$ is actually in $\mathbf{R}^r$ iff in its representation with respect to the new basis $v^{(1)}, v^{(2)}, \dots, v^{(r)}$, any two coefficients, corresponding to two complex conjugate basis vectors, are conjugate themselves.

Our computations, aimed at showing that $E = \mathbf{T}^r$, will be done concerning the set $\tilde{E}$; the simple way $\tilde{\Sigma}$ acts on $\mathbf{C}^r$ makes this convenient. We shall prove that $\tilde{E}$ is sufficiently "big" to ensure that E, as a subset of $\mathbf{T}^r$, is the entire group.

$\tilde{E}$ is known to contain a sequence of nonzero points converging to 0. We intend to work in a nontrivial $\tilde{\Sigma}$-invariant subspace of $\mathbf{C}^r$, minimal with respect to the property of containing such a sequence of points of $\tilde{E}$. The following lemma proves that $\tilde{\Sigma}$-invariant subspaces of $\mathbf{C}^r$ are of an extremely simple character.

LEMMA 4.1. *A subspace V of $\mathbf{C}^r$ is $\tilde{\Sigma}$-invariant iff it is spanned by some subset of the standard basis.*

The if part of the lemma follows immediately from $\tilde{\Sigma}$ being in diagonal form. For the opposite direction it is only necessary to make use of the fact that there exists a $\tilde{\sigma} \in \tilde{\Sigma}$ with its diagonal elements mutually distinct; a subspace, invariant under such a transformation, is easily shown to be of the required form.

The vectors of the standard basis of $\mathbf{C}^r$ are denoted by $e^{(i)}$, $1 \leqslant i \leqslant r$, where $e^{(1)} = (1, 0, \dots, 0)^T$, etc.

Without loss of generality we assume that the subspace, spanned by the first k ($\geqslant 1$) vectors of the standard basis, to be denoted by V_k, is a minimal, nonzero, $\tilde{\Sigma}$-invariant subspace of $\mathbf{C}^r$, containing a sequence of nonzero points of $\tilde{E}$, converging to 0. Let $(u^{(m)})_{m=1}^{\infty}$ be such a sequence. We may assume that all the components of $u^{(m)}$ are nonzero for every m. Points of V_k will usually be denoted as k-dimensional vectors, omitting their last $(r - k)$ zero components. For the time being we work in $\mathbf{C}^r$ only with points belonging to V_k.

LEMMA 4.2. *Let $\sigma \in \Sigma$. Then either $|\lambda_{i,\sigma}| > 1$ for all $1 \leqslant i \leqslant k$ or $|\lambda_{i,\sigma}| \leqslant 1$ for all $1 \leqslant i \leqslant k$.*

PROOF. Assume, to the contrary, that for some $\sigma \in \Sigma$ we have, say, $|\lambda_{i,\sigma}| > 1$ for $1 \leqslant i \leqslant l$ and $|\lambda_{i,\sigma}| \leqslant 1$ for $l < i \leqslant k$, where $1 \leqslant l < k$. Let $N(\sigma) = \max_{1 \leqslant i \leqslant k} |\lambda_{i,\sigma}|$. For $a > 0$ consider the annular region

$$\mathfrak{R}_a = \left\{ (z_1, \dots, z_k)^T \in V_k \,\middle|\, |z_i| \leqslant aN(\sigma) \; \forall 1 \leqslant i \leqslant k, \; \max_{1 \leqslant i \leqslant k} |z_i| \geqslant a \right\}.$$

For all sufficiently large m there exists a positive integer j_m such that $\tilde{\sigma}^{j_m}(u^{(m)}) \in \mathfrak{R}_a$. Since $\mathfrak{R}_a$ is compact there is some limit point $w = w(a)$ of this sequence. w belongs to $\mathfrak{R}_a$ and hence it is nonzero. Since $\tilde{E}$ is $\tilde{\sigma}$-invariant and closed we have $w \in \tilde{E}$. Finally, our assumption concerning the eigenvalues of σ implies that $w \in V_l$.

Applying the same construction to a sequence $(a_j)_{j=1}^{\infty}$ decreasing to 0, instead of to a single number a, we obtain a sequence $(w^{(j)})_{j=1}^{\infty}$ of nonzero points in $\tilde{E}$

converging to 0, each point in which lies in V_l. But this, contradicting the minimality property of V_k, proves the lemma.

The former lemmas enable us to prove that quite a number of semigroups possess the property under investigation, namely that a closed, invariant set containing 0 as a nonisolated point, is necessarily the whole group.

EXAMPLE 4.1. Let Σ be the semigroup of endomorphisms of $\mathbf{T}^2$ generated by $\sigma = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. We have $\lambda_{1,\sigma} = \lambda_{2,\sigma} = 2$, $\lambda_{1,\tau} = (1+\sqrt{5})/2$ and $\lambda_{2,\tau} = (1-\sqrt{5})/2$. Since all the eigenvalues are real, we can diagonalize Σ over $\mathbf{R}$. Since $(1+\sqrt{5})/2 > 1$ while $|(1-\sqrt{5})|/2 < 1$, Lemma 4.2 proves that E contains a sequence of points converging to 0 lying on one of the two characteristic lines of Σ. Since on such a line the points of E form a set invariant under multiplication by 2 and by $(1+\sqrt{5})/2$ (or $(1-\sqrt{5})/2$), the problem is actually reduced to a one-dimensional one. Since the numbers 2 and $(1+\sqrt{5})/2$ (as well as the numbers 2 and $(1-\sqrt{5})/2$) are readily seen to be rationally independent, the ideas of [**1**, Lemmas IV.1–IV.2] can be adopted for our case to prove that E contains one-half of one of the characteristic lines. Since both lines are of irrational slopes, they are dense in $\mathbf{T}^2$, whence $E = \mathbf{T}^2$.

Lemma 4.2 and the fact that for each $1 \leqslant i \leqslant r$ there is some $\sigma \in \Sigma$ with $|\lambda_{i,\sigma}| > 1$ imply together the existence of some $\sigma \in \Sigma$ for which

$$|\lambda_{i,\sigma}| > 1, \qquad 1 \leqslant i \leqslant k. \tag{4.1}$$

LEMMA 4.3. *If $\sigma \in \Sigma$ satisfies* (4.1) *then there exists some point $u^{(0)} \in \tilde{E}$, all of whose coordinates are nonzero, such that the sequence defined by*

$$u^{(n)} = \tilde{\sigma}^{-n}(u^{(0)}), \qquad n \geqslant 0, \tag{4.2}$$

forms a sequence of points in $\tilde{E}$ which approaches 0.

