ADDITIVE RELATIONS IN FIELDS: AN ENTROPY APPROACH

Thomas Ward

University of East Anglia

Journal of Number Theory, to appear

Abstract. Let $\xi_1, \dots, \xi_r$ be complex numbers with $K = \mathbb{Q}(\xi_1, \dots, \xi_r)$ having transcendence degree $r-1$ over $\mathbb{Q}$. Consider the equation

$$a_1 x_1 + \cdots + a_k x_k = 1, \tag{1}$$

in which the a_i's are fixed elements of $K^\times$, no proper subsum $a_{i_1} x_{i_1} + \cdots + a_{i_j} x_{i_j}$ vanishes, and we seek solutions $x_i \in \Gamma = \ll \xi_1, \dots, \xi_r \gg$. It is well–known that (1) has only finitely many solutions; we present here an elementary proof of this fact using results from the entropy theory of commuting group automorphisms.

1. Introduction

If α is a mixing action of $\mathbb{Z}^d$ by automorphisms of a compact connected abelian group, then the action is mixing of all orders (see [SW]). This result depends for its proof on the quantitative S–unit theorem of Schlickewei, [S]. On the other hand, the mixing theorem implies the non–quantitative S–unit theorem in a straightforward way (in fact it is enough to know that a mixing $\mathbb{Z}^d$ action by automorphisms of a finite–dimensional compact connected abelian group is mixing of all orders). Unfortunately, there seems to be no internal ergodic–theoretical proof of the mixing result on finite–dimensional groups. In this paper we consider instead $\mathbb{Z}^d$ actions with completely positive entropy on infinite–dimensional compact groups. It is well–known that such actions are mixing of all orders, and we deduce from this a result on additive relations between elements of a finitely–generated subgroup of $\mathbb{C}^\times$. The result we prove is a special case of a very general principle, illustrated by the following theorem of van der Poorten and Schlickewei.

1991 *Mathematics Subject Classification.* 11D72, 28D20.

Supported in part by NSF grant DMS-91-03056 at the Ohio State University.

Theorem. *Let $\mathbb{F}$ be a field of characteristic zero, let $c_1, \ldots, c_n$ be nonzero elements of $\mathbb{F}$, and let $\Gamma_1, \ldots, \Gamma_n$ be finitely generated subgroups of $\mathbb{F}^\times$. Then the equation $c_1\gamma_1 + \cdots + c_n\gamma_n = 1$ has only finitely many solutions in elements $\gamma_i \in \Gamma_i$ $(i = 1, \ldots, n)$ with the property that no subsum $c_{i_1}\gamma_{i_1} + \cdots + c_{i_k}\gamma_{i_k}$ $(k < i)$ vanishes.*

This result (Theorem $2'$ of Section 6.8 in [PS]) depends on a more conventional S–unit theorem in algebraic number fields, and the proof proceeds via induction on the total rank of the Γ_i's and a specialisation method to reduce to the algebraic setting. A simpler argument is used in [P] to give the (no less general) finiteness result when all the Γ_i's coincide.

I am grateful to Graham Everest for several helpful conversations.

2. Actions with completely positive entropy

Consider an action T of $\mathbb{Z}^d$ by invertible measure–preserving transformations of a Lebesgue space $(X, \mathfrak{B}, \mu)$. For finite measurable partitions $\eta = \{A_1, \ldots, A_n\}$ and $\xi = \{B_1, \ldots, B_m\}$ of X, denote by $\eta \vee \xi$ their common refinement (the partition of X into sets of the form $A_i \cap B_j$), and let $H(\eta) = -\sum_{i=1}^n \mu(A_i) \log \mu(A_i)$. The *entropy of T with respect to η* is defined to be

$$h(T, \eta) = \lim_{n\to\infty} \frac{1}{|F_n|} H\left(\bigvee_{\mathbf{m}\in F_n} T_{-\mathbf{m}}(\eta)\right) \tag{2.1}$$

where $\{F_n\}$ is any Følner sequence in $\mathbb{Z}^d$. The action T has *completely positive entropy* if $h(T, \eta) > 0$ whenever $H(\eta) > 0$.

