A Weyl-type equidistribution theorem in finite characteristic

V. Bergelson and A. Leibman

December 3, 2015

Abstract

We obtain a finite characteristic analogue of the classical Weyl theorem on the distribution of polynomial sequences in a finite dimensional torus.

0. Introduction

The goal of this paper is to obtain analogs, in finite characteristic, of the classical H. Weyl's results ([We]) on uniform distribution of the values of polynomial sequences in a finite dimensional torus.(1) Let F be a finite field of characteristic p; the following are the finite characteristic analogs of the classical objects which we will deal with:
- "the set of integers" is the ring $\mathcal{Z}=F[t]$ of polynomials $\sum_{i=0}^{r}a_it^i$, $a_i\in F$, over F;
- "the set of rationals" is the field $\mathcal{Q}=F(t)$ of rational functions over F, the quotient field of $\mathcal{Z}$;
- "the set of reals" is the field $\mathcal{R}=F((t^{-1}))$ of formal Laurent series $\sum_{i=r}^{-\infty}a_it^i=a_rt^r+a_{r-1}t^{r-1}+\ldots$, $a_i\in F$; $\mathcal{R}$ is the completion of $\mathcal{Q}$ with respect to the valuation $\nu(\alpha)=-r$ for $\alpha=\sum_{i=r}^{-\infty}a_it^i$ with $a_r\neq 0$;
- "the one-dimensional torus" is the group (and the $\mathcal{Z}$-module) $\mathcal{T}=\mathcal{R}/\mathcal{Z}$; the elements of $\mathcal{T}$ are representable by the series $\sum_{i=-1}^{-\infty}a_it^i$, $a_i\in F$;
- and finally, for $c\in\mathbb{N}$, "the c-dimensional torus" is $\mathcal{T}^c$. (2)

In this environment we are going to investigate the distribution of values of *polynomial $\mathcal{Z}$-sequences* $g(n)=\alpha_0+\alpha_1n+\ldots+\alpha_dn^d$, $n\in\mathcal{Z}$, with $\alpha_0,\alpha_1,\ldots,\alpha_d\in\mathcal{T}^c$, in the c-dimensional torus $\mathcal{T}^c$.

To trace the analogy between the classical setup and that of a finite characteristic, let us start with the case $d=1$. Let $\alpha=(\gamma_1,\ldots,\gamma_c)$ be an element of the conventional c-dimensional torus $\mathbb{T}^c=(\mathbb{R}/\mathbb{Z})^c$, and consider the "linear" sequence $\alpha n=(\gamma_1n,\ldots,\gamma_cn)$, $n\in\mathbb{Z}$, in $\mathbb{T}^c$. The following facts were established in [We]:

Supported by NSF grants DMS-0901106, DMS-1162073, and DMS-1500575.

(1) For a comprehensive discussion of advances of the theory of uniform distribution since the appearance of the groundbreaking paper [We] see [KuN] and [DrT].

(2) It seems that there is no stable notation for these objects in the literature. The ring $\mathcal{Z}=F[t]$ is often denoted by $GF[q,t]$, where $q=|F|$, and the field $\mathcal{R}=F((t^{-1}))$ by $GF\{q,t\}$. We have preferred to use the suggestive notation $\mathcal{Z}$, $\mathcal{Q}$, $\mathcal{R}$, and $\mathcal{T}$ to stress the analogy with the classical objects $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{T}$ respectively.

(i) The closure $\mathcal{O} = \overline{\{\alpha n\}}_{n\in\mathbb{Z}}$ of the sequence αn is a closed subgroup of $\mathbb{T}^c$, that is, a union of finitely many translates of a subtorus of $\mathbb{T}^c$. More precisely, $\mathcal{O} = S(\alpha) + K\alpha$, where $S(\alpha)$ is a subtorus and K is a finite subset of $\mathbb{Z}$.

(ii) The sequence αn is uniformly distributed in $\mathcal{O}$.

(iii) $\mathcal{O} = \mathcal{S}(\alpha) = \mathbb{T}^c$ iff the elements $\gamma_1, \ldots, \gamma_d$ are $\mathbb{Z}$-linearly independent.

As we will see, the statements (i), (ii), and (iii) can be transferred to the case of finite characteristic almost literally. We have, however, to adapt the notions of a subtorus and of the uniform distribution to our new setup. We will call an *S-subtorus* of $\mathcal{T}^c$ a linear image $\bigl\{\sum_{i=1}^b m_i x_i,\ x_1, \ldots, x_b \in \mathcal{T}\bigr\}$, with $m_1, \ldots, m_b \in \mathcal{Z}^c$, in $\mathcal{T}^c$ of a torus $\mathcal{T}^b$. (We use the prefix "S-" to distinguish this kind of subgroups of $\mathcal{T}^c$ from the "Φ-subtori", to be defined below.) As for the notion of uniform distribution, we replace it by a stronger notion of *well-distribution*: we say that a mapping $g\colon G \longrightarrow X$ from an abelian (or, more generally, an amenable) group G to a compact topological space X with a probability Borel measure μ is *well distributed in* X if $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} f(g(n)) = \int_X f\,d\mu$ for any $f \in C(X)$ and any Følner sequence(3) (Φ_N) in G. When X is $\mathcal{T}^c$ or a coset of a closed subgroup of $\mathcal{T}^c$, we will assume that X is equipped with the normalized Haar measure. We will also meet the situation where X is a finite union $X = \bigcup_{i=1}^k X_i$ of distinct cosets of a closed subgroup of $\mathcal{T}^c$ and the mapping $g\colon G \longrightarrow X$ is such that, for some subgroup H of G of finite index, for any coset $m + H$, $m \in G$, of H one has $g(m + H) \subset X_i$ for some i and the $\mathcal{Z}$-sequence $g(m + n)$, $n \in H$, is well distributed in X_i; in this case we say that *g is well distributed in the components of X*. Note that even in the case X is itself a closed subgroup of $\mathcal{T}^c$, "g is well distributed in the components of X" does not imply that "g is well distributed in X", because the cardinality of the set of the cosets of H that map to a component X_i of X may be different for distinct i (as for the sequence $\frac{1}{3}n^2 \bmod 1$), and in this case g is well distributed in X with respect to a measure μ that is a linear combination of the Haar measures on the components X_i and is different from the Haar measure on X.

The following result is the finite characteristic analogue of the linear case of Weyl's theory (cf. (i), (ii), (iii) above).

Theorem 0.1. *Let $\alpha = (\gamma_1, \ldots, \gamma_c) \in \mathcal{T}^c$. Then the $\mathcal{Z}$-sequence αn, $n \in \mathcal{Z}$, is well distributed in a subgroup of the form $\mathcal{S}(\alpha) + K\alpha$, where $\mathcal{S}(\alpha)$ is an S-subtorus of $\mathcal{T}^c$ and K is a finite subset of $\mathcal{Z}$, and one has $\mathcal{O} = \mathcal{S}(\alpha) = \mathbb{T}^c$ iff the elements $\gamma_1, \ldots, \gamma_c$ are $\mathcal{Z}$-linearly independent.*

A special case of this result was obtained by Carlitz in [C]. In his paper Carlitz introduced a notion of uniform distribution, which, in the contemporary terminology, is the uniform distribution with respect to the Følner sequence $\Phi_N = \{n \in \mathcal{Z} : \deg n \leq N\}$, $N = 1, 2 \ldots$, in $\mathcal{Z}$. It is shown in [C] that if $\gamma_1, \ldots, \gamma_c \in \mathcal{T}$ are $\mathcal{Z}$-linearly independent, then the $\mathcal{Z}$-sequence $(\gamma_1 n, \ldots, \gamma_c n)$, $n \in \mathcal{Z}$, is uniformly distributed in $\mathcal{T}^c$ in Carlitz's sense.

Let g be a polynomial sequence in the conventional c-dimensional torus $\mathbb{T}^c$, $g(n) =$

(3) A *Følner sequence* in a (discrete abelian) group G is a sequence $(\Phi_N)_{N=1}^\infty$ of finite subsets of G with $|(n + \Phi_N)\triangle\Phi_N|/|\Phi_N| \underset{N\to\infty}{\longrightarrow} 0$ for every $n \in G$. In $\mathcal{Z}$, the "most natural" Følner sequence is the sequence $\Phi_N = \{n \in \mathcal{Z} : \deg n \leq N\} = \{a_0 + a_1 t + \ldots + a_N t^N,\ a_i \in F\}$, $N \in \mathbb{N}$.

$\alpha_0+\alpha_1 n+\ldots+\alpha_d n^d$, $n\in\mathbb{Z}$, where $\alpha_0,\ldots,\alpha_d\in\mathbb{T}^c$. Weyl's theorem ([We]) says that the closure $\mathcal{O}(g)=\overline{g(\mathbb{Z})}$ of the range of this sequence is also a finite union of translates of a subtorus $S(g)$ of $\mathbb{T}^c$, $\mathcal{O}(g)=S(g)+g(K)$ where K is a finite subset of $\mathbb{Z}$, and that g is uniformly (and, actually, well) distributed in the components $S(g)+g(k)$, $k\in K$, of $\mathcal{O}(g)$. Moreover, the monomials of g "generate their subtori independently", in the sense that the torus $S(g)$ is the sum of the subtori generated by the distinct monomials of g: $S(g)=\sum_{i=1}^d S(\alpha_i)$. When $d<p$, a complete analogue of this theorem holds in characteristic p:

Theorem 0.2. *Let $g(n)=\alpha_0+\alpha_1 n+\ldots+\alpha_d n^d$, $n\in\boldsymbol{Z}$, with $\alpha_0,\alpha_1,\ldots,\alpha_d\in\boldsymbol{T}^c$, be a polynomial $\boldsymbol{Z}$-sequence in $\boldsymbol{T}^c$ of degree $d<p$. Then the closure $\mathcal{O}(g)=\overline{g(\boldsymbol{Z})}$ of $g(\boldsymbol{Z})$ has the form $\mathcal{S}(g)+g(K)$, where $\mathcal{S}(g)$ is the S-subtorus $\sum_{i=1}^d\mathcal{S}(\alpha_i)$ of $\boldsymbol{T}^c$ and K is a finite subset of $\boldsymbol{Z}$, and $g(n)$ is well distributed in the components $\mathcal{S}(g)+g(k)$, $k\in K$, of $\mathcal{O}(g)$. In particular, g is well distributed in $\boldsymbol{T}^c$ iff $\boldsymbol{T}^c=\sum_{i=1}^d\mathcal{S}(\alpha_i)$.*

A special case of Theorem 0.2, which says that if at least one of the coefficients $\alpha_1,\ldots,\alpha_d\in\boldsymbol{T}$ is irrational then the $\boldsymbol{Z}$-sequence $\alpha_0+\alpha_1 n+\ldots+\alpha_d n^d$ is uniformly distributed in $\boldsymbol{T}$ in Carlitz's sense, was established in [D2] (see also [D1] and [DM]). Our goal in this paper is to extend Theorem 0.2 to the case $\deg g>p$. In this situation additive polynomials[(4)] of higher degrees come into the game, namely those of the form $g(n)=\sum_{j=1}^l\alpha_j n^{p^j}$. The range $g(\boldsymbol{Z})$ of an additive polynomial $\boldsymbol{Z}$-sequence g is a subgroup of $\boldsymbol{T}^c$, and so is the closure $\mathcal{O}(g)=\overline{g(\boldsymbol{Z})}$; however, unlike the conventional tori, the torus $\boldsymbol{T}^c$ has a lot of closed subgroups which are not representable as a finite union of shifted S-subtori. We show that $\mathcal{O}(g)$ is always a finite union of translates of what we call *a Φ-subtorus*: a Φ-subtorus of $\boldsymbol{T}^c$ of level l and of dimension $\leq b$ is a subgroup of $\boldsymbol{T}^c$ of the form $\bigl\{\sum_{i=1}^b\sum_{j=0}^l m_{i,j}x_i^{p^j},\ (x_1,\ldots,x_b)\in\boldsymbol{T}^b\bigr\}$, with $m_{i,j}\in\boldsymbol{Z}^c$. It is also easy to see (see Section 7) that for any Φ-subtorus $\mathcal{F}$ of $\boldsymbol{T}^c$ there exists an additive polynomial $\boldsymbol{Z}$-sequence g in $\boldsymbol{T}^c$ such that $\mathcal{O}(g)=\mathcal{F}$. Though the definition of a Φ-subtorus looks similar to that of an S-subtorus, Φ-subtori are much more diverse in their structure[(5)], as the following examples show:

Examples. Let $F=\mathbb{Z}_2$. Let $\alpha=a_1t^{-1}+a_2t^{-2}+a_3t^{-3}+\ldots$, $a_i\in F$, be an irrational element of $\boldsymbol{T}$; then $\alpha^2=a_1t^{-2}+a_2t^{-4}+a_3t^{-6}+\ldots$ is also irrational.

1. For the $\boldsymbol{Z}$-sequences $g_1(n)=\alpha n$ and $g_1(n)=\alpha^2 n$ in $\boldsymbol{T}$ we have $\mathcal{O}(g_1)=\mathcal{O}(g_2)=\boldsymbol{T}$, whereas for the $\boldsymbol{Z}$-sequence $g_3(n)=\alpha^2n^2=(\alpha n)^2$ one has $\mathcal{O}(g_3)=\bigl\{x^2,\ x\in\boldsymbol{T}\bigr\}=\bigl\{u_1t^{-2}+u_2t^{-4}+u_3t^{-6}+\ldots,\ u_i\in F\bigr\}$.