PROOF. The same construction as the one applied in the proof of Lemma 4.2 enables us to find a point $u^{(0)} \in \tilde{E}$, a sequence $(\bar{u}^{(m)})_{m=1}^{\infty}$ of points in $\tilde{E}$ converging to 0 and a sequence $(j_m)_{m=1}^{\infty}$ of positive integers such that $\tilde{\sigma}^{j_m}(\bar{u}^{(m)}) \underset{m\to\infty}{\to} u^{(0)}$.

Obviously, j_m tends to infinity with m. Hence, for every n, the sequence $(u^{m,n})_{m=1}^{\infty}$ defined by

$$u^{m,n} = \tilde{\sigma}^{j_m - n}(\bar{u}^{(m)}), \qquad m \geqslant 1,$$

belongs to $\tilde{E}$ for sufficiently large m. Since the sequence converges to $\tilde{\sigma}^{-n}(u^{(0)})$, the lemma is established.

LEMMA 4.4. *If $\sigma, \tau \in \Sigma$ then*

$$\log|\lambda_{i,\tau}|/\log|\lambda_{i,\sigma}| = \alpha, \qquad 1 \leqslant i \leqslant k, \tag{4.3}$$

for some α, dependent on σ and τ, but not on i (*if the denominator vanishes for some i then it vanishes for every i*).

PROOF. It is sufficient to establish (4.3) for some fixed $\sigma \in \Sigma$ and all $\tau \in \Sigma$. Hence we may assume that σ satisfies (4.1). We may also assume that σ satisfies (4.1). In fact, for a sufficiently large m the endomorphism $\sigma^m\tau$ satisfies (4.1), and once (4.3) is established for $\sigma^m\tau$ instead of for τ, it follows for τ as well.

Suppose, to the contrary, that, for example,

$$\begin{aligned} &\log|\lambda_{i,\tau}|/\log|\lambda_{i,\sigma}| = \alpha, \qquad 1 \leqslant i \leqslant l, \\ &\log|\lambda_{i,\tau}|/\log|\lambda_{i,\sigma}| < \alpha, \qquad l < i \leqslant k, \end{aligned} \tag{4.4}$$

for some $1 \leqslant l < k$.

For every nonnegative integer h consider the sequence $(w^{j,h})_{j=h}^{\infty}$ of points in $\tilde{E}$ defined by

$$w^{j,h} = \tilde{\tau}^{j-h}(u^{([j\alpha])}) \tag{4.5}$$

where $(u^{(n)})_{n=0}^{\infty}$ is a sequence satisfying the conditions of Lemma 4.3. (For a real number x we denote by $[x]$ and $\{x\}$ its integral part and its fractional part, respectively.)

For suitable real numbers β_i and γ_i, $1 \leqslant i \leqslant k$, we can decompose the eigenvalues of σ and τ into

$$\begin{aligned} \lambda_{i,\sigma} &= |\lambda_{i,\sigma}| \cdot e(\beta_i), \qquad 1 \leqslant i \leqslant k, \\ \lambda_{i,\tau} &= |\lambda_{i,\tau}| \cdot e(\gamma_i), \qquad 1 \leqslant i \leqslant k, \end{aligned} \tag{4.6}$$

where $e(x) \equiv e^{2\pi i x}$ for $x \in \mathbf{R}$. Denoting by v_i, $1 \leqslant i \leqslant k$, the components of the vector $v \in V_k$, we obtain by (4.4) for some positive numbers ε_i, $1 \leqslant i \leqslant k$,

$$\begin{aligned} w^{j,h} &= \tilde{\tau}^{j-h}\tilde{\sigma}^{-[j\alpha]}(u^{(0)}) = \sum_{i=1}^{k} \lambda_{i,\tau}^{j-h}\lambda_{i,\sigma}^{-[j\alpha]}u_i^{(0)}e^{(i)} \\ &= \sum_{i=1}^{k} |\lambda_{i,\tau}|^{j-h}e((j-h)\gamma_i)|\lambda_{i,\sigma}|^{-[j\alpha]}e(-[j\alpha]\beta_i)u_i^{(0)}e^{(i)} \\ &= \sum_{i=1}^{l} |\lambda_{i,\tau}|^{-h}|\lambda_{i,\sigma}|^{\{j\alpha\}}e((j-h)\gamma_i - [j\alpha]\beta_i)u_i^{(0)}e^{(i)} \\ &\quad + \sum_{i=l+1}^{k} |\lambda_{i,\tau}|^{-j\varepsilon_i - h}|\lambda_{i,\sigma}|^{\{j\alpha\}}e((j-h)\gamma_i - [j\alpha]\beta_i)u_i^{(0)}e^{(i)}. \end{aligned} \tag{4.7}$$

The sequence $(w^{j,h})_{j=h}^{\infty}$ is now immediately seen to be bounded for every h. Let $w^{(h)}$ be some limit point of the sequence. Obviously, $w^{(h)} \in V_l$. Since $u_i^{(0)} \neq 0$ for all $1 \leqslant i \leqslant k$, $w^{(h)}$ is nonzero. Finally, $(w^{(h)})_{h=1}^{\infty}$ is a sequence of points in $\tilde{E}$, converging to 0. This contradicts the minimality property of V_k, which proves the lemma.

EXAMPLE 4.2. The last lemma is sufficient to reduce the problem to the one-dimensional case for a large number of commutative semigroups. In fact, V_k is one-dimensional unless for some i and j the ratio $\log|\lambda_{i,\sigma}|/\log|\lambda_{j,\sigma}|$ is the same for all $\sigma \in \Sigma$. Suppose Σ is generated by two commuting, rationally independent endomorphisms σ and τ, f_{σ^n} being irreducible over $\mathbf{Z}$ for all n. In case all eigenvalues are real, it is unclear whether an equality of the form

$$\log\lambda_{i,\sigma}/\log\lambda_{j,\sigma} = \log\lambda_{i,\tau}/\log\lambda_{j,\tau}$$

can occur. (We dispose of the absolute value signs by passing to σ^2 and τ^2 if necessary.) At any rate, if no such equality is satisfied, we can show, as indicated in Example 4.1, that E contains one-half of one of the characteristic lines. It can be shown that, due to the irreducibility of f_σ, the projection of such a ray on $\mathbf{T}^r$ is necessarily dense, whence $E = \mathbf{T}^r$.