The action T is *mixing of order r* if, for any collection of measurable sets $B_0, \ldots, B_r$,

$$\lim_{\mathbf{n}_l - \mathbf{n}_{l'} \to \infty \text{ for } 0\le l' < l \le r} \mu\left(B_0 \cap T_{-\mathbf{n}_1}(B_1) \cap \cdots \cap T_{-\mathbf{n}_r}(B_r)\right) = \prod_{l=0}^{r} \mu(B_l). \tag{2.2}$$

Here (and below) we adopt the convention that $\mathbf{n}_0 = (0, \ldots, 0)$.

Theorem 2.1. *If T has completely positive entropy, then T is mixing of all orders.*

Proof. Kaminski ([K], Theorem 2) proves this for $d = 2$; modification to $d > 2$ is straightforward.

Let $\alpha : \mathbb{Z}^d \to Aut(X)$ be a homomorphism into the group of continuous automorphisms of the compact abelian group X (so α is a $\mathbb{Z}^d$ action on the Lebesgue space $(X, \mathfrak{B}, \lambda_X)$ where $\mathfrak{B}$ is the Borel σ–algebra on X and μ is normalized Haar measure). Following Kitchens and Schmidt ([KS]), we associate to the pair (X, α) a module $\mathfrak{M}$ over the ring $\mathfrak{R}_d = \mathbb{Z}[u_1^{\pm 1}, \ldots, u_d^{\pm 1}]$ as follows: as an additive group,

$\mathfrak{M}$ is the dual (group of characters) of X. The module structure is determined by identifying multiplication by u_i with the automorphism of $\mathfrak{M}$ dual to the automorphism $\alpha_{\mathbf{e}_i}$ of X (here $\{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ is the standard basis for $\mathbb{Z}^d$.) We may similarly associate a $\mathbb{Z}^d$ action $(X_{\mathfrak{M}}, \alpha^{\mathfrak{M}})$ to any $\mathfrak{R}_d$–module $\mathfrak{M}$. Use $\mathbf{u}^{\mathbf{n}}$ as shorthand for $u_1^{n_1} \ldots u_d^{n_d}$.

By expanding the characteristic function of the sets $B_0, \ldots, B_r$ in (2.2), we see that α is mixing of order r if and only if, for all characters $\chi_0, \ldots, \chi_r \in \widehat{X}$ (not all trivial),

$$\lim_{\mathbf{n}_l - \mathbf{n}_{l'} \to \infty \text{ for } 0 \leq l' < l \leq r} \int (\chi_0)(\chi_1 \cdot \alpha_{\mathbf{n}_1}) \cdots (\chi_r \cdot \alpha_{\mathbf{n}_r}) \, d\lambda_X = 0. \tag{2.3}$$

In terms of the module $\mathfrak{M}$ associated to (X, α), r–mixing is therefore equivalent to the condition that, for all nonzero elements $(a_0, \ldots, a_r) \in \mathfrak{M}^{r+1}$,

$$a_0 + \mathbf{u}^{\mathbf{m}_1} \cdot a_1 + \cdots + \mathbf{u}^{\mathbf{m}_r} \cdot a_r \neq 0 \tag{2.4}$$

whenever $\mathbf{m}_l \in \mathbb{Z}^d$ and $\mathbf{m}_l - \mathbf{m}_{l'}$ lies outside some sufficiently large finite subset of $\mathbb{Z}^d$ for all $0 \leq l' < l \leq r$ (we have again taken $\mathbf{m}_0 = 0$).

Theorem 2.2. *Let $\mathfrak{M} = \mathfrak{R}_d/\mathfrak{p}$ be a cyclic $\mathfrak{R}_d$–module, with $\mathfrak{p}$ a prime ideal. The associated $\mathbb{Z}^d$ action $\alpha^{\mathfrak{M}}$ has completely positive entropy if and only if $\mathfrak{p}$ is principal, and generated by a polynomial not of the form $\mathbf{u}^{\mathbf{m}}\phi(\mathbf{u}^{\mathbf{n}})$ where ϕ is a cyclotomic polynomial.*

Proof. This follows immediately from Theorems 4.2 and 6.5 of [LSW], together with Example 5.4 of [LSW].

Following [LSW], call an ideal *positive* if it is prime and $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ has completely positive entropy. The proof of Theorem 2.2 requires the generalization of Kronecker's theorem to several variables.

From Theorems 2.1 and 2.2, together with the characterization of r–mixing given at (2.4), we obtain the following corollary. Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ denote the algebraic closure of $\mathbb{Q}$.