2. For the $\boldsymbol{Z}$-sequence $g_4(n)=(\alpha n,\alpha^2n^2)$ in $\boldsymbol{T}^2$ we have $\mathcal{O}(g_4)=\bigl\{(x,x^2),\ x\in\boldsymbol{T}\bigr\}=\bigl\{\bigl(u_1t^{-1}+u_2t^{-2}+u_3t^{-3}+\ldots,u_1t^{-2}+u_2t^{-4}+u_3t^{-6}+\ldots\bigr),\ u_i\in F\bigr\}$.

(4) A mapping g is *additive* if it satisfies the identity $g(n+m)=g(n)+g(m)$ for all n,m, that is, is a group homomorphism with respect to addition.

(5) It may be of interest to investigate the geometrical structure of Φ-tori; for some information on this matter see [U].

3. For the $\mathscr{Z}$-sequence $g_5(n)=\alpha n+\alpha^2n^2$ in $\mathscr{T}$, $\mathcal{O}(g_5)=\{x+x^2,\ x\in\mathscr{T}\}=\mathscr{T}$, whereas for $g_6(n)=\alpha n+t\alpha^2n^2$, $\mathcal{O}(g_6)=\{u_2t^{-2}+u_3t^{-3}+u_4t^{-4}+\ldots,\ u_i\in F\}$, which is a subgroup of index 2 in $\mathscr{T}$.

Let us say that a monomial n^r is *separable* if r is not divisible by p; clearly, any polynomial $g(n)$ on $\mathscr{Z}$ can be written in the form $g(n)=\alpha_0+\sum_{i=1}^d\eta_i(n^{r_i})$ where $\eta_1,\ldots,\eta_d$ are additive polynomials and $n^{r_1},\ldots,n^{r_d}$ are separable monomials. The main result of this paper is the following general theorem:

Theorem 0.3. *Any additive polynomial $\mathscr{Z}$-sequence $\eta(n)$ in $\mathscr{T}^c$ is well distributed in a set of the form $\mathcal{F}(\eta)+\eta(K)$, where $\mathcal{F}(\eta)$ is a Φ-subtorus of level $\leq\log_p\deg\eta$ of $\mathscr{T}^c$ and K is a finite subset of $\mathscr{Z}$. For any polynomial $\mathscr{Z}$-sequence $g(n)=\alpha_0+\eta_1(n^{r_1})+\ldots+\eta_d(n^{r_d})$, $n\in\mathscr{Z}$, where $\alpha_0\in\mathscr{T}^c$, $\eta_1,\ldots,\eta_d$ are additive polynomial $\mathscr{Z}$-sequences and $n^{r_1},\ldots,n^{r_d}$ are distinct separable monomials, the closure $\mathcal{O}(g)=\overline{g(\mathscr{Z})}$ of $g(\mathscr{Z})$ has the form $\mathcal{F}(g)+g(K)$, where $\mathcal{F}(g)$ is the Φ-subtorus $\sum_{i=1}^d\mathcal{F}(\eta_i)$ and K is a finite subset of $\mathscr{Z}$, and $g(n)$ is well distributed in the components $\mathcal{F}(g)+g(k)$, $k\in K$, of $\mathcal{O}(g)$. In particular, g is well distributed in $\mathscr{T}^c$ iff $\mathscr{T}^c=\sum_{i=1}^d\mathcal{F}(\eta_i)$.*

If all the monomials of g are separable, we have a complete analogue of Theorem 0.2:

Corollary 0.4. *Let $g(n)=\sum_{i=1}^d\alpha_in^{r_i}$ be a polynomial $\mathscr{Z}$-sequence in $\mathscr{T}^c$ with all of r_i not divisible by p. Then the closure $\mathcal{O}(g)=\overline{g(\mathscr{Z})}$ of $g(\mathscr{Z})$ is of the form $\mathcal{S}(g)+g(K)$, where $\mathcal{S}(g)$ is the S-subtorus $\sum_{i=1}^d\mathcal{S}(\alpha_i)$ of $\mathscr{T}^c$ and K is a finite subset of $\mathscr{Z}$, and $g(n)$ is well distributed in the components $\mathcal{S}(g)+g(k)$, $k\in K$, of $\mathcal{O}(g)$. In particular, g is well distributed in $\mathscr{T}^c$ iff $\mathscr{T}^c=\sum_{i=1}^d\mathcal{S}(\alpha_i)$.*

In particular, for the case $c=1$ we get the following:

Corollary 0.5. *Let $g(n)=\sum_{i=1}^d\alpha_in^{r_i}$ be a polynomial $\mathscr{Z}$-sequence in $\mathscr{T}$ with all of r_i not divisible by p and at least one of α_i be irrational. Then g is well distributed in $\mathscr{T}$.*

In order to have some applications of the above equidistribution results, we use them, in combination with the spectral theorem, to establish some ergodic theoretical and combinatorial facts related to unitary and measure preserving actions of the group $\mathscr{Z}^c$ and analogous to classical theorems, namely the polynomial mean ergodic theorem, the polynomial Khintchine theorem, and the Sárközy theorem. In particular, we prove the following theorem:

Theorem 0.6. *Let T be a measure preserving action of the group $\mathscr{Z}^c$ on a probability measure space $(X,\mathcal{B},\mu)$, let $A\in\mathcal{B}$, $\mu(A)>0$, and let $q\colon\mathscr{Z}\longrightarrow\mathscr{Z}^c$ be a polynomial with $q(0)=0$. Then for any $\varepsilon>0$ there exists a nonzero $m\in\mathscr{Z}$ such that for any Følner sequence $(\Phi_N)_{N=1}^\infty$ in $\mathscr{Z}$, $\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}\mu(A\cap T(-q(mn))A)>\mu(A)^2-\varepsilon$.*

Via Furstenberg's correspondence principle, we get as a corollary the following analogue of the classical Sárközy theorem ([S]):

Theorem 0.7. *Let $q\colon\mathscr{Z}\longrightarrow\mathscr{Z}^c$ be a polynomial with $q(0)=0$ and let $E\subseteq\mathscr{Z}^c$ be a set* *of positive upper Banach density:*

$$d^*(E)=\sup\bigl\{\limsup_{N\to\infty}|E\cap\Psi_N|/|\Psi_N| : (\Psi_N)_{N=1}^{\infty} \textit{ is a Følner sequence in } \mathcal{Z}^c\bigr\}>0.$$

Then for any $\varepsilon>0$ *there exists* $m\in\mathcal{Z}$ *such that, for any Følner sequence* $(\Phi_N)_{N=1}^{\infty}$ *in* $\mathcal{Z}$*,* $\liminf_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}d^*(E\cap(E-q(mn)))>d^*(E)^2-\varepsilon$*.*

The structure of the paper is as follows: Sections 1, 2, and 5 are preparatory. In Sections 3, 4, 6, and 7 we prove some auxiliary special cases of Theorem 0.3. The very Theorem 0.3 is proved in Section 8. In Section 9 we obtain some ergodic theoretical and combinatorial corollaries of Theorem 0.3. Finally, in Section 10 we briefly discuss the extension of our results to the case of $\mathcal{Z}$-polynomials of several variables.

1. S- and Φ-subtori of $\mathcal{T}^c$

Let F be a finite field of finite characteristic p. From now on, our ring of "integers" is $\mathcal{Z}=F[t]$; the field of "rationals" is $\mathcal{Q}=F(t)$, the quotient field of $\mathcal{Z}$; the field of "reals" is $\mathcal{R}=F[t][[t^{-1}]]$, the completion of $\mathcal{Q}$; and the "unit circle", or the "one-dimensional torus", is $\mathcal{T}=\mathcal{R}/\mathcal{Z}$ (Note that, unlike the classical situation, $\mathcal{T}$ can be identified with the subgroup $t^{-1}F[[t^{-1}]]$ of $\mathcal{R}$, so that $\mathcal{R}=\mathcal{Z}\oplus\mathcal{T}$.)

$\mathcal{Z}$ is a Euclidean domain, and for any nonzero $m\in\mathcal{Z}$, the ring $\mathcal{Z}/(m\mathcal{Z})$ of residues modulo m is finite.

For $x\in\mathcal{R}$, $x=a_rt^r+a_{r-1}t^{r-1}+\ldots$, with $a_r\neq 0$, we define $\|x\|=r$. (Under this definition, $\|0\|=-\infty$.) For any $x,y\in\mathbb{R}$ we have $\|x+y\|\leq\max\{\|x\|,\|y\|\}$, $\|xy\|=\|x\|+\|y\|$, and $\|x^{-1}\|=-\|x\|$. For a vector $x=(x_1,\ldots,x_c)\in\mathcal{R}^c$, we put $\|x\|=\max\{\|x_1\|,\ldots,\|x_c\|\}$.

The "one-dimensional torus" $\mathcal{T}=\mathcal{R}/\mathcal{Z}\simeq t^{-1}F[[t^{-1}]]$ is isomorphic, as an abelian group, a topological space, and a measure space, to $F^{\mathbb{N}}$. We define a (translation invariant) metric on $\mathcal{T}$ by $\mathrm{dist}(x,y)=2^{\|x-y\|}$, $x,y\in\mathcal{T}$. We will write elements of $\mathcal{T}$ as $(a_1,a_2,\ldots)$, $a_j\in F$, rather than as $a_1t^{-1}+a_2t^{-2}+\ldots$.

Let $c\in\mathbb{N}$. We call a vector subspace of $\mathcal{R}^c$ *rational* if it is spanned over $\mathcal{R}$ by elements of $\mathcal{Q}^c$. We will call the projection to $\mathcal{T}^c$ of any rational vector subspace of $\mathcal{R}^c$ *an S-subtorus* (a standard subtorus) of $\mathcal{T}^c$. For an S-subtorus $\mathcal{S}$ of $\mathcal{T}^c$ we define *the dimension* of $\mathcal{S}$ as the dimension (over $\mathcal{R}$) of the corresponding subspace. Any b-dimensional S-subtorus of $\mathcal{T}^c$ is the image in $\mathcal{T}^c$ of a torus $\mathcal{T}^b$ under a linear mapping $\phi(x_1,\ldots,x_b)=\sum_{i=1}^{b}m_ix_i$, $(x_1,\ldots,x_b)\in\mathcal{T}^b$, where $m_1,\ldots,m_b\in\mathcal{Z}^c$.

If $q_1,\ldots,q_c\in\mathcal{Q}$, then the set $\mathcal{V}=\bigl\{(q_1x,\ldots,q_cx),\ x\in\mathcal{R}\bigr\}$ is a one-dimensional rational subspace of $\mathcal{R}^c$. Under $\mathcal{S}=\bigl\{(q_1x,\ldots,q_cx),\ x\in\mathcal{T}\bigr\}$ we will understand the one-dimensional S-subtorus that is the image of $\mathcal{V}$ in $\mathcal{T}^c$. (Notice that the elements q_ix, $x\in\mathcal{T}$, are not uniquely defined).

The following lemma implies that any b-dimensional S-subtorus of $\mathcal{T}^c$ is isomorphic, as an $\mathcal{R}$ module, to the b-dimensional torus $\mathcal{T}^b$.

Lemma 1.1. *Let* $\mathcal{V}$ *be a rational subspace of* $\mathcal{R}^c$*; there exists an* $\mathcal{R}$*-basis in* $\mathcal{V}$ *that spans* $\mathcal{Z}^c\cap\mathcal{V}$*.*

Proof. Let $B \subset \mathcal{Q}^c \cap \mathcal{V}$ be a basis of $\mathcal{V}$ such that $\mathcal{Z}B \supseteq \mathcal{Z}^c \cap \mathcal{V}$. For any basis $D \subset \mathcal{Z}^c \cap \mathcal{V}$ of $\mathcal{V}$, let A_D be "the change-of-coordinates matrix" from B to D; the entries of this matrix are from $\mathcal{Z}$. Find a basis $D = \{u_1, \dots, u_b\}$ for which $\|\det A_D\|$ is minimal; we claim that D spans $\mathcal{Z}^c \cap \mathcal{V}$. Indeed, assume that there exists a vector $v \in \mathcal{Z}^c \cap \mathcal{V}$ such that $v \notin \mathcal{Z}D$. Then $v = \frac{k_1}{m}u_1 + \dots + \frac{k_b}{m}u_b$, $m, k_1, \dots, k_b \in \mathcal{Z}$, where not all of k_i are divisible by m. Assume that k_1 is not divisible by m, and let $k_1 = nm + k$, $n, k \in \mathcal{Z}$, $\|k\| < \|m\|$. Let $w = v - nu_1$, then $w = \frac{k}{m}u_1 + \dots + \frac{k_b}{m}u_b$. Take the basis $D' = \{w, u_2, \dots, u_b\}$ of $\mathcal{V}$; then $\|\det A_{D'}\| = \frac{\|k\|}{\|m\|}\|\det A_D\| < \|\det A_D\|$, contradiction. ∎

The *Frobenius endomorphism* $\Phi(x) = x^p$ is defined on $\mathcal{R}$, on $\mathcal{Z}$, and on $\mathcal{T}$; note that for $x = (a_1, a_2, \dots) \in \mathcal{T}$ we have $\Phi(x) = \big(0, \dots, 0, a_1^p, 0, \dots, 0, a_2^p, \dots\big)$ (where each block "$0, \dots, 0$" consists of $p-1$ zeros). The image $\Phi(\mathcal{R})$ is a subfield of $\mathcal{R}$, with $[\mathcal{R} : \Phi(\mathcal{R})] = p$, so that $\mathcal{R}$ is a p-dimensional vector space over $\Phi(\mathcal{R})$. Under the identification of $\mathcal{R}$ with $(\Phi(\mathcal{R}))^p$, the one-dimensional torus $\mathcal{T}$ converts to a p-dimensional torus.