Returning to the general case, we are now going to prove that $\tilde{E}$ contains an arc of a "nice" curve of a very definite character.

LEMMA 4.5. *Let $\sigma \in \Sigma$ satisfy* (4.1). *There are integers $l_0 \geqslant 0, l_1, \ldots, l_k$, not all zero, and a positive number t' such that the vector $w^{(t)}$ defined by*

$$w^{(t)} = \sum_{i=1}^{k} |\lambda_{i,\sigma}|^{l_0 t} e(l_i t + l_0 t \beta_i) u_i^{(0)} e^{(i)} \tag{4.8}$$

belongs to $\tilde{E}$ for every $t \in [0, t']$. (*Here $u^{(0)}$ is as in Lemma* 4.3 *and $\beta_1, \beta_2, \ldots, \beta_k$ are given through* (4.6).)

PROOF. Let $\tau \in \Sigma$ be rationally independent of σ. We may assume that τ satisfies (4.1). In fact, for some sufficiently large m the endomorphism $\sigma^m(\tau)$ satisfies (4.1) and is also rationally independent of σ. Hence, $\sigma^m \tau$ may be chosen instead of τ.

We now consider the sequence $(w^{(j)})_{j=0}^{\infty}$, which arises from the class of sequences $(w^{j,h})_{j=h}^{\infty}$, defined by (4.5), in the special case $h = 0$:

$$w^{(j)} = \tilde{\tau}^j(u^{([j\alpha])}).$$

By Lemma 4.4, (4.7) reads

$$\begin{aligned} w^{(j)} &= \sum_{i=1}^{k} |\lambda_{i,\sigma}|^{\{j\alpha\}} e(j\gamma_i - [j\alpha]\beta_i) u_i^{(0)} e^{(i)} \\ &= \sum_{i=1}^{k} |\lambda_{i,\sigma}|^{\{j\alpha\}} e(\{j(\gamma_i - \alpha\beta_i)\}) e(\{j\alpha\}\beta_i) u_i^{(0)} e^{(i)}. \end{aligned} \tag{4.9}$$

The rational independence of σ and τ implies that the vector $(\{\alpha\}, \{\gamma_1 - \alpha\beta_1\}, \ldots, \{\gamma_k - \alpha\beta_k\})$, considered as an element of $\mathbf{T}^{k+1}$, is not a torsion element. In fact, assume it is of finite order. Then, in particular, for suitable integers p, q, p_1, q_1 we have $\alpha = p/q$ and $\gamma_1 - \alpha\beta_1 = p_1/q_1$. Hence by (4.3) and (4.6) we obtain $\lambda_{1,\sigma}^{pq_1} = \lambda_{1,\tau}^{qq_1}$. But this implies $\sigma^{pq_1} = \tau^{qq_1}$, contradicting the rational independence of σ and τ. Thus, the element in question is a torsion element.

The closure of the set $\{x^n \mid n \in \mathbf{N}\}$, x being an element of a given compact group, forms a subgroup. Every infinite closed subgroup of $\mathbf{T}^{k+1}$ contains a connected one-dimensional subgroup, the form of which is $\{(\{l_0 t\}, \{l_1 t\}, \ldots, \{l_k t\}) \mid 0 \leqslant t < 1\}$, where $l_0, l_1, \ldots, l_k$ are integers, not all zero, and we may assume that $l_0 \geqslant 0$. Hence, since $\tilde{E}$ is closed and $w^{(j)} \in \tilde{E}$ for all j, the equality (4.9) proves the lemma.

Let us now summarize what we have achieved up to this point and describe the strategy to be applied in the following. Starting with a set $\tilde{E}$, known to be closed and $\tilde{\Sigma}$-invariant and to contain 0 as a nonisolated point, we proved that $\tilde{E}$ contains an arc of a "nice" curve. (The curve is elliptical in case $l_0 = 0$ and spiral in case $l_0 > 0$.) From now on we use only this arc and its images under large powers of an endomorphism satisfying (4.1). We want to establish the existence of arbitrarily long subarcs of these images, which are "almost straight". Returning to $\mathbf{T}^r$, E will prove to contain such arcs as well. Passing to the limit, we shall find in E a translate of some infinite subgroup of $\mathbf{T}^r$. Having such exact information, we shall be able to show that the set E is the whole of $\mathbf{T}^r$.

We note that, in some sense, the way we adopt may seem excessively lengthy. In fact, in course of the proof of Lemma 4.5 we were content to find some one-dimensional subgroup in the closure of the set $\{(\{j\alpha\}, \{j(\gamma_1 - \alpha\beta_1)\}, \dots, \{j(\gamma_k - \alpha\beta_k)\}) \mid j = 0, 1, 2, \dots\}$. The group actually generated may be much larger. The reason for not attempting to use the entire group is the difficulty of characterizing it. At any rate, in some cases this group is in fact exactly one-dimensional.

Example 4.3. Let Σ be generated by $\sigma = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 1 & 4 \\ -1 & 3 \end{smallmatrix}\right)$. The eigenvalues of τ are $2 \pm i\sqrt{3}$. Since the components of each real vector with respect to the basis $v^{(1)}$, $v^{(2)}$ are conjugate, such a vector is uniquely determined by its first component. The subset of $\mathbf{C}$, formed by taking for each vector in E its first component, contains 0 as a nonisolated point and is invariant under multiplication by 2 and $2 + i\sqrt{3}$. From the proof of Lemma 4.5 it can be seen that, unless the three numbers 1, $\log_2 \sqrt{7}$, $(2\pi)^{-1}\arctan\sqrt{3/2}$ are linearly dependent over $\mathbf{Q}$, the set in question is $\mathbf{C}$ itself, which implies that $E = \mathbf{T}^2$. Since an attempt at characterizing for every case the exact subset of $\mathbf{C}$ obtained in this way seems impracticable, we are content to know that E contains in this case an arc of a spiral.