Corollary 2.3. *Let $\mathfrak{p} \subset \mathfrak{R}$ be a positive ideal and let $\mathfrak{M} = \mathfrak{R}_d/\mathfrak{p}$. Assume that $\mathfrak{M}$ is torsion–free as an additive group. Let $a_0, \ldots, a_r \in \mathfrak{M} \otimes \overline{\mathbb{Q}}$ be non–zero. Then*

$$a_0 + \mathbf{u}^{\mathbf{m}_1} \cdot a_1 + \cdots + \mathbf{u}^{\mathbf{m}_r} \cdot a_r \neq 0$$

whenever $\mathbf{m}_l \in \mathbb{Z}^d$ and $\mathbf{m}_l - \mathbf{m}_{l'}$ lies outside some sufficiently large finite subset of $\mathbb{Z}^d$ for all $0 \leq l' < l \leq r$.

Proof. By (2.4), it is sufficient to show that the $\mathbb{Z}^d$ action corresponding to the $\mathfrak{R}_d$–module $\mathfrak{M} \otimes \overline{\mathbb{Q}}$ has completely positive entropy if the action corresponding to $\mathfrak{M}$ has. Assume therefore that $\alpha^{\mathfrak{M}}$ has completely positive entropy and $\mathfrak{M}$ is torsion free. For each $n \in \mathbb{N}$, $\mathfrak{M} \cong \mathfrak{M} \otimes \frac{1}{n}\mathbb{Z}$, so $\alpha^{\mathfrak{M} \otimes \frac{1}{n}\mathbb{Z}}$ is isomorphic (as a measure–preserving action) to $\alpha^{\mathfrak{M}}$. It follows that $\alpha^{\mathfrak{M} \otimes \frac{1}{n}\mathbb{Z}}$ has completely positive entropy. Now notice that

$$\mathfrak{M} \otimes \mathbb{Q} = \varinjlim \left(\mathfrak{M} \otimes \tfrac{1}{n!}\mathbb{Z}, \iota_{\mathfrak{M}} \otimes \iota_n \right)$$

where $\iota_{\mathfrak{M}}$ is the identity on $\mathfrak{M}$ and $\iota_n : \frac{1}{n!}\mathbb{Z} \hookrightarrow \frac{1}{(n+1)!}\mathbb{Z}$ is the inclusion map, so that

$$X_{\mathfrak{M} \otimes \mathbb{Q}} = \varprojlim X_{\mathfrak{M} \otimes \frac{1}{n!}\mathbb{Z}}. \tag{2.5}$$

It follows that $\alpha^{\mathfrak{M} \otimes \mathbb{Q}}$ also has completely positive entropy: if η is a non–trivial partition of $X_{\mathfrak{M} \otimes \mathbb{Q}}$ then by (2.5) it must project to a non–trivial partition $\overline{\eta}$ of $X_{\mathfrak{M} \otimes \frac{1}{n!}\mathbb{Z}}$ for some n, so $h(\alpha^{\mathfrak{M} \otimes \mathbb{Q}}, \eta) \geq h(\alpha^{\mathfrak{M} \otimes \frac{1}{n!}\mathbb{Z}}, \overline{\eta}) > 0$.

Now assume we have shown that $\alpha^{\mathfrak{M} \otimes k}$ has completely positive entropy for some algebraic number field k, and let θ be algebraic with degree s over k. Then, as $\mathfrak{R}_d$–modules,

$$\mathfrak{M} \otimes k[\theta] \cong (\mathfrak{M} \otimes k)^s,$$

so that $\alpha^{\mathfrak{M} \otimes k[\theta]}$ is simply the s–fold Cartesian power of $\alpha^{\mathfrak{M} \otimes k}$. It follows that $\alpha^{\mathfrak{M} \otimes k[\theta]}$ has completely positive entropy. Choose a chain of simple extensions $\mathbb{Q} \subset k_1 = \mathbb{Q}[\theta_1] \subset k_2 = k_1[\theta_2] \subset \ldots$ with $\overline{\mathbb{Q}} = \varinjlim k_n$. Since $\mathfrak{M} \otimes \overline{\mathbb{Q}} \cong \varinjlim \mathfrak{M} \otimes k_n$, and each of the $\alpha^{\mathfrak{M} \otimes k_n}$ has completely positive entropy (by the above inductive argument), we conclude that $\alpha^{\mathfrak{M} \otimes \overline{\mathbb{Q}}}$ has completely positive entropy as required.