We say that a mapping $\tau: \mathcal{R}^b \longrightarrow \mathcal{R}^c$ is *a Φ-homomorphism* (or *a Φ-linear mapping*) *of level l* if it has the form $\tau(x_1, \dots, x_b) = \sum_{i=1}^b \sum_{j=0}^l \alpha_{i,j} x_i^{p^j}$ for some $\alpha_{i,j} \in \mathcal{R}^c$; a mapping $\tau: \mathcal{T}^b \longrightarrow \mathcal{T}^c$ is *a Φ-homomorphism of level l* if $\tau(x_1, \dots, x_b) = \sum_{i=1}^b \sum_{j=0}^l m_{i,j} x_i^{p^j}$ for some $m_{i,j} \in \mathcal{Z}^c$. We define a Φ-subtorus of $\mathcal{T}^c$ as the image of a torus $\mathcal{T}^b$ under a Φ-homomorphism $\tau: \mathcal{T}^b \longrightarrow \mathcal{T}^c$: a b-dimensional Φ-subtorus of level l of $\mathcal{T}^c$ is a set of the form

$$\Big\{\sum_{i=1}^b \sum_{j=0}^l m_{i,j} x_i^{p^j},\ (x_1, \dots, x_b) \in \mathcal{T}^b\Big\},$$

where $m_{i,j} \in \mathcal{Z}^c$, $i = 1, \dots, b$, $j = 0, \dots, l$. (In particular, S-subtori are just Φ-subtori of level 0.)

Examples. For $F = \mathbb{Z}_2$, the sets $\mathcal{F}_1 = \big\{tx^2,\ x \in \mathcal{T}\big\} = \big\{(a_1, 0, a_2, 0, \dots) \in \mathcal{T},\ a_1, a_2, \dots \in F\big\}$, $\mathcal{F}_2 = \big\{x^2,\ x \in \mathcal{T}\big\} = \big\{(0, a_1, 0, a_2, 0, \dots) \in \mathcal{T},\ a_1, a_2, \dots \in F\big\}$, $\mathcal{F}_3 = \big\{(1+t)x^2,\ x \in \mathcal{T}\big\} = \big\{(a_1, a_1, a_2, a_2, \dots) \in \mathcal{T},\ a_1, a_2, \dots \in F\big\}$, $\mathcal{F}_4 = \big\{x + tx^2,\ x \in \mathcal{T}\big\} = \big\{(a_1 + a_1, a_2, a_3 + a_2, a_4, \dots) \in \mathcal{T},\ a_1, a_2, \dots \in F\big\}$ are 1-dimensional Φ-subtori of level 1 of $\mathcal{T}$; $\mathcal{F}_5 = \big\{tx^2 + t^2x^4,\ x \in \mathcal{T}\big\} = \big\{(a_1, a_1, a_2, 0, a_3, a_2, a_4, 0, a_5, \dots) \in \mathcal{T},\ a_1, a_2, \dots \in F\big\}$ is a Φ-subtorus of level 2 of $\mathcal{T}$. Note that $\mathcal{F}_4 = \big\{(0, u_1, u_2, \dots),\ u_i \in \mathcal{T}\big\}$, which is a subgroup of index 2 in $\mathcal{T}$.

Unlike S-subtori, Φ-subtori cannot, in general, be defined by a finite system of linear equations[(6)]; this fact complicates the proof of our results. We will bypass this problem with the help of the following construction. The "1-dimensional torus" $\mathcal{T}$ with the action of $F[t^p] \simeq \mathcal{Z}$ on it is isomorphic to "the p-dimensional torus" $\mathcal{T}^p$ with the action of $F[t] = \mathcal{Z}$ on it: the isomorphism $\psi_1: \mathcal{T} \longrightarrow \mathcal{T}^p$ (the *splitting isomorphism*) is given by

$$\psi_1(a_1, a_2, \dots) = \big((a_1^{p^{-1}}, a_{p+1}^{p^{-1}}, \dots), (a_2^{p^{-1}}, a_{p+2}^{p^{-1}}, \dots), \dots, (a_p^{p^{-1}}, a_{2p}^{p^{-1}}, \dots)\big), \tag{1.1}$$

[(6)] Indeed, Φ-subtori cannot, in general, be defined by finitely many $\mathcal{R}$-linear equations, since such equations may only define S-subtori; and they cannot, in general, be defined by finitely many F-linear equations, since they may have infinite index in $\mathcal{T}^c$.

then for any $n \in \mathbb{Z}$ and $\alpha \in \mathbb{T}$ we have $\psi_1(\alpha n^p) = \psi_1(\alpha)n$. The inverse of ψ_1, *the merging isomorphism* $\varphi_1 = \psi_1^{-1}: \mathbb{T}^p \longrightarrow \mathbb{T}$ has the form $\varphi_1(x_1, \ldots, x_p) = \sum_{i=1}^p t^{p-i} x_i^p$, $(x_1, \ldots, x_p) \in \mathbb{T}^p$.

For a mapping τ and $c \in \mathbb{N}$ we will denote by $\tau^{\times c}$ the product of c copies of τ, $\tau^c(x_1, \ldots, x_c) = \big(\tau(x_1), \ldots, \tau(x_c)\big)$. For each $l \geq 2$, we define $\psi_l: \mathbb{T} \longrightarrow \mathbb{T}^{p^l}$ by

$$\psi_l = \psi_1^{\times p^{l-1}} \circ \psi_{l-1}. \tag{1.2}$$

For $n \in \mathbb{Z}$ and $\alpha \in \mathbb{T}$ we have $\psi_l(\alpha n^{p^l}) = \psi_l(\alpha)n$. Let $\varphi_l = \psi_l^{-1}$; then

$$\varphi_l(x_1, \ldots, x_{p^l}) = \sum_{i=1}^{p^l} t^{r_i} x_i^{p^l}, \quad (x_1, \ldots, x_{p^l}) \in \mathbb{T}^{p^l}, \tag{1.3}$$

for some constants $r_1, \ldots, r_{p^l} \in \{0, \ldots, p^l - 1\}$. We also put φ_0 and ψ_0 to be the identical self-mapping of $\mathbb{T}$.

For $l \geq 0$, let $\mathbb{T}^{(l)}$ be the torus $\mathbb{T}^{p^0} \oplus \mathbb{T}^{p^1} \oplus \ldots \oplus \mathbb{T}^{p^l} = \mathbb{T}^{p^0+p^1+\ldots+p^l}$, and let $\sigma_l: \mathbb{T}^{(l)} \longrightarrow \mathbb{T}$ be the homomorphism defined by $\sigma_l(x_0, x_1, \ldots, x_l) = \sum_{j=0}^l \varphi_j(x_j)$, $x_j \in \mathbb{T}^{p^j}$, $j = 0, \ldots, l$. By (1.3), we see that

$$\sigma_l(y_1, \ldots, y_b) = y_1 + \sum_{i=2}^{b} t^{r_i} y_i^{p^{l_i}}, \quad (y_1, \ldots, y_b) \in \mathbb{T}^b, \quad b = 1 + p + \ldots + p^l, \tag{1.4}$$

for some integers $1 \leq l_i \leq d$ and $0 \leq r_i \leq p^d$, $i = 2, \ldots, b$. Thus, σ_l is a Φ-homomorphism; it follows that if $\mathcal{S}$ is a b-dimensional S-subtorus of $\mathbb{T}^{(l)c} = (\mathbb{T}^{(l)})^c$, $c \in \mathbb{N}$, then the set $\mathcal{F} = \sigma_l^{\times c}(\mathcal{S}) \subseteq \mathbb{T}^c$ is a b-dimensional Φ-subtorus of level l of $\mathbb{T}^c$.

The converse is also true:

Proposition 1.2. *For any Φ-subtorus $\mathcal{F}$ of $\mathbb{T}^c$ of level l there exists an S-subtorus $\mathcal{S}$ of $\mathbb{T}^{(l)c}$ such that $\sigma_l^{\times c}(\mathcal{S}) = \mathcal{F}$.*

Proof. Since any Φ-subtorus is a sum of 1-dimensional Φ-subtori, we may assume that $\mathcal{F}$ is 1-dimensional, and has the form $\mathcal{F} = \big\{\sum_{j=0}^l m_j x^{p^j},\ x \in \mathbb{T}\big\}$, $m_j \in \mathbb{Z}^c$. For each $j = 0, \ldots, l$ let $M_j = \psi_j^{\times c}(m_j) \in \mathbb{T}^{p^j c}$, where φ_j is the splitting isomorphism introduced by (1.1) and (1.2); then for any $x \in \mathbb{T}$, $\varphi_j^{\times c}(M_j x) = m_j x^{p^j}$. Hence, for any $x \in \mathbb{T}$, $\sigma_l(M_0 x, M_1 x, \ldots, M_l x) = \sum_{j=0}^l m_j x^{p^j}$. Thus for the 1-dimensional S-subtorus $\mathcal{S} = \big\{(M_0 x, M_1 x, \ldots, M_l x),\ x \in \mathbb{T}\big\} \subset \mathbb{T}^{(l)c}$ we have $\sigma_l(\mathcal{S}) = \mathcal{F}$. ∎

It follows from the definition that the sum of two Φ-subtori of level l is a Φ-subtorus of level l. We now have:

Lemma 1.3. *Φ-subtori of bounded levels satisfy the increasing chain condition: if $\mathcal{F}_1, \mathcal{F}_2, \ldots$ are subtori of level l of $\mathbb{T}^c$ such that $\mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \ldots$, then there exists r such that $\mathcal{F}_i = \mathcal{F}_r$ for all $i \geq r$.*

Proof. For each i, let $\mathcal{S}_i$ be a subtorus of $\mathbb{T}^{(l)c}$ such that $\sigma_l^{\times c}(\mathcal{S}_i) = \mathcal{F}_i$. Then, for each i, $\mathcal{F}_i = \sigma_l^{\times c}(\mathcal{S}'_i)$ where $\mathcal{S}'_i = \mathcal{S}_1 \cup \ldots \cup \mathcal{S}_i$. Since the sequence $(\mathcal{S}'_i)$ stabilizes, so does the sequence $(\mathcal{F}_i)$. ∎

We cannot say much about the structure of Φ-subtori; the examples above show that it may be quite complicated. The following proposition describes a situation where an Φ-subtorus is "almost" the whole torus.

Proposition 1.4. *Let $\mathcal{S}$ be an S-subtorus of $\mathbb{T}^{(l)c} = \mathbb{T}^{p^0 c} \oplus \mathbb{T}^{p^1 c} \oplus \ldots \oplus \mathbb{T}^{p^l c}$ whose projection onto the first summand is surjective. Then the Φ-subtorus $\sigma_l^{\times c}(\mathcal{S})$ is a subgroup of finite index in $\mathbb{T}^c$.*

Proof. To simplify notation we will only prove this proposition in the case $c = 1$; the proof of the general case is similar. Let $b = 1 + p + \ldots + p^l$; choose a 1-dimensional subtorus $\mathcal{S}'$ of $\mathcal{S}$ of the form $\mathcal{S}' = \{(z, q_2 z, \ldots, q_b z) \in \mathbb{T}^{(l)} = (\mathbb{T})^b,\ z \in \mathbb{T}\}$, with $q_2, \ldots, q_b \in \mathbb{Q}$. By (1.4), for $x = (x_1, \ldots, x_b)$ we have $\sigma_l(x) = x_1 + \sum_{i=2}^b t^{r_i} x_i^{p^{l_i}}$ for some $r_i \geq 0$, $l_i \geq 1$, $i = 2, \ldots, b$. So, for $x = (z, q_2 z, \ldots, q_b z) \in \mathcal{S}'$, $z \in \mathbb{T}$, we get

$$\sigma_l(x) = z + \sum_{i=2}^{b} t^{r_i} (q_i z)^{p^{l_i}}.$$

If $z \in t^{-r}\mathbb{T}$ for some $r \in \mathbb{N}$, say, $z = t^{-r} y$ for $y \in \mathbb{T}$, we get $\sigma_l(x) = z + \sum_{i=2}^b t^{r_i - r p^{l_i}} q_i^{p^{l_i}} y^{p^{l_i}}$. When r is large enough so that $r p^{l_i} > r + r_i + \|q_i\| p^{l_i}$, $i = 2, \ldots, b$, we obtain that $\sigma_l(x) = z \bmod t^{-(r+1)}\mathbb{T}$. It follows that elements of $\sigma_l(\mathcal{S}')$ are dense in the group $t^{-r}\mathbb{T}$ for some r, and so, $\sigma_l(\mathcal{S}') \supseteq t^{-r}\mathbb{T}$. ∎

Example. Let $F = \mathbb{Z}_2$, and let $\mathcal{S} = \{(x, (x, 0)),\ x \in \mathbb{T}\} \subset \mathbb{T}^{(1)} = \mathbb{T}^3$. Then the Φ-subtorus $\mathcal{F} = \sigma_1(\mathcal{S})$ consists of all elements of the form $(a_1, a_2, a_3, a_4, \ldots) + (a_1, 0, a_2, 0, \ldots)$, $a_i \in F$, $i \in \mathbb{N}$, which is the subgroup $\{(0, u_2, u_3, \ldots),\ u_i \in F\}$ of index 2 in $\mathbb{T}$.