As another example, let Σ be generated by $\sigma = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 5 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 3 & -4 \\ 4 & 3 \end{smallmatrix}\right)$. We have $\lambda_{1,\tau} = 3 + 4i$ and $\lambda_{2,\tau} = 3 - 4i$, so that the eigenvalues of both σ and τ are of modulus 5. Here, the resulting subset of $\mathbf{C}$ contains 0 as a nonisolated point and is invariant under multiplication by 5 and by $3 + 4i$. Such a set is not necessarily $\mathbf{C}$ itself. The union of all circles, whose centers are at the origin and whose radii are of the form 5^k, k an arbitrary integer, is an example of a set having these properties.

Let us return to the general case. A set A in a metric space (X, d) forms an *ε-net* for the set B if for every $b \in B$ there exists an $a \in A$ such that $d(a, b) < \varepsilon$. With this definition we state

Lemma 4.6. *For every $\varepsilon > 0$, $\tilde{E}$ forms an ε-net for arbitrarily long line segments in V_k.*

Proof. We start with an endomorphism σ satisfying (4.1) and an arc $\{w^{(t)} \mid 0 \leqslant t \leqslant t'\}$ in $\tilde{E}$, as given by Lemma 4.5. We shall use images of this arc under high powers of $\tilde{\sigma}$ and show that they form ε-nets for long line segments. Define, therefore,

$$w^{m,t} = \tilde{\sigma}^m(w^{(t)}), \qquad 0 \leqslant t \leqslant t', m = 0, 1, 2, \dots.$$

By (4.8) we have

$$w^{m,t} = \sum_{j=1}^{k} \lambda_{j,\sigma}^m |\lambda_{j,\sigma}|^{l_0 t} e\big(l_j t + l_0 t\beta_j\big) u_j^{(0)} e^{(j)}.$$

To obtain a line segment for which the arc $\{w^{m,t} \mid 0 \leqslant t \leqslant t'\}$ is a good approximation, we naturally select the segment formed by taking the linear part of that arc (expanding $w^{m,t}$ into a power series in t). Hence we define

$$v^{m,t} = \sum_{j=1}^{k} \lambda_{j,\sigma}^m \big(1 + l_0 t \ln |\lambda_{j,\sigma}| + 2\pi i\big(l_j + l_0\beta_j\big)t\big) u_j^{(0)} e^{(j)}, \tag{4.10}$$

$$0 \leqslant t \leqslant t', m = 0, 1, 2, \dots.$$

First we want to examine how closely $w^{m,t}$ approximates $v^{m,t}$:

$$w_j^{m,t} - v_j^{m,t} = \lambda_{j,\sigma}^m\Big(\exp\big(l_0 t\ln|\lambda_{j,\sigma}| + 2\pi i(l_j + l_0\beta_j)t\big) \\ -1 - l_0 t\ln|\lambda_{j,\sigma}| - 2\pi i\big(l_j + l_0\beta_j\big)t\Big)\cdot u_j^{(0)}, \qquad 1 \leqslant j \leqslant k.$$

It is easily seen that

$$|\exp(z) - 1 - z| \leqslant |z|^2\exp(|z|)/2, \qquad z \in \mathbf{C}.$$

Hence

$$|w_j^{m,t} - v_j^{m,t}| \leqslant |\lambda_{j,\sigma}|^m c_j^2 t^2 \exp(c_j t)\cdot|u_j^{(0)}|/2 \\ \leqslant c_j' t^2 |\lambda_{j,\sigma}|^m, \qquad 1 \leqslant j \leqslant k,$$

where

$$c_j = \Big(\big(l_0\ln|\lambda_{j,\sigma}|\big)^2 + \big(2\pi(l_j + l_0\beta_j)\big)^2\Big)^{1/2}, \quad c_j' = c_j^2\exp(c_j t')\cdot|u_j^{(0)}|/2.$$

Suppose, for example, that $|\lambda_{1,\sigma}|$ is maximal among all the $|\lambda_{j,\sigma}|$, $1 \leqslant j \leqslant k$. Using some norm $\|\cdot\|$ on V_k, we obtain for some c, independent of t and m,

$$\text{(4.11)} \qquad \|w^{m,t} - v^{m,t}\| \leqslant ct^2|\lambda_{1,\sigma}|^m, \qquad 0 \leqslant t \leqslant t', m = 0,1,2,\ldots.$$

The expression appearing on the right-hand side of (4.11) is quite large if m is large, unless t is restricted to be small. Hence, we take only the partial arcs

$$\tilde{\mathfrak{S}}^{(m)} = \{w^{m,t} | 0 \leqslant t \leqslant t_m\} \subseteq E, \qquad m = 0,1,2,\ldots,$$

and the corresponding line segments

$$\tilde{\mathfrak{J}}^{(m)} = \{v^{m,t} | 0 \leqslant t \leqslant t_m\} \subseteq V_k, \qquad m = 0,1,2,\ldots.$$

For every $\varepsilon > 0$, we want the set $\tilde{\mathfrak{S}}^{(m)}$ to form an ε-net for the set $\tilde{\mathfrak{J}}^{(m)}$ for sufficiently large m. In view of (4.11) a sufficient condition for this is

$$\text{(4.12)} \qquad t_m^2|\lambda_{1,\sigma}|^m \underset{m\to\infty}{\to} 0.$$

It is also desired that the length of $\tilde{\mathfrak{J}}^{(m)}$ will tend to infinity with m. Let $\mathfrak{J}(0, r, e)$ denote the line segment whose center is at 0, of radius r and in the same direction as the unit vector e, that is,

$$\mathfrak{J}(0, r, e) = \{0 + te \,|\, |t| \leqslant r\}.$$

Let $\tilde{\mathfrak{J}}^{(m)} = \mathfrak{J}(\tilde{0}^{(m)}, \tilde{r}^{(m)}, \tilde{e}^{(m)})$, $m = 0,1,2,\ldots$. By (4.10) we have, for some $d > 0$, $\tilde{r}^{(m)} \geqslant dt_m|\lambda_{1,\sigma}|^m$. (Actually, this is true only if l_0 and l_1 are not both zero. If $l_0 = 0$ then we have to choose among all indices j, for which $l_j \neq 0$, that j for which $|\lambda_{j,\sigma}|$ is maximal. Both (4.11) and the last inequality are seen to hold with that j. Alternatively, we observe that, in the proof of Lemma 4.5, l_0, $l_1,\ldots,l_k$ could have been chosen with l_0 and l_1 not both zero.)