3. Proof of theorem

Theorem 3.1. *Let $\xi_1, \ldots, \xi_r$ be complex numbers with the property that $K = \mathbb{Q}(\xi_1, \ldots, \xi_r)$ has transcendence degree $r-1$ over $\mathbb{Q}$. Then the equation*

$$a_1 x_1 + \cdots + a_k x_k = 1, \tag{3.1}$$

in which the a_i's are fixed elements of $K^\times$, has only finitely many solutions x_i in $\Gamma = \ll \xi_1, \ldots, \xi_r \gg$ for which no proper subsum $a_{i_1} x_{i_1} + \cdots + a_{i_j} x_{i_j}$ vanishes.

Proof. Assume first that the multiplicative group Γ has maximal rank, so $\Gamma \cong \mathbb{Z}^r$. Assume that (3.1) does have infinitely many solutions $x_i \in \Gamma$ with non–vanishing subsums. Parametrize the infinite family of solutions to obtain

$$a'_0 + a'_1 x_1^{(n)} + \cdots + a'_k x_k^{(n)} = 0, \tag{3.2}$$

where $a'_i \in \mathbb{Q}[\xi_1, \ldots, \xi_r]$, no subsums vanish, the equation holds for $n = 1, 2, \ldots$, and without loss of generality $(x_1^{(n)}, \ldots, x_k^{(n)}) \neq (x_1^{(m)}, \ldots, x_k^{(m)})$ if $n \neq m$.

Denote by $\eta : \mathfrak{R}_r \otimes \overline{\mathbb{Q}} \to \mathbb{C}$ the evaluation map $\eta(h) = h(\xi_1, \dots, \xi_r)$. The transcendence assumption implies that the kernel of η is a principal prime ideal, $\mathfrak{p} = \langle f \rangle$ say (by the transcendence assumption, there is an algebraic relation $F(\xi_1, \dots, \xi_r) = 0$; let $V = \{\mathbf{z} \in \overline{\mathbb{Q}}^r \mid F(\mathbf{z}) = 0\}$. The kernel of η is then the ideal attached to V, and this is the radical of $\langle F \rangle$, which is still principal). If $f(\mathbf{u}) = \mathbf{u}^{\mathbf{m}}\phi(\mathbf{u}^{\mathbf{n}})$ where ϕ is a cyclotomic polynomial, then $\xi_1^{n_1} \dots \xi_r^{n_r}$ is a unit root, so $\xi_1^{sn_1} \dots \xi_r^{sn_r} = 1$ for some $s \in \mathbb{N}$. This relation is forbidden by the requirement that the set $\{\xi_1, \dots, \xi_r\}$ multiplicatively generate a group of rank r. Since η induces an isomorphism $\overline{\eta} : \mathfrak{R}_r \otimes \overline{\mathbb{Q}}/\mathfrak{p} \to \overline{\mathbb{Q}}[\xi_1, \dots, \xi_r]$, we may pull the equation (3.2) up to the module $\mathfrak{M} = \mathfrak{R}_r \otimes \overline{\mathbb{Q}}/\mathfrak{p}$ to obtain

$$m_0 + m_1 \mathbf{u}^{\mathbf{m}_1^{(n)}} + \dots + m_k \mathbf{u}^{\mathbf{m}_k^{(n)}} = 0, \tag{3.3}$$

where $m_i \in \mathfrak{M}$, no subsums vanish, the equation holds for $n = 1, 2, \dots$, and $(\mathbf{m}_1^{(n)}, \dots, \mathbf{m}_k^{(n)}) \neq (\mathbf{m}_1^{(m)}, \dots, \mathbf{m}_k^{(m)})$ if $n \neq m$.

We now claim that from the infinite family of solutions to (3.3) we can find an infinite family of solutions to an equation of the form

$$m'_1 \mathbf{u}^{\mathbf{m}_{i_1}^{(n_p)}} + \dots + m'_s \mathbf{u}^{\mathbf{m}_{i_s}^{(n_p)}} = 0 \tag{3.4}$$