For any $s \leq l$, the subtorus $\mathbb{T}^{p^s c} \oplus \ldots \oplus \mathbb{T}^{p^l c}$ of $\mathbb{T}^{(l)c} = \mathbb{T}^{p^0 c} \oplus \mathbb{T}^{p^1 c} \oplus \ldots \oplus \mathbb{T}^{p^l c}$ with the restriction of the homomorphism $\sigma_l^{\times c}$ thereon can be seen as the torus $\mathbb{T}^{((l-s))p^{s-l} c}$ with the homomorphism $\sigma_{l-s}^{\times p^{s-l} c}$ to $\mathbb{T}^{p^{s-l} c}$ followed by the isomorphism $\varphi_{s-l}^{\times c}$ to $\mathbb{T}^c$. Applying Proposition 1.4 to this situation, we get

Corollary 1.5. *Let $\mathcal{S}$ be an S-subtorus of $\mathbb{T}^{(l)c}$ which projects trivially to the first s summands of $\mathbb{T}^{(l)c}$ and whose projection to the $(s+1)$-st summand $\mathbb{T}^{p^s c}$ is surjective. Then the Φ-subtorus $\sigma_l^{\times c}(\mathcal{S})$ is a subgroup of finite index in $\mathbb{T}^c$.*

We will also need the following technical lemma:

Lemma 1.6. *Let $\tau\colon \mathbb{T}^b \longrightarrow \mathbb{T}$ be a Φ-homomorphism and let $\tilde{\tau}(z, x) = z + \tau(x)$, $z \in \mathbb{T}$, $x \in \mathbb{T}^b$. If $\mathcal{S}$ is a (one-dimensional) subtorus of $\mathbb{T}^{b+1}$ of the form $\mathcal{S} = \{(z, q_1 z, \ldots, q_b z) : z \in \mathbb{T}\}$ with $q_1, \ldots, q_b \in \mathbb{Q}$ such that $\|q_1\|, \ldots, \|q_b\|$ are small enough, then $\tau(\mathcal{S}) = \mathbb{T}$.*

Proof. Let $\tau(x_1,\ldots,x_b)=\sum_{i=1}^b\sum_{j=0}^l m_{i,j}x_i^{p^j}$, $m_{i,j}\in\mathcal{Z}$, $i=1,\ldots,b$, $j=0,\ldots,l$. Then for any $r\in\mathbb{N}$ and $z\in t^{-r}\mathcal{T}$, $z=t^{-r}y$, $y\in\mathcal{T}$, for $x=(z,q_1z,\ldots,q_bz)\in\mathcal{S}$ we have $\tilde{\tau}(z,x)=z+\sum_{i=1}^b\sum_{j=0}^l m_{i,j}t^{-rp^j}q_i^{p^j}y^{p^j}$. If, for each i, $\|q_i\|<-\max_j\|m_{i,j}\|$, then for all i and j, $\left\|m_{i,j}t^{-rp^j}q_i^{p^j}y^{p^j}\right\|=\|m_{i,j}\|-rp^j+\|q_i\|p^j<r$, so $\tilde{\tau}(z,x)=z \bmod t^{-r-1}\mathcal{T}$. Hence, $\tilde{\tau}(S)$ is dense in $\mathcal{T}$, and so, $\tilde{\tau}(S)=\mathcal{T}$. ■

2. F-characters and S-characters on $\mathcal{T}^c$ and well distribution of $\mathcal{Z}$-sequences

$\mathcal{T}^c$ is a vector space over F; we will call continuous F-linear functionals on $\mathcal{T}^c$ F-*characters*. Any F-character on $\mathcal{T}$ is a finite F-linear combination of F-coordinates of the argument, $\rho(x)=\sum_{i=1}^r b_ia_i$, $x=(a_1,a_2,\ldots)$, for some $r\in\mathbb{N}$ and $b_1,\ldots,b_r\in F$; taking $m=\sum_{i=0}^{r-1}b_{i+1}t^i\in\mathcal{Z}$, this can be written as $\rho(x)=(mx)_1$ (where y_1 denotes the first entry of an element $y=(y_1,y_2,\ldots)\in\mathcal{T}$). Every F-character on $\mathcal{T}^c$, $c\in\mathbb{N}$, is therefore uniquely representable in the form $\rho(x)=\sum_{j=1}^c(m_jx_j)_1=(m\cdot x)_1$, $x=(x_1,\ldots,x_c)\in\mathcal{T}^c$, for some $m=(m_1,\ldots,m_c)\in\mathcal{Z}^c$.

$\mathcal{T}^c$ is also a vector space over $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$, which is identified with the prime subfield of F; we will call continuous $\mathbb{Z}_p$-linear functionals on $\mathcal{T}^c$ (which are just continuous homomorphisms of the additive group of $\mathcal{T}^c$ to $\mathbb{Z}_p$) $\mathbb{Z}_p$-*characters* on $\mathcal{T}^c$. Choose a basis of F over $\mathbb{Z}_p$, and for $a\in F$ let a_1 stand for the first coordinate of a with respect to this basis; then any $\mathbb{Z}_p$-linear functional on F has the form $\eta(a)=(ba)_1$, $a\in F$, for some $b\in F$. Any $\mathbb{Z}_p$-character θ on $\mathcal{T}$ is of the form $\theta(x)=\sum_{i=1}^r\eta_i(a_i)$, $x=(a_1,a_2,\ldots)$, for some $\mathbb{Z}_p$-characters η_i on F. So, $\theta(x)=\sum_{i=1}^r(b_ia_i)_1=\left(\sum_{i=1}^r b_ia_i\right)_1$, $x=(a_1,a_2,\ldots)$, for some $b_1,\ldots,b_r\in F$, that is, $\theta(x)=(\rho(x))_1$, $x\in\mathcal{T}$, for some F-character ρ on $\mathcal{T}$, and so, $\theta(x)=((mx)_1)_1$, $x\in\mathcal{T}$ for some $m\in\mathcal{Z}$. Every $\mathbb{Z}_p$-character on $\mathcal{T}^c$, $c\in\mathbb{N}$, is therefore uniquely representable in the form $\theta(x)=((m\cdot x)_1)_1$, $x=(x_1,\ldots,x_c)\in\mathcal{T}^c$, for some $m=(m_1,\ldots,m_c)\in\mathcal{Z}^c$.

Let $m=(m_1,\ldots,m_c)\in\mathcal{Z}^c$; we will call the homomorphism $\chi\colon\mathcal{T}^c\longrightarrow\mathcal{T}$ of the form $\chi(x)=m\cdot x=\sum_{j=1}^c m_jx_j$, $x=(x_1,\ldots,x_c)\in\mathcal{T}^c$, *an S-character.* If $m_1,\ldots,m_c$ are relatively prime (that is, their greatest common divisor is 1), we call the S-character χ *primitive.* Any nonprimitive S-character has the form $l\chi'$, where χ' is a primitive S-character and $l\in\mathcal{Z}$. Notice that S-characters commute with the $\mathcal{Z}$-action on $\mathcal{T}^c$: for any S-character χ and any $n\in\mathcal{Z}$ we have $\chi(nx)=n\chi(x)$, $x\in\mathcal{T}^c$. (An analogous fact does not, of course, hold for the F- or $\mathbb{Z}_p$-characters on $\mathcal{T}^c$.)

Any S-subtorus of $\mathcal{T}^c$ can be defined by a system of S-characters. In complete analogy with the classical situation, if χ is a primitive S-character on $\mathcal{T}^c$, then the kernel of χ is an S-subtorus of $\mathcal{T}^c$; if χ is non-primitive, say, $\chi=m\chi'$ where χ' is primitive and $m\in\mathcal{Z}$, then $\ker\chi=\ker\chi'+\mathcal{L}$, where $\mathcal{L}$ is the finite group $\{x\in\mathcal{T}^c : mx=0\}$.

Let us remind some terminology introduced in the introduction. We call mappings from $\mathcal{Z}$ to a set X, $\mathcal{Z}$-*sequences* in X. If X is a compact topological space with a probability Borel measure μ, we will say that a $\mathcal{Z}$-sequence g in X is *well distributed in* X if $\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}f(g(n))=\int_X f\,d\mu$ for any $f\in C(X)$ and any Følner sequence (Φ_N) in $\mathcal{Z}$. When X is a coset of closed subgroup of $\mathcal{T}^c$, we assume that μ is the Haar measure on X. If X is a finite union $X=\bigcup_{i=1}^k X_i$ of cosets of a closed subgroup of $\mathcal{T}^c$ and a mapping $g: G \longrightarrow X$ is such that, for some subgroup H of G of finite index, for any coset $m+H$, $m \in G$, of H one has $g(m+H) \subset X_i$ for some i and the $\mathbb{Z}$-sequence $g(m+n)$, $n \in H$, is well distributed in X_i, we say that g *is well distributed in the components of* X.

Since linear combinations of multiplicative characters on $\mathbb{T}^c$ (that is, continuous homomorphisms $\mathbb{T}^c \longrightarrow \mathbb{C}^*$) are dense in the space $C(\mathbb{T}^c)$, a $\mathbb{Z}$-sequence g is well distributed in $\mathbb{T}^c$ iff $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} \omega(n) = 0$ for every nontrivial multiplicative character ω on $\mathbb{T}^c$ and any Følner sequence (Φ_N) in $\mathbb{Z}$. Any multiplicative character ω on $\mathbb{T}^c$ has the form $\omega(x) = e^{(2\pi i/p)\theta(x)}$ where θ is a $\mathbb{Z}_p$-character; thus, g is well distributed in $\mathbb{T}^c$ iff the $\mathbb{Z}$-sequence $\theta(g(n))$ is well distributed in $\mathbb{Z}_p$ for every nonzero $\mathbb{Z}_p$-character θ on $\mathbb{T}^c$. We also have:

Lemma 2.1. *A $\mathbb{Z}$-sequence $g(n)$, $n \in \mathbb{Z}$, is well distributed in $\mathbb{T}^c$ iff for every nonzero F-character ρ on $\mathbb{T}^c$, the $\mathbb{Z}$-sequence $\rho(g(n))$, $n \in \mathbb{Z}$, is well distributed in F, and iff for every nonzero S-character χ on $\mathbb{T}^c$, the $\mathbb{Z}$-sequence $\chi(g(n))$, $n \in \mathbb{Z}$, is well distributed in $\mathbb{T}$.*

Proof. If $g(n)$ is well distributed in $\mathbb{T}^c$ and ρ (respectively, χ) is a nonzero F- (respectively, S-) character on $\mathbb{T}^c$, then, since ρ (respectively, χ) is a continuous measure preserving mapping, the $\mathbb{Z}$-sequence $\rho(g(n))$ (respectively, $\chi(g(n))$), $n \in \mathbb{Z}$, is well distributed in F (respectively, $\mathbb{T}$).

On the other hand, if $g(n)$ is not well distributed in $\mathbb{T}^c$, then there is a nonzero $\mathbb{Z}_p$-character θ, $\theta(x) = \sum_{j=1}^{c} e((m_j x_j)_1)$, such that $\theta(g(n))$ is not well distributed in F. Then for the F-character $\rho(x) = \sum_{j=1}^{c} (m_j x_j)_1$ and the S-character $\chi(x) = \sum_{j=1}^{c} m_j x_j$, the $\mathbb{Z}$-sequences $\rho(g(n))$ and $\chi(g(n))$ are not well distributed in F and $\mathbb{T}$ respectively. ∎

3. Irrational elements and the $\mathbb{Z}$-sequence αn in $\mathbb{T}$

We will call the elements of $\mathbb{Q}/\mathbb{Z}$ of the torus $\mathbb{T}$ *rational* and the other elements of $\mathbb{T}$ *irrational*.

Theorem 3.1. *An element $\alpha = (a_1, a_2, \ldots) \in \mathbb{T}$ is rational iff the sequence $a_1, a_2, \ldots$ is eventually periodic. If $\alpha \in \mathbb{T}$ is rational, then the set $\{\alpha n,\ n \in \mathbb{Z}\}$ is finite. If $\alpha \in \mathbb{T}$ is irrational, then the $\mathbb{Z}$-sequence $\{\alpha n,\ n \in \mathbb{Z}\}$ is well distributed in $\mathbb{T}$.*

Proof. The proof is almost the same as in the "classical" situation. Let $\alpha \in \mathbb{Q}/\mathbb{Z}$, $\alpha = \frac{k}{m}$, $k, m \in \mathbb{Z}$, $m \neq 0$. For any $n \in \mathbb{Z}$, $\alpha n = \frac{kn}{m} \bmod \mathbb{Z}$ is the remainder after dividing the polynomial kn by the polynomial m; since there are only finitely many remainders when one divides by m, the set $\{\alpha n \bmod \mathbb{Z}, n \in \mathbb{Z}\}$ is finite.

If $\alpha = \frac{k}{m}$, the "digits" $a_1, a_2, \ldots$ of α are obtained by successive dividing the remainders appearing when k is divided by m. Namely, let k_1 be the remainder after the division of k by m; then a_1 is the integer part of $k_1 t/m$. Let k_2 be the remainder after this division; then a_2 is the integer part of $k_2 t/m$. And so on; since there can be only finitely many such remainders, the sequence (a_i) is eventually periodic.