Hence we need also

$$\text{(4.13)} \qquad t_m|\lambda_{1,\sigma}|^m \underset{m\to\infty}{\to} \infty.$$

Now, there is no difficulty in choosing $(t_m)_{m=0}^{\infty}$ in such a way that both (4.12) and (4.13) hold. For example, $t_m = |\lambda_{1,\sigma}|^{-3m/4}$.

The line segments $\tilde{\mathfrak{J}}^{(m)}$, $m \geqslant 0$, satisfy the conditions of the lemma.

PROPOSITION 4.1. *For every $\varepsilon > 0$, E forms an ε-net for arbitrarily long line segments in $\mathbf{R}^r$.*

PROOF. Instead of the sets $\tilde{\mathfrak{S}}^{(m)}$ and $\tilde{\mathfrak{J}}^{(m)}$, $m \geqslant 0$, used in the proof of Lemma 4.6, we now take the sets $\mathfrak{S}^{(m)}$ and $\mathfrak{J}^{(m)}$, which are the corresponding sets before the diagonalization, i.e. $\mathfrak{S}^{(m)} = U(\tilde{\mathfrak{S}}^{(m)})$, $\mathfrak{J}^{(m)} = U(\tilde{\mathfrak{J}}^{(m)})$, $m \geqslant 0$ (U being the matrix built of the basis vectors $v^{(1)}, v^{(2)}, \ldots, v^{(r)}$, represented relative to the standard basis).

Since U is nonsingular there exist constants $a_2 > a_1 > 0$ such that

$$a_1\|u^{(2)} - u^{(1)}\| \leqslant \|U(u^{(2)}) - U(u^{(1)})\| \leqslant a_2\|u^{(2)} - u^{(1)}\|, \qquad u^{(1)}, u^{(2)} \in \mathbf{C}^r.$$

The left inequality shows that the lengths of the segments $\mathfrak{J}^{(m)}$ tend to infinity with m; the right one that for every $\varepsilon > 0$, $\mathfrak{S}^{(m)}$ forms an ε-net for $\mathfrak{J}^{(m)}$ for sufficiently large m.

The only point yet to be proved is that the segments $\mathfrak{J}^{(m)}$, $m \geqslant 0$, are contained in $\mathbf{R}^r$. According to the remarks at the outset of this section, we need only verify that if, for example, $v^{(2)} = \overline{v^{(1)}}$, then $v_2^{m,t} = \overline{v_1^{m,t}}$. But if $v^{(2)} = \overline{v^{(1)}}$ then $\lambda_{2,\sigma} = \overline{\lambda_{1,\sigma}}$ and $u_2^{(0)} = \overline{u_1^{(0)}}$ Now we see that in (4.6) we can take $\beta_2 = -\beta_1$ and $\gamma_2 = -\gamma_1$ (since (4.6) determines these numbers only modulo 1). The construction of the group $\{(\{l_0 t\}, \{l_1 t\}, \ldots, \{l_k t\}) \mid 0 \leqslant t \leqslant t'\}$ in the proof of Lemma 4.5 shows then that $l_2 = -l_1$. By (4.10) we finally have $v_2^{m,t} = \overline{v_1^{m,t}}$. Hence the segment $\mathfrak{J}^{(m)}$ may indeed be assumed to lie in $\mathbf{R}^r$, which completes the proof.

PROPOSITION 4.2. *E contains a translate of some infinite, closed subgroup of $\mathbf{T}^r$.*

PROOF. Let the sequence of line segments, the existence of which was established in Proposition 4.1, be given by $\mathfrak{J}^{(m)} = \mathfrak{J}(0^{(m)}, r^{(m)}, z^{(m)})$, $m = 0, 1, 2, \ldots$.

Let π denote the natural projection of $\mathbf{R}^r$ on $\mathbf{T}^r$. By the compactness of $\mathbf{T}^r$ and of the unit sphere $\mathbf{S}^{r-1}$ in $\mathbf{R}^r$ we may assume, passing to a subsequence if necessary, that

$$\pi(0^{(m)}) \underset{m\to\infty}{\to} 0' \in \mathbf{T}^r, \quad r^{(m)} \underset{m\to\infty}{\to} \infty, \quad z^{(m)} \underset{m\to\infty}{\to} z' \in \mathbf{S}^{r-1}.$$

Now we claim that the line passing through $0'$ and in the same direction as z', which may be denoted by $\mathfrak{J}(0', \infty, z')$, is contained in E. In fact, given any point in $\mathfrak{J}(0', \infty, z')$, there are points arbitrarily close to it in $\mathfrak{J}^{(m)}$ for sufficiently large m. Since E is closed and contains points arbitrarily close to these, it contains the whole line $\mathfrak{J}(0', \infty, z')$.

The proposition follows now from the fact that the closure of a line in $\mathbf{T}^r$ is a translate of some subgroup of $\mathbf{T}^r$.

The former results in this section were independent of the fact that Σ contains an endomorphism σ with f_{σ^n} irreducible over $\mathbf{Z}$ for all n. Only the much weaker property of Σ being diagonalizable was assumed. Thus, Proposition 4.2 holds, for example, for the semigroup generated by $\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)$, which is obviously not an

ID semigroup. Now we have to utilize the existence of such a σ in Σ, but first we need the following

LEMMA 4.7. *Let G be a compact, abelian, metric group and let Γ be the dual group. A sequence $(G_m)_{m=1}^{\infty}$ of closed subgroups of G satisfies $G_m \underset{m\to\infty}{\to} G$ (in the Hausdorff metric) iff for every nonzero $\gamma \in \Gamma$ we have $\gamma \notin \mathrm{Ann}(G_m)$ for sufficiently large m (where $\mathrm{Ann}(H)$ denotes the annihilator in Γ of a closed subgroup H of G).*

PROOF. The "only if" part is trivial, so we turn to prove the "if" part.