in which the m'_i are non–zero, and $\mathbf{m}_{i_r}^{(n_p)} - \mathbf{m}_{i_t}^{(n_p)} \to \infty$ as $p \to \infty$ for $r \neq t$. We allow the possibility that one of the i_s's is 0, and make $\mathbf{m}_0^{(n_p)} = 0$ for all p. The equation (3.4) is obtained as follows. If the exponents $\mathbf{m}_i^{(n)}$ in (3.3) are all moving apart then (3.4) is chosen to be identical to (3.3). If this is not the case, then for each pair of terms that do not move apart, say $\mathbf{u}^{\mathbf{m}_r^{(n)}}$ and $\mathbf{u}^{\mathbf{m}_t^{(n)}}$, we may pass to a subsequence (in n) along which $\mathbf{u}^{\mathbf{m}_r^{(n)}} - \mathbf{u}^{\mathbf{m}_t^{(n)}}$ is a constant. Grouping this into one term contributes one term to (3.4). This process has to stop with a non–trivial equation of the form (3.4) because there are infinitely many solutions to (3.3).

The equation (3.4) contradicts Corollary 2.3, so the original equation (3.1) can have only finitely many solutions if Γ has rank r.

If Γ has smaller rank, then $\Gamma \cong \mathbb{Z}^{r-d} \times F$ for some $d > 0$ and finite group F, and we may therefore replace the equation (3.1) with finitely many different equations, each corresponding to a field extension of the form $\mathbb{Q}(\xi_{i_1}, \dots, \xi_{i_{r-d}})$ with $\ll \xi_{i_1}, \dots, \xi_{i_{r-d}} \gg$ having rank $r - d$.

4. Remark

The connection between equations of the form (3.1) and $\mathbb{Z}^r$ actions by automorphisms of compact groups provides an interesting context in which to see the effect of the transcendence degree of K. Consider the equation

$$a_1 x_1 + \dots + a_k x_k = 1, \tag{4.1}$$

where we seek solutions in $\Gamma = \ll \xi_1, \ldots, \xi_r \gg$ with no vanishing subsums, and let $K = \mathbb{Q}(\xi_1, \ldots, \xi_r)$ have transcendence degree t over $\mathbb{Q}$. For brevity let us assume that Γ has maximal rank.

(1) If $t = r$ then it is clear that (4.1) has only finitely many solutions. The corresponding dynamical system is the full $\mathbb{Z}^r$ shift with alphabet $\mathbb{T}$: this is an *infinite entropy Bernoulli shift*, which is clearly mixing of all orders.

(2) If $t = r - 1$, then we have seen above that the corresponding dynamical system is a *finite* entropy system with completely positive entropy. Such systems are mixing of all orders, and we deduce that there can be only finitely many solutions to (4.1). These dynamical systems are conjectured to be isomorphic to finite entropy Bernoulli shifts (see [LSW], Section 6).

(3) If $t = r - d$, for some $d > 1$, then the corresponding $\mathbb{Z}^r$ dynamical system has zero entropy (though subsystems obtained by restriction to copies of $\mathbb{Z}^{r-d+1}$ do have completely positive entropy). These systems are mixing of all orders, but the proof of this fact uses the S–unit theorem for number fields (see [SW] for the details).

(4) If $t = 0$ then the ξ_i are algebraic numbers, and the corresponding dynamical system is an r–tuple of commuting automorphisms of a finite–dimensional compact group (or *solenoid*); here (4.1) is exactly the usual S–unit equation for number fields, and mixing of all orders in the dynamical system is exactly the same statement as the non–quantitative S–unit theorem.

References

[K] B. Kamiński, *Mixing properties of two–dimensional dynamical systems with completely positive entropy*, Bull. Acad. Polonaise Sci. **27** (1980), 453–463.

[KS] B. Kitchens and K. Schmidt, *Automorphisms of compact groups*, Ergod. Th. & Dynam. Sys. **9** (1989), 691–735.

[LSW] D. Lind, K. Schmidt, and T. Ward, *Mahler measure and entropy for commuting automorphisms of compact groups*, Invent. Math. **101** (1990), 593–629.

[P] A.J. van der Poorten, *Additive relations in number fields*, Séminaire de Théorie des nombres de Paris (1982–83), 259–266.

[PS] A.J. van der Poorten and H.P. Schlickewei, *Additive relations in fields*, J. Austral. Math. Soc. **51** (1991), 154–170.

[S] H.P. Schlickewei, *S-unit equations over number fields*, Invent. Math. **102** (1990), 95–107.

[SW] K. Schmidt and T. Ward, *Mixing automorphisms of compact groups and a theorem of Schlickewei*, Invent. Math. **111** (1993), 69–76.

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, U.K.
E-mail address: tomward@ function.mps.ohio--state.edu