Conversely, if there are s and j such that $a_{i+j} = a_i$ for all $i > s$, then

$$\begin{aligned}\alpha &= a_1 t^{-1} + \ldots + a_s t^{-s} + (a_{s+1} t^{j-1} + a_{s+2} t^{j-2} + \ldots + a_{s+j}) t^{-j-s} (1 + t^{-1} + t^{-2} + \ldots) \\ &= a_1 t^{-1} + \ldots + a_s t^{-s} + (a_{s+1} t^{j-1} + a_{s+2} t^{j-2} + \ldots + a_{s+j}) t^{-j-s} (1 - t)^{-1} \in \mathcal{Q}.\end{aligned}$$

Now let $\alpha \in \mathcal{T}$ be irrational. Then the elements $\alpha n \in \mathcal{T}$, $n \in \mathcal{Z}$, are all distinct. Let $r \in \mathbb{N}$. Since $\mathcal{T}$ is compact, there are $n', n'' \in \mathcal{Z}$ such that $\mathrm{dist}(\alpha n', \alpha n'') < \frac{1}{r}$, and so, for $m = n' - n''$, $\mathrm{dist}(\alpha m, 0) < \frac{1}{r}$. Let $\alpha m = a_j t^{-j} + a_{j+1} t^{-j-1} + \ldots$ with $a_j \neq 0$; then $j > r$. The elements $m t^i \alpha$, $i = j - r, j - r + 1, \ldots, j - 1$, clearly span the group $\mathcal{C}_r = \mathcal{T}/(t^{-r}\mathcal{T})$ over F, and so, the elements $mn\alpha$ are dense in $\mathcal{C}_r$. Since the mapping $n \mapsto mn\alpha$ is a homomorphism, the $\mathcal{Z}$-sequence $mn\alpha$, $n \in \mathcal{Z}$, is well distributed in $\mathcal{C}_r$. The subgroup $m\mathcal{Z}$ has finite index in $\mathcal{Z}$, thus the $\mathcal{Z}$-sequence $n\alpha$, $n \in \mathcal{Z}$, is also well distributed in $\mathcal{C}_r$. Since this is true for any r, the $\mathcal{Z}$-sequence $n\alpha$, $n \in \mathcal{Z}$, is well distributed in $\mathcal{T}$. ■

4. $\mathcal{Z}$-sequence αn in $\mathcal{T}^c$

Let us say that an element $\alpha = (\alpha_1, \ldots, \alpha_c)$ of $\mathcal{T}^c$ is *rational* if $\alpha_1, \ldots, \alpha_c \in \mathcal{Q}$, and is *irrational* if for every S-character χ on $\mathcal{T}^c$, $\chi(\alpha)$ is either irrational or zero. (In other words, if no linear combination of α_i with integer (that is, from $\mathcal{Z}$) coefficients is a nonzero rational element of $\mathcal{T}$.) (Notice that under this definition, there are elements of $\mathcal{T}^c$ that are neither rational nor irrational. Also, $0 \in \mathcal{T}^c$ is both rational and irrational; we do not care about this.)

Lemma 4.1. *For any $\alpha \in \mathcal{T}^c$ there exists $m \in \mathcal{Z}$ such that $m\alpha$ is irrational.*

Proof. Let $\alpha \in \mathcal{T}^c$. Since $\mathcal{Z}$ is a Euclidean ring, the group of S-characters χ on $\mathcal{T}^c$ for which $\chi(\alpha) \in \mathcal{Q}/\mathcal{Z}$ is finitely generated. Let this group be generated by $\chi_1, \ldots, \chi_r$, and let $m \in \mathcal{Z}$ be such that $\chi_i(m\alpha) = m\chi_i(\alpha) = 0$ for all $i = 1, \ldots, r$; then $m\alpha$ is irrational. ■

Theorem 4.2. *Let $\alpha \in \mathcal{T}^c$ and let $g(n) = \alpha n$, $n \in \mathcal{Z}$. If α is irrational, then $\mathcal{S} = \mathcal{O}(g)$ is an S-subtorus of $\mathcal{T}^c$ and g is well distributed in $\mathcal{S}(g)$. If α is not irrational, then $\mathcal{O}(g) = \mathcal{S} + K\alpha$ where $\mathcal{S}$ is an S-subtorus and K is a finite subgroup of $\mathcal{Z}$, and g is well distributed in $\mathcal{O}(g)$; more exactly, there exists a nonzero $m \in \mathcal{Z}$ such that $K = \{k\alpha : \|k\| < \|m\|\}$ and for every $k \in \mathcal{Z}$ the $\mathcal{Z}$-sequence $g(mn + k)$, $n \in \mathcal{Z}$, is well distributed in the translated S-subtorus $\mathcal{S} + k\alpha$.*

Proof. Let α be irrational, and let $\mathcal{S}$ be the minimal S-subtorus of $\mathcal{T}$ that contains α. If the $\mathcal{Z}$-sequence $(n\alpha)$, $n \in \mathcal{Z}$, is not well distributed in $\mathcal{S}$, then there exists an S-character χ on $\mathcal{S}$ such that the $\mathcal{Z}$-sequence $\chi(g(n)) = \chi(\alpha n) = \chi(\alpha)n$ is not well distributed in $\mathcal{T}$, which means that $\chi(\alpha)$ is rational, and so, $\chi(\alpha) = 0$. Hence, α is contained in the proper subtorus $\mathcal{S}' = \ker \chi$ of $\mathcal{S}$, which contradicts the choice of $\mathcal{S}$.

If α is not irrational, find $m \in \mathcal{Z}$ such that $m\alpha$ is irrational and put $\mathcal{S} = \mathcal{O}(g(mn))$ and $K = \big\{k \in \mathcal{Z} : \|k\| < \|m\|\big\}$. ■

Let us denote the S-subtorus $\mathcal{S} = \mathcal{O}((n\alpha))$ appearing in the assertion of Theorem 4.2 by $\mathcal{S}(\alpha)$. Clearly, $\mathcal{S}(m\alpha) = \mathcal{S}(\alpha)$ for all $m \in \mathcal{Z}$, and if α is irrational, $\mathcal{S}(\alpha)$ is the minimal S-subtorus of $\mathcal{T}^c$ that contains α.

5. Van der Corput Lemma

We will need a version of the van der Corput lemma:

Lemma 5.1. (Cf. [BMZ], Lemma 4.2) *Let $n \mapsto a_n$, $n \in G$, be a bounded mapping from a discrete countable abelian group G to $\mathbb{C}$. Then for any Følner sequence $\{\Phi_N\}_{N=1}^{\infty}$ in G and any finite set $\Psi \subseteq G$,*

$$\limsup_{N\to\infty}\left|\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_n\right|^2 \leq \limsup_{N\to\infty}\frac{1}{|\Psi|^2}\sum_{m,k\in\Psi}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_{n+m}\overline{a_{n+k}} \in \mathbb{R}.$$

Proof. For any $N \in \mathbb{N}$ we have

$$\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_n = \frac{1}{|\Psi|}\sum_{m\in\Psi}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_n = \Big(\frac{1}{|\Psi|}\sum_{m\in\Psi}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_{n+m}\Big) - A_N + B_N,$$

where $A_N = \frac{1}{|\Psi|}\sum_{m\in\Psi}\frac{1}{|\Phi_N|}\sum_{\substack{n\in\Phi_N\\ n+m\notin\Phi_N}} a_{n+m}$ and $B_N = \frac{1}{|\Psi|}\sum_{m\in\Psi}\frac{1}{|\Phi_N|}\sum_{\substack{n\notin\Phi_N\\ n+m\in\Phi_N}} a_{n+m}$. Since $\{\Phi_N\}_{N=1}^{\infty}$ is a Følner sequence and $\{a_n\}_{n\in G}$ is a bounded set, $|A_N|, |B_N| \to 0$ as $N \to \infty$. Thus,

$$\limsup_{N\to\infty}\left|\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_n\right| = \limsup_{N\to\infty}\left|\frac{1}{|\Psi|}\sum_{m\in\Psi}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_{n+m}\right|.$$

And by the Cauchy-Schwartz inequality,

$$\left|\frac{1}{|\Psi|}\sum_{m\in\Psi}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_{n+m}\right|^2 = \frac{1}{|\Psi|^2}\left|\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}\sum_{m\in\Psi} a_{n+m}\right|^2 \leq \frac{1}{|\Psi|^2}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}\left|\sum_{m\in\Psi} a_{n+m}\right|^2$$
$$= \frac{1}{|\Psi|^2}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}\sum_{m,k\in\Psi} a_{n+m}\overline{a_{n+k}}.$$

■

Let G be a discrete countable abelian group. A set $S \subseteq G$ is said to have *zero uniform density* in G if $\lim_{M\to\infty}\frac{1}{|\Psi_M|}|S \cap \Psi_M| = 0$ for any Følner sequence (Ψ_M) in G. One can easily show that if $S \subseteq G$ has zero uniform density, then for any $\varepsilon > 0$ there exists a finite set $\Psi \subseteq G$ such that $\frac{1}{|\Psi|}|(S+k)\cap\Psi| < \varepsilon$ for all $k \in G$. Let us say that a statement $P(m)$, $m \in G$, *is true for almost all* $m \in G$ if the set of m for which $P(m)$ fails has zero uniform density in G. We say that a mapping $g\colon G \longrightarrow X$ from G to a probability Borel measure space X is well distributed in X if $\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} f(n) = \int f$ for any $f \in C(X)$ and any Følner sequence (Φ_N) in G. As a corollary of Lemma 5.1, we get:

Proposition 5.2. *Let $g\colon G \longrightarrow H$ be a mapping from a discrete countable abelian group G to a compact abelian Hausdorff group H, and let V be a subgroup of G. If the mapping $D_u g\colon G \longrightarrow H$, $D_u g(n) = g(n+u) - g(n)$, $n \in G$, is well distributed in H for almost all $m \in V$, then g is also well distributed in H.*

Proof. g is well distributed in H iff for any nontrivial multiplicative character ω on H and any Følner sequence (Φ_N) in G, $\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}\omega(g(n)) = 0$. Let ω be a multiplicative character on H and let (Φ_N) be a Følner sequence in G. For each $n \in G$, let $a_n = \omega(g(n))$. By assumption, we have $\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_{n+m}\overline{a_n} = \lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}\omega(D_m g(n)) = 0$ for almost all $m \in V$; let S be the set of $m \in V$ for which this is not true. Given any $\varepsilon > 0$, choose a set $\Psi \subseteq V$ such that $\frac{1}{|\Psi|}|(S+k)\cap\Psi| < \varepsilon$ for all $k \in V$. Then

$$\frac{1}{|\Psi|}\sum_{m\in\Psi}\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_{n+m}\overline{a_{n+k}} = \frac{1}{|\Psi|}\sum_{m\in\Psi}\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_{n+m-k}\overline{a_n} < \varepsilon$$

for all $k \in V$, and so

$$\frac{1}{|\Psi|^2}\sum_{m,k\in\Psi}\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N} a_{n+m}\overline{a_{n+k}} < \varepsilon.$$

By Lemma 5.1, this implies that $\limsup_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}\omega(g(n)) < \varepsilon$. Since this is true for any $\varepsilon > 0$, $\lim_{N\to\infty}\frac{1}{|\Phi_N|}\sum_{n\in\Phi_N}\omega(g(n)) = 0$. ■

6. Small degree polynomial $\mathcal{Z}$-sequences in $\mathcal{T}^c$

Theorem 6.1. *Let $g(n) = \alpha_0 + \alpha_1 n + \ldots + \alpha_d n^d$, $\alpha_0, \ldots, \alpha_d \in \mathcal{T}$, $\alpha_d \neq 0$, be a polynomial $\mathcal{Z}$-sequence in $\mathcal{T}$ with $\deg g = d < p$. If at least one of the coefficients $\alpha_1, \ldots, \alpha_d$ is nonzero irrational, then the $\mathcal{Z}$-sequence $g(n)$, $n \in \mathcal{Z}$, is well distributed in $\mathcal{T}$.*

Proof. We may assume that this is α_d that is nonzero and irrational. Indeed, suppose that $\alpha_d, \ldots, \alpha_{r+1}$ are rational and α_r is irrational for some $r < d$. Let m be a common multiple of the denominators of $\alpha_d, \ldots, \alpha_{r+1}$; then the polynomial $\alpha_{r+1}n^{r+1} + \ldots + \alpha_d n^d$ is constant on each of the (finitely many) cosets $k + m\mathcal{Z}$, $k \in \mathcal{Z}$, $\|k\| < \|m\|$. Replacing $\mathcal{Z}$ by one (and each) of these cosets, we reduce the situation to the case where the senior coefficient of g is irrational.

