ERGODIC AUTOMORPHISMS OF THE INFINITE TORUS ARE BERNOULLI

BY

D. A. LIND

ABSTRACT

We show that ergodic algebraic automorphisms of the infinite torus are measure isomorphic to Bernoulli shifts. Using the same techniques, we also show that the existence of such an automorphism with finite entropy is equivalent to an open problem in algebraic number theory.

1. Introduction

One of the simplest examples of a measure-preserving transformation is a continuous algebraic automorphism of a compact abelian group equipped with Haar measure. The ergodic properties of such automorphisms have been given close attention. Long ago it was realized that ergodicity of an automorphism is equivalent to aperiodicity of its dual automorphism, and that these imply that the automorphism is already strongly mixing [4]. Rokhlin [10] showed that ergodicity even implies that the automorphism is measure isomorphic to a Kolmogorov automorphism. Recently Katznelson [5] proved that for automorphisms of finite dimensional tori, ergodicity implies the strongest form of mixing, namely being measure isomorphic to a Bernoulli shift.

The purpose of this paper is to extend Katznelson's result to the infinite dimensional torus. We also show how attempting to construct an ergodic automorphism of the infinite torus with finite entropy inevitably leads to an open problem in algebraic number theory.

2. Automorphisms of the infinite torus

Our aim is to prove the following result.

Received December 28, 1973

THEOREM 1. *Ergodic automorphisms of the infinite torus are Bernoulli.*

PROOF. Let us first introduce notation and recall some facts. $\mathbb{T}^\infty$ denotes the countable direct product of copies of the circle group $\mathbb{T}$. $\mathbb{Z}_\infty$ denotes the countable direct sum of copies of the integers $\mathbb{Z}$ and is the dual group of $\mathbb{T}^\infty$. An automorphism A of $\mathbb{T}^\infty$ induces its dual automorphism B of $\mathbb{Z}_\infty$ in the usual way.

Since we will mostly find ourselves in the dual group, it is a useful abbreviation to say for B an automorphism of a discrete group H that B is Bernoulli on H (or (H, B) is Bernoulli) if the dual automorphism $\hat{B}$ on the compact group $\hat{H}$ is measure isomorphic to a Bernoulli shift. Recall that $\hat{B}$ is ergodic on $\hat{H}$ if and only if B is aperiodic on H, that is, $B^k h = h$ with $k > 0$ implies $h = 0$. The dual of Katznelson's result then has the following statement.

TORUS THEOREM. *Aperiodic automorphisms of finite rank, free abelian groups are Bernoulli.*

Ornstein's theorem that factors of Bernoulli shifts are Bernoulli [9] has its dual as follows.

FACTOR THEOREM. *If B is Bernoulli on H and H_0 is a completely invariant subgroup of H, then B is Bernoulli on H_0.*

Similarly, Ornstein's theorem that a transformation which is Bernoulli on each of an increasing sequence of σ-subalgebras is Bernoulli on their span [8] also has its dual.

MONOTONE THEOREM. *If B is an automorphism of H and $\{H_n\}$ is an increasing sequence of completely invariant subgroups on each of which B is Bernoulli, then B is Bernoulli on $\bigcup_1^\infty H_n$.*

We return to the case where B is an automorphism of $\mathbb{Z}_\infty$. If R denotes the ring $\mathbb{Z}[x, x^{-1}]$, consider $\mathbb{Z}_\infty$ as an R-module via the action

$$\left(\sum_{j=-m}^{n} a_j x^j\right) z = \sum_{j=-m}^{n} a_j B^j z \qquad (z \in \mathbb{Z}_\infty).$$