To prove that $G_m \underset{m\to\infty}{\to} G$ it is certainly sufficient to show that $\mu_m \underset{m\to\infty}{\to} \mu$ in the weak topology of measures, where μ_m and μ denote the Haar measures of G_m and G, respectively. Since Γ is discrete, this is equivalent to showing that

$$(4.14)\qquad \int_G \gamma(x)\,d\mu_m(x) \underset{m\to\infty}{\to} \int_G \gamma(x)\,d\mu(x) \quad \forall\gamma\in\Gamma.$$

Let ν be either one of the μ_m, $m \in \mathbf{N}$, or μ. Then

$$\int_G \gamma(x)\,d\nu(x) = \int_{\mathbf{T}} z\,d(\nu\circ\gamma^{-1})(z).$$

(Here $\mathbf{T}$ is the unit circle in the complex plane.) The measure $\nu\circ\gamma^{-1}$, induced by ν on the subgroup $\gamma(G)$ of $\mathbf{T}$, is clearly a translation-invariant measure on $\gamma(G)$, whence it is the Haar measure of $\gamma(G)$. It follows that, unless the restriction of γ to G_m is the trivial character, the integral on the left-hand side of (4.14) vanishes. But the conditions of the lemma guarantee that if γ is nontrivial on G, then for sufficiently large m its restriction to G_m is nontrivial as well. Thus (4.14) holds, which proves the lemma.

We shall have to apply the lemma during the proof of the next proposition. The dual group of $\mathbf{T}^r$ is $\mathbf{Z}^r$, the points of which are regarded as row vectors $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_r)$. The action of γ on a point $x = (x_1, x_2, \ldots, x_r)^T$ in $\mathbf{T}^r$ is given by $\gamma(x) = e(\sum_{j=1}^r \gamma_j x_j)$.

PROPOSITION 4.3. *Let σ be an endomorphism of $\mathbf{T}^r$ such that f_{σ^n} is irreducible over $\mathbf{Z}$ for every positive integer n, and let H be an infinite closed subgroup of $\mathbf{T}^r$. Then there exists a sequence $(m_l)_{l=1}^{\infty}$ of positive integers such that $\sigma^{m_l}(H) \underset{l\to\infty}{\to} \mathbf{T}^r$.*

PROOF. In view of Lemma 4.7 it is sufficient to establish the existence of a sequence (m_l) such that for every nonzero $\gamma \in \mathbf{Z}^r$ we have $\gamma \notin \mathrm{Ann}(\sigma^{m_l}(H))$ for sufficiently large l. Suppose, to the contrary, that no such sequence exists. Then there exists a finite set of nonzero characters $\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(s)}$ such that for every positive integer m we have $\gamma \in \mathrm{Ann}(\sigma^m(H))$ for some i. In other words, every positive integer belongs to one of the following subsets of $\mathbf{N}$:

$$N_i = \{m \in \mathbf{N} \mid \gamma^{(i)} \in \mathrm{Ann}(\sigma^m(H))\}, \qquad 1 \leqslant i \leqslant s.$$

Consequently, by a well-known theorem of van der Waerden (see, for example, Khinchin **[2]**), there is some i_0, $1 \leqslant i_0 \leqslant s$, such that N_{i_0} contains arbitrarily long arithmetic progressions. In particular, for some positive integers a and d we have a, $a+d, \ldots, a+(r-1)d \in N_{i_0}$.

Let us denote the character $\gamma^{(i_0)}\sigma^a$ by γ' and the endomorphism σ^d by σ_d. Then, since $\gamma \in \mathrm{Ann}(\sigma^m(H))$ iff $\gamma\sigma^m \in \mathrm{Ann}(H)$, we have $\gamma'\sigma_d^j \in \mathrm{Ann}(H)$ for every $0 \leqslant j \leqslant r-1$. This implies that for some integers $l_0, l_1, \ldots, l_{r-1}$, not all of which are zero, we have

$$(4.15) \qquad l_0\gamma' + l_1\gamma'\sigma_d + \cdots + l_{r-1}\gamma'\sigma_d^{r-1} = 0.$$

In fact, since H is infinite and isomorphic with the dual of $\mathbf{Z}^r/\mathrm{Ann}(H)$, $\mathrm{Ann}(H)$ is not of finite index in $\mathbf{Z}^r$. Hence $\mathrm{Ann}(H)$ is of rank not exceeding $r-1$.

Now, (4.15) implies that the matrix $\Sigma_{j=0}^{r-1} l_j\sigma_d^j$ is singular. The nontrivial polynomials $\Sigma_{j=0}^{r-1} l_j x^j$ and f_{σ_d} have, therefore, a nontrivial common divisor. Since f_{σ_d} is known to be irreducible, we have arrived at a contradiction, which proves the proposition.

It is a simple matter now to show that $E = \mathbf{T}^r$. By Proposition 4.2 we have $x + H \subseteq E$ for some point x in $\mathbf{T}^r$ and some infinite, closed subgroup H of $\mathbf{T}^r$. In view of Proposition 4.3 $\sigma^{m_l}(H) \underset{l\to\infty}{\to} \mathbf{T}^r$ for some sequence $(m_l)_{l=1}^{\infty}$, where σ is an endomorphism in Σ which satisfies the first condition in Theorem 2.1. Since $\sigma^{m_l}(x+H) = \sigma^{m_l}(x) + \sigma^{m_l}(H)$, we obviously have $\sigma^{m_l}(x+H) \underset{l\to\infty}{\to} \mathbf{T}^r$ as well. Since E is σ-invariant and closed, we arrive at the desired conclusion.

5. The sufficiency of the conditions. Throughout this section Σ denotes a commutative semigroup of endomorphisms of $\mathbf{T}^r$, satisfying the conditions of Theorem 2.1. We proceed to show that Σ satisfies the ID property. Here we mostly extend the ideas used in [**1**] for the one-dimensional case.