We will now use induction on d. If $d = 1$, Theorem 3.1 says that $g(n)$ is well distributed in $\mathcal{T}$. If $d \geq 2$, then for any nonzero $u \in \mathcal{Z}$ the $\mathcal{Z}$-sequence $D_u g(n) = g(n+u) - g(n)$, $n \in \mathcal{Z}$, is polynomial of degree $d-1$ with an irrational senior coefficient, so, by induction, it is well distributed in $\mathcal{T}$. By Proposition 5.2, this implies that g is also well distributed in $\mathcal{T}$. ■

Theorem 6.2. *Let $g(n) = \alpha_0 + \alpha_1 n + \ldots + \alpha_d n^d$, $\alpha_0, \ldots, \alpha_d \in \mathcal{T}^c$, be a polynomial $\mathcal{Z}$-sequence in $\mathcal{T}^c$ with $\deg g = d < p$; define the S-subtorus $\mathcal{S}(g)$ by $\mathcal{S}(g) = \sum_{i=1}^d \mathcal{S}(\alpha_i)$. If $\alpha_1, \ldots, \alpha_d$ are all irrational, then g is well distributed in $\alpha_0 + \mathcal{S}(g)$. If not all of α_i are irrational, then $\mathcal{O}(g) = \mathcal{S}(g) + g(K)$, where K is a finite subgroup of $\mathcal{Z}$, and g is well distributed in the components $\mathcal{S}(g) + g(k)$, $k \in K$, of $\mathcal{O}(g)$; more exactly, there exists a nonzero $m \in \mathcal{Z}$ such that for every $k \in K = \{k \in \mathcal{Z} : \|k\| < \|m\|\}$ the $\mathcal{Z}$-sequence $g(mn+k)$, $n \in \mathcal{Z}$, has irrational coefficients, and is well distributed in the translated S-subtorus $\mathcal{S}(g) + g(k)$.*

Proof. We may assume that $\alpha_0 = 0$. Assume that $\alpha_1, \dots, \alpha_d$ are all irrational. For any S-character χ on $\mathcal{T}^c$ that is nontrivial on $\mathcal{S}(g)$, the $\mathcal{Z}$-sequence $\chi(g_k(n))$, $n \in \mathcal{Z}$, is a nonconstant polynomial $\mathcal{Z}$-sequence in $\mathcal{T}$ with all irrational coefficients and of degree $< p$. By Theorem 6.1, $\chi(g(n))$ is well distributed in $\mathcal{T}$, thus by Lemma 2.1, g is well distributed in $\mathcal{S}(g)$.

Now assume that not all of α_i are irrational. Find a nonzero $m \in \mathcal{Z}$ such that $m\alpha_i$, $i = 1, \dots, d$, are all irrational. For each $k \in \mathcal{Z}$ with $\|k\| < \|m\|$ consider the polynomial $\mathcal{Z}$-sequence $g_k(n) = g(mn + k) - g(k)$. All the coefficients of g_k are irrational, so it is well distributed in the S-subtorus $\mathcal{S}(g_k)$.

It remains to show that $\mathcal{S}(g_k)$, for distinct k, are all equal. But this is so since the span of the coefficients of g_k is the same for all k, and $\mathcal{S}(g_k)$ is the minimal S-subtorus of $\mathcal{T}^c$ that contains this span. ■

Remark. The number m in the assertion of Theorem 6.2 is any nonzero element of $\mathcal{Z}$ such that, in the proof of this theorem, the numbers $m\beta_i$ are all irrational. Thus, any multiple of m also satisfies the assertion.

7. Additive $\mathcal{Z}$-sequences in $\mathcal{T}^c$

Additive polynomial $\mathcal{Z}$-sequences, or just *additive $\mathcal{Z}$-sequences*, in $\mathcal{T}^c$ are polynomial mappings $g\colon \mathcal{Z} \longrightarrow \mathcal{T}^c$ satisfying $g(n+m) = g(n) + g(m)$, $n, m \in \mathcal{Z}$; they all have the form $g(n) = \alpha_0 n + \alpha_1 n^p + \ldots + \alpha_l n^{p^l}$, $l \in \mathbb{N}$, $\alpha_0, \dots, \alpha_l \in \mathcal{T}^c$, and we will call l *the Frobenius level* of g.

We will now utilize the torus $\mathcal{T}^{(l)}$ with the mappings $\varphi_i, \psi_i, \sigma_i$ introduced in Section 1:

Proposition 7.1. *Let g be an additive $\mathcal{Z}$-sequence in $\mathcal{T}^c$ of Frobenius level $\leq l$. Then there exists an element $\beta \in \mathcal{T}^{(l)c}$ such that $g(n) = \sigma_l^{\times c}(\beta n)$, $n \in \mathcal{Z}$.*

Proof. Let $g(n) = \alpha_0 n + \alpha_1 n^p + \ldots + \alpha_l n^{p^l}$, $\alpha_0, \alpha_1, \dots, \alpha_l \in \mathcal{T}^c$. Then

$$\big(\psi_0^{\times c}(\alpha_0 n), \psi_1^{\times c}(\alpha_1 n^p), \dots, \psi_l^{\times c}(\alpha_l n^{p^l})\big) = \beta n,\ n \in \mathcal{Z},$$

where $\beta = \big(\psi_0^{\times c}(\alpha_0), \psi_1^{\times c}(\alpha_1), \dots, \psi_l^{\times c}(\alpha_l)\big)$, and we have

$$\sigma_l^{\times c}(\beta n) = \sum_{j=0}^{l} \varphi_j^{\times c}\big(\psi_j^{\times c}(\alpha_j n^{p^j})\big) = \sum_{j=0}^{l} \alpha_j n^{p^j} = g(n),\ n \in \mathcal{Z}.$$

■

Let us say that elements $\alpha_1 \in \mathcal{T}^{c_1}, \dots, \alpha_d \in \mathcal{T}^{c_d}$ are *jointly irrational* if any linear combination of coordinates of α_i with integer coefficients is either irrational or zero; in other words, if $(\alpha_1, \dots, \alpha_d)$ is an irrational element of $\mathcal{T}^{c_1+\dots+c_d}$. It follows from Lemma 4.1 that for any $\alpha_1, \dots, \alpha_d \in \mathcal{T}^c$ there exists a nonzero $m \in \mathcal{Z}$ such that $m\alpha_1, \dots, m\alpha_d$ are jointly irrational. For an additive $\mathcal{Z}$-sequence $g(n) = \alpha_0 n + \alpha_1 n^p + \ldots + \alpha_l n^{p^l}$ in $\mathcal{T}^c$, we will say that g *is irrational* if the elements $\psi_0^{\times c}(\alpha_0), \dots, \psi_l^{\times c}(\alpha_l)$ are jointly irrational. It is clear from the proof of Proposition 7.1 that g is irrational iff the corresponding element $\beta \in \mathcal{T}^{(l)c}$ is irrational.

Theorem 7.2. *Let g be an additive $\mathbb{Z}$-sequence of Frobenius level $\leq l$ in $\mathbb{T}^c$, $g(n) = \alpha_0 n + \alpha_1 n^p + \ldots + \alpha_l n^{p^l}$. If g is irrational, then $\mathcal{F}(g) = \mathcal{O}(g)$ is a Φ-subtorus of $\mathbb{T}^c$ of level $\leq l$ and g is well distributed in $\mathcal{F}(g)$. If g is not irrational then $\mathcal{O}(g) = \mathcal{F}(g) + g(K)$ where $\mathcal{F}$ is a Φ-subtorus of level $\leq l$ and K is a finite subgroup of $\mathbb{Z}$, and g is well distributed in $\mathcal{O}(g)$; more exactly, there exists a nonzero $m \in \mathbb{Z}$ such that for every $k \in K = \{k \in \mathbb{Z} : \|k\| < \|m\|\}$ the $\mathbb{Z}$-sequence $g(mn+k)$, $n \in \mathbb{Z}$, is irrational and well distributed in the translated Φ-subtorus $\mathcal{F}(g) + g(k)$.*

Proof. Let $\beta \in \mathbb{T}^{(l)c}$ be as in Proposition 7.1, and let $G(n) = \beta n$, $n \in \mathbb{Z}$. Since $\mathcal{O}(G)$ is compact, $\sigma_l^{\times c}(\mathcal{O}(G))$ is closed, so $\mathcal{O}(g) = \sigma_l^{\times c}(\mathcal{O}(G))$. Since G is well distributed in $\mathcal{O}(G)$, g is well distributed in $\mathcal{O}(g)$.

If g is an irrational additive $\mathbb{Z}$-sequence, then β is an irrational element of $\mathbb{T}^{(l)}$, thus $\mathcal{O}(G) = \mathcal{S}(\beta)$ is an S-subtorus of $\mathbb{T}^{(l)}$, and we have $\mathcal{O}(g) = \sigma_l^{\times c}(\mathcal{O}(G)) = \sigma_l^{\times c}(\mathcal{S}(\beta)) = \mathcal{F}(g)$, which is a Φ-subtorus of Frobenius level $\leq l$.

If g is not irrational, then there exists a nonzero $m \in \mathbb{Z}$ such that $g'(n) = g(mn)$, $n \in \mathbb{Z}$, is irrational. Let $\mathcal{F}(g) = \mathcal{O}(g')$. Put $K = \{k \in \mathbb{Z} : \|k\| < \|m\|\}$; then $\mathcal{O}(g) = \mathcal{F}(g) + g(K)$. ■

It is clear from the proof of Theorem 7.2 that if g is an additive $\mathbb{Z}$-sequence in $\mathbb{T}^c$, $m \in \mathbb{Z}$, and $g'(n) = g(mn)$, $n \in \mathbb{Z}$, then $\mathcal{F}(g') = \mathcal{F}(g)$; if g is irrational, then $\mathcal{F}(g)$ is the minimal Φ-subtorus of $\mathbb{T}^c$ that contains g.

Since for any S-subtorus $\mathcal{S}$ of $\mathbb{T}(l)c$ one can find an element $\beta \in \mathbb{T}(l)c$ such that $\mathcal{S} = \mathcal{S}(\beta)$, from Proposition 1.2 we also get the following fact:

Proposition 7.3. *For any Φ-subtorus $\mathcal{F}$ of $\mathbb{T}^c$ there exists an additive $\mathbb{Z}$-sequence g in $\mathbb{T}^c$ such that $\mathcal{F}(g) = \mathcal{F}$.*

Let us say that an element $\alpha \in \mathbb{T}^c$ is *spanning* if $\mathcal{S}(\alpha) = \mathbb{T}^c$, that is, if $\chi(\alpha) \neq 0$ for every nonzero F-character χ on $\mathbb{T}^c$. In the case the first coefficient α_0 of g is spanning, Proposition 1.4 and the construction used in the proof of Theorem 7.2 give us the following:

Theorem 7.4. *Let $\alpha_0, \alpha_1, \ldots, \alpha_l \in \mathbb{T}^c$, let α_0 be spanning, and let $g(n) = \alpha_0 n + \alpha_1 n^p + \ldots + \alpha_l n^{p^l}$. Then $\mathcal{O}(g)$ is a subgroup of finite index in $\mathbb{T}^c$.*

More generally, applying Corollary 1.5 instead of Proposition 1.4, we get:

Theorem 7.5. *Let $\alpha_0, \ldots, \alpha_l \in \mathbb{T}^c$, $\alpha_0, \ldots, \alpha_{s-1}$ be rational, $\psi_s(\alpha_s)$ be spanning the torus $\mathbb{T}^{p^s c}$, and let $g(n) = \alpha_s n^{p^s} + \alpha_{s+1} n^{p^{s+1}} + \ldots + \alpha_l n^{p^l}$. Then $\mathcal{O}(g)$ is a subgroup of finite index in $\mathbb{T}^c$.*

8. General polynomial $\mathbb{Z}$-sequences in $\mathbb{T}^c$

For a polynomial g over $\mathbb{R}$, or a polynomial $\mathbb{Z}$-sequence g in $\mathbb{T}^c$, we define the *d-degree* (the derivational degree), d-deg g, of g as the minimal nonnegative integer d such that the dth formal derivative of g is constant. It is easy to see that the d-degree of a polynomial is the maximum of the d-degree of its monomials, and that the d-degree of a monomial x^r is equal to the sum of the digits in the p-ary expansion of r. Note also that if $\deg g < p$, then $\text{d-deg}\, g = \deg g$; that additive polynomials are those of d-degree 1 (and without constant term); and that if η is an additive polynomial, then $\text{d-deg}(\eta\circ g) = \text{d-deg}\, g$ for any polynomial g.

We say that a monomial n^r on $\mathcal{Z}$ is *separable* if r is not divisible by p. Any polynomial $\mathcal{Z}$-sequence g is uniquely representable in the form $g(n) = \alpha_0 + \sum_{i=1}^{d} \eta_i(n^{r_i})$, where $n^{r_1}, \ldots, n^{r_d}$ are distinct separable monomials and $\eta_1, \ldots, \eta_d$ are additive $\mathcal{Z}$-sequences; the d-degree of g is the maximum of the d-degrees of n^{r_i}, $i = 1, \ldots, d$.