Then the term *R-submodule* means the same as *completely invariant subgroup.*

Suppose the R-torsion submodule of $\mathbb{Z}_\infty$ were a direct summand with a complementary free R-submodule. Then the Torus and Monotone theorems would show that B is Bernoulli on the torsion submodule, while B is automatically Bernoulli on a free R-submodule because there it is isomorphic to a direct sum of shifts on $\mathbb{Z}_\infty$. Since the direct sum of Bernoulli automorphisms is Bernoulli (dualize this fact for products), B would be Bernoulli on $\mathbb{Z}_\infty$. Unfortunately, R is not a principal

ideal domain, so we cannot invoke the Structure Theorem for modules over such domains to obtain the suggested splitting. The obstruction to R being principal lies in the nontrivial ideal structure of the coefficient ring $\mathbb{Z}$. The purpose of the following is to wipe out this ideal structure by embedding the coefficients into a field. We can then apply the Structure Theorem to obtain a splitting of the larger system which suffices for our needs.

Notice that $\mathbb{Z}_\infty$ is a subgroup of $\mathbb{Q}_\infty$, the countable direct sum of copies of the rationals $\mathbb{Q}$. We can extend B to an automorphism of $\mathbb{Q}_\infty$ by putting

$$B(q) = (1/m)B(mq)$$

for $q \in \mathbb{Q}_\infty$, where m is any integer such that $mq \in \mathbb{Z}_\infty$. Then $\mathbb{Q}_\infty$ is a module over the ring $S = \mathbb{Q}[x, x^{-1}]$ via the same action as before. The relevant algebraic properties of these rings are that R is noetherian and S is principal, as one easily verifies.

Since $\mathbb{Z}_\infty$ is countable, the Monotone Theorem shows that it suffices to prove that B is Bernoulli on every finitely generated R-submodule of $\mathbb{Z}_\infty$. Let H be the R-submodule of $\mathbb{Z}_\infty$ generated by $z_1, \cdots, z_n \in \mathbb{Z}_\infty$, and K be the S-submodule of $\mathbb{Q}_\infty$ generated by $z_1, \cdots, z_n$. Since K is a finitely generated module over a principal ideal domain, $K = F \oplus U$, where F is a free S-module of rank r and U is the S-torsion submodule of K.

The action of B on F is isomorphic to the product of r shifts on $\mathbb{Q}_\infty$. Hence (F, B) is Bernoulli.

Since an element of $\mathbb{Z}_\infty$ is annihilated by an element of R if and only if it is annihilated by an element of S, the R-torsion submodule T of H is $H \cap U$. It follows that U is the increasing union of the R-submodules $(m!)^{-1}T$. Thus in order to show that (U, B) is Bernoulli, it suffices to show by the Monotone Theorem that each $((m!)^{-1}T, B)$ is Bernoulli. Since the action of B on $(m!)^{-1}T$ is isomorphic to its action on T, we are reduced to considering (T, B).

We claim that T is a finite rank, free abelian group. Once this is established, then (T, B) is Bernoulli by the Torus Theorem. Since R is noetherian, T is generated over R by a finite number of elements, say $y_1, \cdots, y_k$. There are polynomials $f_i(x)$ in $\mathbb{Z}[x]$ with $f_i(B)y_i = 0$. The set of elements $\{B^j y_i : 0 \leqq j \leqq \deg f_i,\ 1 \leqq i \leqq k\}$ depends on only a finite number of coordinates in $\mathbb{Z}_\infty$, and since T consists of linear combinations of these elements, the same is true of T. Hence T is contained in the finite rank, free abelian group generated by the coordinates where T is nonzero, and so T itself is a finite rank, free abelian group.

Thus we have shown that B is Bernoulli on both F and U. This proves that B is Bernoulli on $F \oplus U = K$. Since H is an invariant subgroup of K, we have B Bernoulli on H by the Factor Theorem. This completes the proof.

REMARK 1. Essentially the same proof shows that an ergodic endomorphism of $\mathbb{T}^\infty$ onto itself is Bernoulli, that is, that its natural extension is measure isomorphic to a Bernoulli shift. The only modifications necessary are an extension of the Torus Theorem to endomorphisms (see [5]) and replacement of R and S by $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, respectively.