LEMMA 5.1. *If σ is an epimorphism of $\mathbf{T}^r$ then its kernel is a finite set of torsion elements of $\mathbf{T}^r$.*

PROOF. Since σ is an epimorphism, the matrix representing it is invertible over $\mathbf{Q}$. Let τ be the inverse matrix. Let l be the least common multiple of the denominators of all elements of τ. The matrix $l\tau$ is integer, hence an endomorphism of $\mathbf{T}^r$. Consequently, if some $x \in \mathbf{T}^r$ satisfies $\sigma(x) = 0$ then also $l\tau(\sigma(x)) = 0$, which amounts to $lx = 0$. Since there are only l^r points x in $\mathbf{T}^r$ satisfying $lx = 0$, the lemma follows.

LEMMA 5.2. *Let σ be an ergodic endomorphism of $\mathbf{T}^r$. A finite σ-invariant set is necessarily composed only of torsion elements.*

PROOF. Let E be a finite σ-invariant set and $x \in E$. For some integers $m > n > 0$ we have $\sigma^m(x) = \sigma^n(x)$, and hence $(\sigma^m - \sigma^n)(x) = 0$. In view of Lemma 5.1 it is sufficient, therefore, to show that $\sigma^m - \sigma^n$ is an epimorphism. Now, if $\lambda_1, \lambda_2, \ldots, \lambda_r$ are the eigenvalues of σ, then $\lambda_1^m - \lambda_1^n, \lambda_2^m - \lambda_2^n, \ldots, \lambda_r^m - \lambda_r^n$ are those of $\sigma^m - \sigma^n$. Since, by the ergodicity of σ, none of the eigenvalues of σ is either 0 or a root of unity, the eigenvalues of $\sigma^m - \sigma^n$ are all nonzero. Hence $\sigma^m - \sigma^n$ is an epimorphism, which implies the lemma.

LEMMA 5.3. *Σ has a subsemigroup Σ_0, generated by at most* $\max\{2, r\}$ *endomorphisms, which still satisfies the conditions of Theorem* 2.1.

Proof. The case $r = 1$ is trivial, so we consider only the case $r \geqslant 2$.

It is required to select r endomorphisms (or less) in Σ, generating a subsemigroup Σ_0 which satisfies the conditions in question. First, we take an endomorphism σ_1 with $f_{\sigma_1^n}$ irreducible over $\mathbf{Z}$ for all n. Next, we take additional endomorphisms $\sigma_2, \ldots, \sigma_k \in \Sigma$ such that, for every common eigenvector of Σ, at least one of the σ_i, $1 \leqslant i \leqslant k$, has a corresponding eigenvalue of modulus greater than unity.

We have, by now, at most r endomorphisms. To verify this it is necessary to show that σ_1 has some eigenvalue with modulus greater than unity. In fact, otherwise all the eigenvalues of σ_1 would lie on the unit circle, whence by [**3**, Theorem 2.1(i)] all of them would have been roots of unity. But we have noticed already that if $r \geqslant 2$ and $f_{\sigma_1^n}$ is irreducible for all n, then σ_1 has no roots of unity among its eigenvalues.

If we have less than r endomorphisms, then taking an endomorphism σ_{k+1} which is rationally independent of σ_1, the semigroup Σ_0 generated by σ_1, $\sigma_2, \ldots, \sigma_{k+1}$ evidently satisfies the conditions. If we have exactly r endomorphisms, no two of which are rationally independent (which is possible, for example, if $r = 2$ and the selected endomorphisms are an automorphism σ_1 and its inverse σ_1^{-1}), then we replace σ_r by $\sigma_r' = \sigma_r^m \tau$, where $\tau \in \Sigma$ is rationally independent of σ_1. σ_r' is rationally independent of σ_1. For sufficiently large m, the eigenvalues of σ_r', corresponding to eigenvalues of σ_r' of modulus greater than unity, have the same property themselves. Hence, the semigroup Σ_0 generated by $\sigma_1, \sigma_2, \ldots, \sigma_r'$ has the desired properties.

The basic step, formulated a little bit differently than in the original paper, is given in the following

Proposition [**1**, p. 45]. *Let Σ denote a commutative semigroup of endomorphisms of* $\mathbf{T}^r$. *We assume* (i) *that there exists some ergodic endomorphism σ in Σ, and* (ii) *that there exists a prime q with the property that all* $\det \sigma$, $\sigma \in \Sigma$, *are relatively prime to q. Then if M and B are closed Σ-invariant subsets of* $\mathbf{T}^r$ *and M is minimal with respect to these properties, $M + B = \mathbf{T}^r$ implies $B = \mathbf{T}^r$.*

The following proposition generalizes Proposition IV.2 of [**1**] to the r-dimensional case.

Proposition 5.1. *Let M be a Σ-minimal subset of* $\mathbf{T}^r$. *Then M is necessarily a finite set of torsion elements.*

Proof. In the proof of Proposition 3.2 it was noted that Σ contains an ergodic endomorphism. Hence, in view of Lemma 5.2, it is sufficient to prove that M is finite.

We want to apply the proposition cited from [**1**]. The first condition of that proposition is satisfied. As to the second condition, we select a subsemigroup Σ_0 of Σ which if finitely generated and still satisfies the conditions in Theorem 2.1, as is possible by Lemma 5.3. Σ_0 satisfies both conditions of the aforementioned proposition. Now, if we prove that the conclusion of our proposition holds for Σ_0, then it holds for Σ as well. In fact, M contains a Σ_0-minimal subset M_0, which is then a finite set of torsion elements. The set M, being Σ-minimal and containing a torsion element, is necessarily a finite set of torsion elements. Hence we may assume that Σ satisfies both conditions of the preceding proposition.

We have to show that M is finite. Suppose, to the contrary, that it is not. Then $M - M$ is a closed, Σ-invariant subset of $\mathbf{T}^r$, which contains 0 as a nonisolated point. Hence, by the results of §4, $M - M = \mathbf{T}^r$. Applying the preceding proposition, we obtain $M = \mathbf{T}^r$, which is impossible. The contradiction proves the proposition.