We will now move to proving the main result of this paper:

Theorem 8.1. *Let g be a polynomial $\mathcal{Z}$-sequence in $\mathcal{T}^c$, $g(n) = \alpha_0 + \sum_{i=1}^{d} \eta_i(n^{r_i})$, where $n^{r_1}, \ldots, n^{r_d}$ are distinct separable monomials and $\eta_1, \ldots, \eta_d$ are additive $\mathcal{Z}$-sequences; define the Φ-subtorus $\mathcal{F}(g)$ of $\mathcal{T}^c$ by $\mathcal{F}(g) = \sum_{i=1}^{d} \mathcal{F}(\eta_i)$. If all $\eta_1, \ldots, \eta_d$ are irrational, then g is well distributed in $\alpha_0 + \mathcal{F}(g)$. If not all of η_i are irrational, then $\mathcal{O}(g) = \mathcal{F}(g) + g(K)$, where K is a finite subgroup of $\mathcal{Z}$, and g is well distributed in the components $\mathcal{F}(g) + g(k)$, $k \in K$, of $\mathcal{O}(g)$; more exactly, there exists a nonzero $m \in \mathcal{Z}$ such that for every $k \in K = \{k \in \mathcal{Z} : \|k\| < \|m\|\}$ the $\mathcal{Z}$-sequence $g(mn + k)$, $n \in \mathcal{Z}$, is well distributed in the translated Φ-subtorus $\mathcal{F}(g) + g(k)$.*

We will say that a polynomial $\mathcal{Z}$-sequence g in $\mathcal{T}^c$ is *separable* if g is a linear combination of separable monomials: $g(n) = \sum_{i=1}^{d} \alpha_i n^{r_i}$ with $r_1, \ldots, r_d$ being distinct positive integers not divisible by p. For such g we get the following corollary, generalizing Theorem 6.2:

Corollary 8.2. *Let $g(n) = \sum_{i=1}^{d} \alpha_i n^{r_i}$ be a separable polynomial $\mathcal{Z}$-sequence in $\mathcal{T}^c$, and let $\mathcal{S}(g)$ be the S-subtorus $\sum_{i=1}^{d} \mathcal{S}(\alpha_i)$. If $\alpha_1, \ldots, \alpha_d$ are all irrational, then g is well distributed in $\mathcal{S}(g)$. Otherwise, g is well distributed in the components $\mathcal{S}(g) + g(k)$, $k \in K$, of $\mathcal{S}(g) + g(K)$, where $K = \{k \in \mathcal{Z} : \|k\| < \|m\|\}$ for some $m \in \mathcal{Z}$.*

In particular, in the case $c = 1$ we get

Corollary 8.3. *Let $g(n) = \sum_{i=1}^{d} \alpha_i n^{r_i}$ be a separable polynomial $\mathcal{Z}$-sequence in $\mathcal{T}$ with at least one nonzero irrational coefficient. Then g is well distributed in $\mathcal{T}$.*

Proof of Theorem 8.1. We will use induction on $\text{d-deg}\, g$; for $\text{d-deg}\, g = 1$, Theorem 7.2 and Theorem 4.2 give the result. Assume that $\text{d-deg}\, g \geq 2$.

Let l be the maximum of the Frobenius level of η_i, $i = 1, \ldots, d$. Using Proposition 7.1, find elements $\beta_1, \ldots, \beta_d \in \mathcal{T}^{(l)c}$ such that $\eta_i(n) = \sigma_l^{\times c}(\beta_i n)$, $n \in \mathcal{Z}$, $i = 1, \ldots, d$, and lift g to a polynomial $\mathcal{Z}$-sequence $G(n) = \sum_{i=1}^{d} \beta_i n^{r_i}$, $n \in \mathcal{Z}$, in $\mathcal{T}^{(l)c}$, so that $\sigma_l(G(n)) = g(n)$, $n \in \mathcal{Z}$, and $\mathcal{O}(g) = \sigma_l(\mathcal{O}(G))$.

Assume that $\eta_1, \ldots, \eta_d$ are all irrational; then all β_i are irrational. We need to show that G is well distributed in the S-subtorus $\mathcal{S}(G) = \sum_{i=1}^{d} \mathcal{S}(\beta_i)$ of $\mathcal{T}^{(l)c}$. For this to be true, we need to show that for any S-character χ on $\mathcal{T}^{(l)c}$ that is nontrivial on $\mathcal{S}(G)$ the $\mathcal{Z}$-sequence $h(n) = \chi(G(n))$, $n \in \mathcal{Z}$, is well distributed in $\mathcal{T}$. h is a separable polynomial $\mathcal{Z}$-sequence whose all nonzero coefficients are irrational. (Every coefficient of h is a linear combination of coordinates of the corresponding β_i.)

If $\deg h = 1$, then h is well distributed in $\mathcal{T}$ by Theorem 3.1; assume that $\text{d-deg}\, h \geq 2$. For each nonzero $u \in \mathcal{Z}$, let $h_u(n) = D_u h(n) - D_u h(0) = h(u + n) - h(n) - h(u)$, $n \in \mathcal{Z}$;

this is a polynomial $\mathbb{Z}$-sequence of d-degree $\text{d-deg}\, h-1 \leq \text{d-deg}\, g-1$, so, by our induction hypothesis, the assertion of Theorem 8.1 applies to it. Let λ_u be the additive part of h_u, $u \in \mathbb{Z}$; since, by induction hypothesis, $\mathcal{F}(h_u) \supseteq \mathcal{F}(\lambda_u)$, we get that if λ_u is well distributed in $\mathbb{T}$ then h_u is also well distributed in $\mathbb{T}$.

The additive $\mathbb{Z}$-sequences λ_u are of the form $\lambda_u(n) = \delta u^s n + \sum_{i=0}^{b} \bigl(\sum_j \delta_{i,j} u^{s_{i,j}}\bigr) n^{p^i}$, $n \in \mathbb{Z}$, $u \in \mathbb{Z}$, where $b \geq 0$, $\delta, \delta_{i,j} \in \mathbb{T}$, δ_0 is irrational, and $1 \leq s_{i,j} < s$ for all i, j. Define

$$\xi_u = \Bigl(\psi_0\bigl(\delta u^s n + \textstyle\sum_j \delta_{0,j} u^{s_{0,j}}\bigr), \psi_1\bigl(\sum_j \delta_{1,j} u^{s_{1,j}}\bigr), \ldots, \psi_b\bigl(\sum_j \delta_{b,j} u^{s_{b,j}}\bigr)\Bigr) \in \mathbb{T}^{(b)},$$

$u \in \mathbb{Z}$, so that $\lambda_u(n) = \sigma_b(\xi_u n)$, $n \in \mathbb{Z}$. Taking u^{p^b} instead of u, we get

$$\xi_{u^{p^b}} = \Bigl(\delta u^{p^b s} + \textstyle\sum_j \delta_{0,j} u^{p^b s_{0,j}}, \sum_j \psi_1(\delta_{1,j}) u^{p^{b-1} s_{1,j}}, \ldots, \sum_j \psi_b(\delta_{b,j}) u^{s_{b,j}}\Bigr).$$

Now put $\zeta_u = \bigl(\delta u^r, \gamma_1 u^{r_1}, \ldots, \gamma_{b'} u^{r_{b'}}\bigr) \in \mathbb{T}^{b'+1}$, $u \in \mathbb{Z}$, where each γ_j is a coordinate of one of $\psi_i(\delta_{i,j'})$, $r = p^b s$, $r_j < r$ for all j, and define a mapping $\tau: \mathbb{T}^{b'+1} \longrightarrow \mathbb{T}^{(b)}$ that acts by adding certain coordinates of elements of $\mathbb{T}^{b'+1}$, so that $\tau(\zeta_{u^{p^b}}) = \xi_{u^{p^b}}$, $u \in \mathbb{Z}$. Let $\mathcal{S}_u = \mathcal{S}(\zeta_{u^{p^b}})$, $u \in \mathbb{Z}$. Find $q_1, \ldots, q_{b'} \in \mathbb{Q}$ such that the 1-dimensional subtorus $\mathcal{S}'_1 = \bigl\{(x_0, q_1 x_0, \ldots, q_{b'} x_0),\ x_0 \in \mathbb{T}\bigr\}$ is contained in $\mathcal{S}_1$. (That is, 1 and q_j, $j = 1, \ldots, b'$, satisfy all linear equations over $\mathbb{Z}$ that are satisfied by δ and the corresponding γ_j.) Then for any $u \in \mathbb{Z}$, the 1-dimensional subtorus $\mathcal{S}'_u = \bigl\{(x_0, u^{r_1 - r} q_1 x_0, \ldots, u^{r_{b'} - r} q_{b'} x_0),\ x_0 \in \mathbb{T}\bigr\}$ is contained in $\mathcal{S}_u$. The mapping $\tau \circ \sigma_b$ has the form $\tau(\sigma_b(x_0, x_1, \ldots, x_{b'})) = x_0 + \sum_{j=2}^{b'} t^{r_j} x_j^{p^{l_j}}$ for certain r_j, l_j, $j = 1, \ldots, b'$. Thus, by Lemma 1.6, for all u with $\|u\|$ large enough, $\tau \circ \sigma_b(\mathcal{S}'_u) = \mathbb{T}$. So, $\tau \circ \sigma_b(\mathcal{S}_u) = \mathbb{T}$, and so, the $\mathbb{Z}$-sequence $\lambda_{u^{p^b}}(n) = \tau(\sigma_b(\zeta_u n))$ is well distributed in $\mathbb{T}$ for all but finitely many $u \in \mathbb{Z}$. Hence, $h_{u^{p^b}}$ is well distributed in $\mathbb{T}$ for all but finitely many $u \in \mathbb{Z}$. Thus, by Proposition 5.2, h is well distributed in $\mathbb{T}$.

Now assume that not all of η_i and so, β_i are irrational. Find a nonzero $m \in \mathbb{Z}$ such that $m\beta_i$ $i = 1, \ldots, d$, are all irrational. For each $k \in \mathbb{Z}$ with $\|k\| < \|m\|$ let $G_k(n) = G(mn + k) - G(k)$, $n \in \mathbb{Z}$; then $g(mn + k)$, $n \in \mathbb{Z}$, is well distributed in $\sigma_l(\mathcal{O}(G_k)) + g(k)$, and we only need to show that $\mathcal{O}(G_k) = \mathcal{F}(G_k) = \mathcal{S}(G)$. All the coefficients of G_k are contained in $\sum_{i=1}^{d} \mathcal{S}(m\beta_i) = \mathcal{S}(G)$, so $\mathcal{O}(G_k) \subseteq \mathcal{S}(G)$. On the other hand, let χ be a nonzero S-character on $\mathcal{S}(G)$, and, assuming that $r_1 > r_2 > \ldots > r_d$, let $1 \leq i \leq d$ be the minimal index such that $\chi(m\beta_i) \neq 0$. Then the $\mathbb{Z}$-sequence $\chi(G_k)$ has the form $\beta_i m^{r_i} n^{r_i} + H(n)$ where $\deg H < r_i$, and thus is well distributed in $\mathbb{T}$. Hence, G_k is well distributed in $\mathcal{S}(G)$. ■

Remark. The number m in the assertion of Theorem 8.1 is any nonzero element of $\mathbb{Z}$ such that, in the proof of this theorem, the numbers $m\beta_i$ are all irrational. Thus, any multiple of m also satisfies the assertion.

9. An application: $\mathbb{Z}$-polynomial unitary actions and an analogue of Sárközy's theorem

Let U be a unitary action of $\mathbb{Z}^c$ on a Hilbert space $\mathcal{H}$, and let $q: \mathbb{Z} \longrightarrow \mathbb{Z}^c$ be a polynomial; we call the $\mathbb{Z}$-sequence $U(q(n))$, $n \in \mathbb{Z}$, *a polynomial unitary action* of $\mathbb{Z}$ on $\mathcal{H}$. Combining the spectral theorem with the results obtained above, we get the following mean ergodic theorem:

Theorem 9.1. *For any $f \in \mathcal{H}$, the limit* $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} U(q(n))f$ *exists for any Følner sequence* $(\Phi_N)_{N=1}^{\infty}$ *in* $\mathbb{Z}$. (It follows that the limit is the same for all Følner sequences in $\mathbb{Z}$.)

Proof. We may assume that f is cyclic for U, that is, $\overline{U(\mathbb{Z}^c)f} = \mathcal{H}$. The dual group of $\mathbb{Z}^c$ is $\mathbb{T}^c$, with the pairing of $w \in \mathbb{Z}^c$ and $x \in \mathbb{T}^c$ defined by the formula $\langle w, x\rangle = e(w \cdot x)$, where $e(\alpha) = e^{(2\pi i/p)(\alpha_1)_1}$, $\alpha \in \mathbb{T}$. (See Section 2.) By the spectral theorem, we may replace $\mathcal{H}$ by the space $L^2(\mathbb{T}^c, \lambda)$ for some finite measure λ on $\mathbb{T}^c$, with $U(w)$, $w \in \mathbb{Z}^c$, being represented by the operator of multiplication by the function $e(w \cdot x)$, $U(w)(h)(x) = e(w \cdot x)h(x)$, $x \in \mathbb{T}^c$, $h \in L^2(\mathbb{T}^c, \lambda)$. By Theorem 8.1, for any $x \in \mathbb{T}^c$, $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(n) \cdot x)$ exists. Hence, by the dominated convergence theorem, $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(n) \cdot x)f(x)$ exists in $L^2(\mathbb{T}^c, \lambda)$. ■

The classical Sárközy theorem ([S]) says that for any polynomial q with zero constant term, any set of positive upper Banach density(7) in $\mathbb{Z}$ contains two elements a, b with $b - a = q(n)$ for some nonzero $n \in \mathbb{Z}$. An equivalent, via Furstenberg's correspondence principle(8), ergodic theoretical statement is that for any polynomial q with zero constant term, any invertible finite measure preserving system $(X, \mathcal{B}, \mu, T)$ and any $A \in \mathcal{B}$ with $\mu(A) > 0$ there exists $n \in \mathbb{N}$ such that $\mu(A \cap T^{-q(n)}A) > 0$; moreover, one can show that the set of such n has positive lower Banach density in $\mathbb{Z}$ (see [F]). Combining again Theorem 8.1 with the spectral theorem, we can obtain analogous results in our setup:

Theorem 9.2. *Let T be a measure preserving action of the group $\mathbb{Z}^c$ on a probability measure space $(X, \mathcal{B}, \mu)$, let $A \in \mathcal{B}$, $\mu(A) > 0$, and let $q\colon \mathbb{Z} \longrightarrow \mathbb{Z}^c$ be a polynomial with $q(0) = 0$. Then for any Følner sequence $(\Phi_N)_{N=1}^{\infty}$ in $\mathbb{Z}$, the limit $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} \mu(A \cap T(-q(n))A)$ exists, does not depend on (Φ_N), and is positive.*

Remark. The positivity of $\limsup_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} \mu(A \cap T(-q(n))A)$ (but not the existence of the limit) was proved in [BLM].