REMARK 2. The algebraic techniques used here are not as special as the reader may surmise. Using them together with an idea of B. Weiss we can show that Theorem 1 is true for $\mathbb{T}^\infty$ replaced by any group whose dual is a torsion group.

3. Finite entropy

It is natural to ask whether there are any ergodic automorphisms of $\mathbb{T}^\infty$ with finite entropy. By *entropy* we mean either topological or Haar measure theoretic entropy, since these coincide for group automorphisms [1].

The most direct way of constructing an automorphism A of $\mathbb{T}^\infty$ is to multiply automorphisms A_i of finite dimensional tori. Then A is ergodic if and only if the same is true of each A_i. If $h(A)$ denotes the entropy of A, then $h(A) = h(A_1) + h(A_2) + \cdots$. Thus in order for this process to yield an ergodic A with finite entropy, it is sufficient that there exist ergodic automorphisms of finite dimensional tori with arbitrarily small entropy. Theorem 2 below shows this is also necessary.

Let A_0 be an automorphism of $\mathbb{T}^n$. With respect to the standard basis on the dual group $\mathbb{Z}^n$, the dual automorphism of A_0 is given by an $n \times n$ integer-valued matrix with determinant ± 1. If $f(x) = \prod_1^n (x - \lambda_i) \in \mathbb{Z}[x]$ is the characteristic polynomial of this matrix, then it is known that (see [3])

$$(*) \qquad h(A_0) \equiv h(f) = \sum_{|\lambda_i| > 1} \log |\lambda_i|.$$

The roots λ_i are by definition algebraic integers whose product is ± 1. Kronecker [6] proved that if all the conjugates of an algebraic integer lay on the unit circle, then they must be roots of unity. Since A_0 is ergodic if and only if $f(x)$ has no roots which are roots of unity (see [4]), it follows that $h(A_0) > 0$ if A_0 is ergodic.

The problem of minimizing the right-hand side of (*) for ergodic automorphisms dates back about forty years to a paper of D.H. Lehmer [7], where it arose while

using a technique to factor large integers. It is still unknown whether this quantity can be arbitrarily small. In the same paper Lehmer found the smallest value known to date, namely log 1.176280821, which corresponds to

$$f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1.$$

C.L. Siegel [11] showed that if just one of the λ_i is on or outside the unit circle (that is, this root is a Pisot-Vijayaraghavan number), then the logarithm of the positive root of $x^3 - x - 1$ (about $\log 1.324$) is the smallest possible. Finally, P.E. Blanksby and H.L. Montgomery [2] have proved that

$$h(A_0) \geqq \log\left(1 + \frac{1}{52n \log 6n}\right),$$

where A_0 acts ergodically on $\mathbb{T}$.

THEOREM 2. *Ergodic automorphisms of $\mathbb{T}^\infty$ with finite entropy exist if and only if there are ergodic automorphisms of finite dimensional tori with arbitrarily small entropy.*

PROOF. Sufficiency follows from the above remarks.

Conversely, suppose A is an ergodic automorphism of $\mathbb{T}^\infty$ with $h(A) < \infty$. Consider the dual automorphism B on $\mathbb{Z}_\infty$, and treat $\mathbb{Z}_\infty$ as an $R = \mathbb{Z}[x, x^{-1}]$ module as in the previous section. We claim that $\mathbb{Z}_\infty$ is a torsion R-module. Suppose the contrary. Then there would be a $z \in \mathbb{Z}_\infty$ such that for any nonzero polynomial $f(x)$, $f(B)z \neq 0$. Then the action of B on Rz would be isomorphic to the shift on $\mathbb{Z}_\infty$. This means $(\mathbb{T}^\infty, A)$ would have a factor isomorphic to the shift on $\mathbb{T}^\infty$. Since the entropy of the shift is infinite and entropy can only drop when passing to factors, we obtain the contradiction $h(A) = \infty$.