Now we can complete the proof of the sufficiency of the conditions in Theorem 2.1. Let E be an infinite, closed, Σ-invariant subset of $\mathbf{T}^r$. We proceed to show that $E = \mathbf{T}^r$. Let E' denote the set of all accumulation points of E. From Lemma 5.1 it follows that E' is Σ-invariant. E' contains a Σ-minimal subset M, and hence by Proposition 5.1 there exists some torsion element x in E'. Suppose x is of order l. Then lE is a closed, Σ-invariant subset of $\mathbf{T}^r$ which contains 0 as a nonisolated point. Hence $lE = \mathbf{T}^r$. This implies $(E + x^{(1)}) \cup (E + x^{(2)}) \cup \cdots \cup (E + x^{(l^r)}) = \mathbf{T}^r$ where $x^{(1)}, x^{(2)}, \ldots, x^{(l^r)} \in \mathbf{T}^r$ are the solutions of $lx = 0$. Since each of the sets $E + x^{(i)}$, $1 \leqslant i \leqslant l^r$, is closed, one of these sets has a nonempty interior. Hence E has a nonempty interior. Since Σ contains an ergodic endomorphism, this implies $E = \mathbf{T}^r$.

Thus the proof of Theorem 2.1 is complete.

6. Remarks. In this section we want to make a few remarks concerning the verification of the conditions of Theorem 2.1 for given semigroups, to note that "most" commutative semigroups satisfy these conditions, and to give a general example.

First we note that ID semigroups are not necessarily large. The following theorem is an immediate consequence of Theorem 2.1 and Lemma 5.3.

THEOREM 6.1. *Let Σ be a commutative semigroup of endomorphisms of $\mathbf{T}^r$ satisfying the ID property. There exists a subsemigroup Σ_0 of Σ, also satisfying the ID property, which is generated by at most* $\max\{2, r\}$ *endomorphisms.*

The first condition in Theorem 2.1, i.e. that there exists an endomorphism σ in Σ such that f_{σ^n} is irreducible over $\mathbf{Z}$ for every positive integer n, is a very weak one. In some sense, most polynomials in $\mathbf{Z}[x]$ are irreducible. If σ is an endomorphism such that f_σ is irreducible, then an endomorphism τ commuting with σ is uniquely determined by $\lambda_{1,\tau}$. Now, τ satisfies the desired property iff $\mathbf{Q}(\lambda^n_{1,\tau}) = K\ (= \mathbf{Q}(\lambda_{1,\sigma}))$ for all n. The proof of Proposition 3.1 shows that most numbers α in K satisfy $\mathbf{Q}(\alpha^n) = K$ for all n. In fact, all the other numbers belong to a finite union of finite group extensions of the multiplicative groups of the proper subfields of K. All that indicates that most endomorphisms satisfy the condition under consideration.

We also note that, given an endomorphism σ, it is possible effectively to determine whether f_{σ^n} is irreducible for every $n \in \mathbf{N}$. First, we observe that there exists some n' such that if f_{σ^n} is irreducible for all n, $1 \leqslant n \leqslant n'$, then it is irreducible for all $n \in \mathbf{N}$. In fact, suppose f_σ is irreducible but f_{σ^n} is reducible for some $n \geqslant 2$. Then it can be shown that f_{σ^n} has multiple roots. Hence for a certain pair of roots of f_σ, say λ_1 and λ_2, we have $(\lambda_1/\lambda_2)^n = 1$. The number λ_1/λ_2 is of a degree not exceeding $r(r-1)$ over $\mathbf{Q}$. Since the degree over $\mathbf{Q}$ of a primitive root of unity of order m is $\varphi(m)$ (φ being Euler's function), we can choose n' as a number such that $\varphi(m) > r(r-1)$ for all $m > n'$. (Evidently, such an n' can be found.) Finally, we recall that the question concerning the irreducibility of f_{σ^n} can be decided for each n separately (see, for example, van der Waerden [**5**, p. 77]).

Concerning the second condition of Theorem 2.1, we note that, since the product of the absolute values of all eigenvalues of an epimorphism is at least 1, "on the average" at least half of the eigenvalues lie outside the unit disc. Hence it should be easy to have for each of the common eigenvectors an endomorphism, the corresponding eigenvalue of which is of modulus greater than 1.

The third condition is, in some sense, the strongest. It asserts that the common objects of interest—semigroups and groups generated by only one endomorphism—never have the ID property. Yet, the proof of Proposition 3.2 shows that this condition is not much more restrictive than that.

We also note that, given two commuting endomorphisms σ and τ with f_σ irreducible over $\mathbf{Z}$, we can effectively determine whether they are rationally independent. First, suppose σ and τ are not automorphisms. If the two integers $\det \sigma$ and $\det \tau$ are rationally independent then the same holds for σ and τ as well. Assume, therefore, that $\det \sigma^l = \det \tau^m$. For σ and τ to be rationally dependent we must have $(\sigma^l \tau^{-m})^n = I$ for some positive integer n. Considerations used earlier in this section prove that a number n' can be found such that, if the last equality holds for some n at all, then it holds for some $n \leqslant n'$. Next, we turn to the case of automorphisms. The proof of Proposition 3.2 shows that the question concerning the rational dependence of σ and τ is equivalent to that of the rational dependence of the numbers $\lambda_{1,\sigma}$ and $\lambda_{1,\tau}$. Since these numbers are units, the effective Dirichlet unit theorem [**4**, Theorem 11.3.5] enables us to decide the last question.

We conclude with a general example of ID semigroups of $\mathbf{T}^r$.

EXAMPLE 6.1. Let σ be an endomorphism of $\mathbf{T}^r$ ($r \geqslant 2$) such that f_{σ^n} is irreducible for all n and let $l \geqslant 2$ be an integer. Then the commutative semigroup Σ generated by the two endomorphisms σ and lI satisfies the ID property. In fact, the first condition in Theorem 2.1 is satisfied by σ while the second is satisfied by lI. Since $f_{(lI)}k = (x - l^k)^r$ is reducible over $\mathbf{Z}$, σ and lI are rationally independent. Thus we have an ample supply of ID semigroups generated by just two endomorphisms.

REFERENCES

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

2. A. Y. Khinchin, *Three pearls of number theory*, Graylock Press, Baltimore, Md., 1952.

3. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN, Warsaw, 1974.

4. K. B. Stolarsky, *Algebraic numbers and diophantine approximations*, Dekker, New York, 1974.

5. B. L. van der Waerden, *Modern algebra*, vol. I, Ungar, New York, 1953.

INSTITUTE OF MATHEMATICS, THE HEBREW UNIVERSITY OF JERUSALEM, JERUSALEM, ISRAEL

Current address: Department of Mathematics, University of California, Los Angeles, California 90024