Proof. Applying Theorem 9.1 to the Hilbert space $\mathcal{H} = L^2(X)$, the unitary action induced

(7) For a subset E of a discrete countable commutative group G, *the upper density* of E with respect to a Følner sequence (Φ_N) in G is $\overline{d}_{(\Phi_N)}(E) = \mathrm{limsup}_{N\to\infty} \frac{1}{|\Phi_N|}|E \cap \Phi_N|$ and *the lower density* of E with respect to (Φ_N) is $\underline{d}_{(\Phi_N)}(E) = \mathrm{liminf}_{N\to\infty} \frac{1}{|\Phi_N|}|E \cap \Phi_N|$. *The upper Banach density* $d^*(E)$ of E in G is the supremum of $\overline{d}_{(\Phi_N)}(E)$ over the set of all Følner sequences (Φ_N) in G, and *the lower Banach density* $d_*(E)$ of E is the infimum of $\underline{d}_{(\Phi_N)}(E)$ over the set of all Følner sequences (Φ_N) in G.

(8) *The Furstenberg correspondence principle* says that for any discrete countable commutative group G and a set $E \subseteq G$ there exists an action T of G on a probability space $(X, \mathcal{B}, \mu)$ and a set $A \in \mathcal{B}$ such that $\mu(A) = d^*(E)$ and for any $w_1, \ldots, w_k \in G$, $\mu(T(-w_1)A \cap \ldots \cap T(-w_k)A) \leq d^*((E - w_1) \cap \ldots (E - w_k))$. (See, for instance, [B].)

by T on $\mathcal{H}$, and the vector $f = 1_A \in \mathcal{H}$, we obtain that the limit

$$\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} \mu(A \cap T(-q(n))A) = \lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} \langle f, T(q(n))f\rangle$$

$$= \left\langle f, \lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} T(q(n))f \right\rangle$$

exists and does not depend on the choice of (Φ_N). The positivity of this limit follows from the following stronger result:

Theorem 9.3. *Under the assumptions of Theorem 9.2, for any $\varepsilon > 0$ there exists a nonzero $m \in \mathbb{Z}$ such that for any Følner sequence $(\Phi_N)_{N=1}^{\infty}$ in $\mathbb{Z}$, $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N}$ $\mu(A \cap T(-q(mn))A) > \mu(A)^2 - \varepsilon$.*

Proof. As in the proof of Theorem 9.1, let λ be the measure on $\mathbb{T}^c$ for which (the closure of $T(\mathbb{Z}^c)f$ in) $\mathcal{H} = L^2(X)$ can be replaced by $L^2(\mathbb{T}^c, \lambda)$ with $T(w)$, $w \in \mathbb{Z}^c$, being represented by the operator of multiplication by the functions $e(w \cdot x)$ and, additionally, f represented by the constant function 1. The function $\tilde{f} = \lim_{N\to\infty} \frac{1}{|\Psi_N|} \sum_{w\in\Psi_N} T(w)f$, where (Ψ_N) is any Følner sequence in $\mathbb{Z}^c$, is represented in $L^2(\mathbb{T}^c, \lambda)$ by the function $1_{\{0\}}$. Since the orthogonal projection of $\tilde{f}$ to the subspace of constants in $L^2(X)$ is the constant $\mu(A)$, which has the norm $\mu(A)$, we have $\|\tilde{f}\|_{L^2(X)} \geq \mu(A)$, and so, $\lambda(\{0\}) \geq \mu(A)^2$.

We now have $\mu(T(-w)A \cap A) = \int_{\mathbb{T}^c} e(w\cdot x)\, d\lambda(x)$, $w \in \mathbb{Z}^c$, and so, $\mu(T(-w)A \cap A) = \int_{\mathbb{T}^c} e(q(n)\cdot x)\, d\lambda(x)$, $n \in \mathbb{Z}$. For any $x \in \mathbb{T}^c$ consider the polynomial $\mathbb{Z}$-sequence $q(n)\cdot x$, $n \in \mathbb{Z}$. By Theorem 8.1 and the remark after the proof of this theorem, there exists a nonzero $m_x \in \mathbb{Z}$ such that for any $m \in \mathbb{Z}$ divisible by m_x the $\mathbb{Z}$-sequence $q(mn)\cdot x$, $n \in \mathbb{Z}$, is well distributed in a Φ-subtorus $\mathcal{F}_x$ of $\mathbb{T}$. Hence, the $\mathbb{Z}$-sequence $e(q(mn)\cdot x)$, $n \in \mathbb{Z}$, is well distributed in the subgroup $e(\mathcal{F}_x)$ of the group P of the roots of 1 of degree p in $\mathbb{C}$. This implies that $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(mn)\cdot x) = \frac{1}{|e(\mathcal{F}_x)|} \sum_{z\in e(\mathcal{F}_x)} z = \begin{cases} 0, & \text{if } e(\mathcal{F}_x) = P \\ 1, & \text{if } e(\mathcal{F}_x) = \{1\}. \end{cases}$

Find $m \in \mathbb{Z}$ "divisible enough" so that for $D = \{x \in \mathbb{T}^c : m_x \bigm| m\} \cup \{0\}$ one has $\lambda(\mathbb{T}^c \setminus D) < \varepsilon$. For any $x \in D$ we have $\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(mn)\cdot x) \geq 0$, and for any $x \in \mathbb{T}^c \setminus D$, $\left|\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(mn)\cdot x)\right| \leq 1$, so

$$\begin{aligned}
\lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} \mu(A \cap T(-q(mn))A) &= \lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} \int_{\mathbb{T}^c} e(q(mn)\cdot x)\, d\lambda(x) \\
&= \int_{\mathbb{T}^c} \lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(mn)\cdot x)\, d\lambda(x) \\
&= \int_{\{0\}} \lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(mn)\cdot x)\, d\lambda(x) \\
&\quad + \int_{D\setminus\{0\}} \lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(mn)\cdot x)\, d\lambda(x) \\
&\quad + \int_{\mathbb{T}^c\setminus D} \lim_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} e(q(mn)\cdot x)\, d\lambda(x) \\
&\geq \lambda(\{0\}) + 0 - \lambda(\mathbb{T}^c \setminus D) > \mu(A)^2 - \varepsilon.
\end{aligned}$$

$\blacksquare$

As a corollary, we get the following fact:

Corollary 9.4. *Under the assumptions of Theorem 9.2, for any $\varepsilon > 0$ the set $E = \{n \in \mathbb{Z} : \mu(A \cap T(-q(n))A) > \mu(A)^2 - \varepsilon\}$ is syndetic in $\mathbb{Z}$.*[(9)]

Proof. Let $(\Phi'_N)_{N=1}^{\infty}$ be any Følner sequence in $\mathbb{Z}$. If S is not syndetic then for every $N \in \mathbb{N}$ there exists some $k_N \in \mathbb{Z}$ such that $(k_N + \Phi'_N) \cap S = \emptyset$. For each N let $\Phi_N = k_N + \Phi'_N$, then $(\Phi_N)_{N=1}^{\infty}$ is also a Følner sequence in $\mathbb{Z}$. For any $m \in \mathbb{Z} \setminus \{0\}$, any $N \in \mathbb{N}$, and any $n \in \Phi_N/m$ one now has $\mu(A \cap T(-q(mn))A) \leq \mu(A)^2 - \varepsilon$, which contradicts Theorem 9.3 (applied to the Følner sequence $(\Phi_N/m)_{N=1}^{\infty}$). $\blacksquare$

Applying the Furstenberg correspondence principle, we get from Theorem 9.2, Theorem 9.3, and Corollary 9.4 the following Sárközy's theorem type results, where d^* stands for the upper Banach density in $\mathbb{Z}^c$:

Theorem 9.5. *Let $q: \mathbb{Z} \longrightarrow \mathbb{Z}^c$ be a polynomial with $q(0) = 0$ and let $E \subseteq \mathbb{Z}^c$, $d^*(E) > 0$. Then for any Følner sequence $(\Phi_N)_{N=1}^{\infty}$ in $\mathbb{Z}$, $\liminf_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} d^*(E \cap (E - q(n))) > 0$. Moreover, for any $\varepsilon > 0$ there exists $m \in \mathbb{Z}$ such that, for any Følner sequence $(\Phi_N)_{N=1}^{\infty}$ in $\mathbb{Z}$, $\liminf_{N\to\infty} \frac{1}{|\Phi_N|} \sum_{n\in\Phi_N} d^*(E \cap (E - q(mn))) > d^*(E)^2 - \varepsilon$; it also follows that the set $S = \{n \in \mathbb{Z} : d^*(E \cap (E - q(n)) > d^*(E)^2 - \varepsilon\}$ is syndetic in $\mathbb{Z}$.*

Remark. It is easy to see that, in complete analogy with the classical situation (see [KM]), the class of polynomials for which the results of this section hold is wider than just the set of polynomials q with $q(0) = 0$, and consists of all *intersective* polynomials, that is, the polynomials q with the property that for any subgroup Λ of finite index in $\mathbb{Z}^c$ there exists $m \in \mathbb{Z}$ such that $q(mn) \in \Lambda$ for all $n \in \mathbb{Z}$.

10. Polynomial $\mathbb{Z}$-sequences in several variables

The results obtained above can be extended to the case of "polynomial sequences" in several variables, that is, the mappings $g: \mathbb{Z}^l \longrightarrow \mathbb{T}^c$ of the form

$$g(n_1, \ldots, n_l) = \sum_{0 \leq r_1, \ldots, r_l \leq \rho} \alpha_{r_1, \ldots, r_l} n^{r_1} \ldots n^{r_l}.$$

Such a "$\mathbb{Z}^l$-polynomial sequence" g in $\mathbb{T}^c$ is uniquely representable in the form $g(n) = \alpha_0 + \sum_{i=1}^{d} \eta_i(n^{r_i})$, where $\eta_1, \ldots, \eta_d$ are additive $\mathbb{Z}$-sequences and "the monomials" $n^{r^{(i)}} = n_1^{r_1^{(i)}} \ldots n_l^{r_l^{(i)}}$ are distinct and *separable*, which means that, for each i, not all of $r_1^{(i)}, \ldots, r_1^{(i)}$ are divisible by p. For such g one can obtain the following theorem:

(9) A subset S of a discrete commutative group G is said to be *syndetic* if there is a finite set $\Phi \subseteq G$ such that $S - \Phi = G$, or, equivalently, for every $g \in G$ one has $(g + \Phi) \cap S \neq \emptyset$.

Theorem 10.1. *Let $\mathcal{F}(g)=\sum_{i=1}^{d}\mathcal{F}(\eta_i)$. If all $\eta_1,\dots,\eta_d$ are irrational, then g is well distributed in $\alpha_0+\mathcal{F}(g)$. If not all of η_i are irrational, then $\mathcal{O}(g)=\mathcal{F}(g)+g(K)$, where K is a finite subgroup of $\mathbb{Z}^l$, and g is well distributed in the components $\mathcal{F}(g)+g(k)$, $k\in K$, of $\mathcal{O}(g)$.*

Bibliography

[B] V. Bergelson, Ergodic theory and diophantine problems, Topics in symbolic dynamics and applications (edited by F. Blanchard, A. Maass, and A. Nogueira), *London Math. Soc. Lecture Note Series* **279** (2000), 167–205.

[BLM] V. Bergelson, A. Leibman, and R. McCutcheon, Polynomial Szemeredi theorem for countable modules over integral domains and finite fields, *J. d'Analyse Math.* **95** (2005), 243–296.

[BMZ] V. Bergelson, R. McCutcheon, and Q. Zhang, A Roth theorem for amenable groups, *Amer. J. Math.* **119** (1997), 1173–1211.

[C] L. Carlitz, Diophantine approximation in fields of characteristic p, *Trans. of AMS* **72** (1952), 187–208.

[D1] A. Dijksma, Uniform distribution of polynomials over $GF\{q,x\}$ in $GF[q,x]$, I, *Indag. Math.* **31** (1969), 376–383.

[D2] A. Dijksma, Uniform distribution of polynomials over $GF\{q,x\}$ in $GF[q,x]$, II, *Indag. Math.* **32** (1970), 187–195.

[DM] A. Dijksma and H. Meijer, On uniform distribution of sequences in $GF[q,x]$ and $GF\{q,x\}$, *Duke Math. J.* **37** (1970), 507–514.

[DrT] M. Drmota and R.F. Tichy, *Sequences, Discrepancies and Applications*, Springer-Verlag, 1997.

[F] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton University Press, 1981.

[KM] T. Kamae and M. Mendès France, Van der Corputs difference theorem, *Israel J. Math.* **31** (1977), 335–342.

[KuN] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Dover Publ., 2006.

[U] A. Ustian, *Additive Polynomial Flows on Tori in Positive Characteristic*, Dissertation, the Ohio State University, Math. Dept., 2012.

[S] A. Sárközy, On difference sets of sequences of integers, I, *Acta Math. Acad. Sci. Hungar.* **31** (1978), 125–149.

[We] H. Weyl, Über die Gleichverteilung von Zahlen mod Eins, *Math. Ann.* **77** (1916), 313-352.