We now establish an R-module analogue of the primary decomposition for abelian groups, splitting up most of $\mathbb{Z}_\infty$ using irreducible polynomials instead of prime numbers. Recall that irreducibility in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ coincide by the Gauss lemma. Let $p(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$, and put

$$H(p) = \{z \in \mathbb{Z}_\infty : p(B)^k z = 0 \text{ for some } k \geqq 1\}.$$

Then for distinct irreducibles $p(x)$ and $q(x)$ the corresponding R-submodules $H(p)$ and $H(q)$ have trivial intersection. For if $z \in H(p) \cap H(q)$, there are k and m such that $p(B)^k z = 0 = q(B)^m z$. Since p^k and q^m are relatively prime in $\mathbb{Q}[x]$, there are $r(x)$ and $s(x)$ in $\mathbb{Q}[x]$ with $r(x)p(x)^k + s(x)q(x)^m \equiv 1$. For some integer n we have

$nr(x)$, $ns(x) \in \mathbb{Z}[x]$. Then $nz = nr(B)p(B)^k z + ns(B)q(B)^m z = 0$, which forces $z = 0$.

Also note that $\mathbb{Z}_\infty / \oplus H(p)$ is a torsion group. For any $z \in \mathbb{Z}_\infty$ is annihilated by some polynomial $f(x)$ with relatively prime coefficients. Let

$$f(x) = p_1(x)^{e_1} \cdots p_m(x)^{e_m}$$

be its decomposition into irreducibles, which can be chosen to be in $\mathbb{Z}[x]$ by the Gauss lemma. Put $f_i(x) = f(x)/p_i(x)^{e_i}$. Then the $f_i(x)$ are relatively prime polynomials, so as before there are $r_i(x) \in \mathbb{Z}[x]$ with $r_1(x)f_1(x) + \cdots + r_m(x)f_m(x) \equiv n \in \mathbb{Z}$. Then $r_i(B)f_i(B)z \in H(p_i)$, so that $nz \in H(p_1) \oplus \cdots \oplus H(p_m)$. This shows that $\mathbb{Z}_\infty / \oplus H(p)$ is indeed a torsion group.

We employ finiteness of entropy again to show that each $H(p)$ has finite group rank rk $H(p)$. An argument similar to one in the proof of Theorem 1 shows that $H(p)$ is the increasing union of finite rank invariant subgroups. If K is such a subgroup, then since a power of $p(B)$ annihilates K, the characteristic polynomial of B restricted to K has the form $p(x)^k$, where $k \cdot \deg p = \text{rk } K$. We denote the entropy of $\hat{B}$ on $\hat{K}$ by $h(K, B)$. Then $h(K, B) = h(p^k) = k \cdot h(p)$, where $h(p)$ is defined as in (*). Hence

$$\frac{\text{rk } K}{\deg p} h(p) = h(K, B) \leqq h(A).$$

This shows that

$$\text{rk } H(p) \leqq \frac{h(A) \deg p}{h(p)} < \infty.$$

Since $\mathbb{Z}_\infty / \oplus H(p)$ is a torsion group, and each $H(p)$ has finite rank, infinitely many of the $H(p)$ are nonzero. On these B is aperiodic, so that $h(H(p), B) > 0$ if $H(p) \neq 0$. By the additivity of entropy over direct sums,

$$\sum_p h(H(p), B) = h(\oplus_p H(p), B) \leqq h(\mathbb{Z}_\infty, B) = h(A) < \infty.$$

Hence there are $H(p)$ on which B has arbitrarily small entropy, and the duals of these $H(p)$ are isomorphic to finite dimensional tori. This finishes the proof.

References

1. K. R. Berg, *Convolutions of invariant measures, maximal entropy*, Math. Systems Theory 3 (1969), 146–150.

2. P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. **18** (1971), 355–369.

3. Rufus Bowen, *Entropy for group automorphisms and homogeneous spaces*, Trans. Amer. Math. Soc. **153** (1971), 401–414.

4. P. R. Halmos, *On automorphisms of compact groups*, Bull. Amer. Math. Soc. **49** (1943), 619–624.

5. Y. Katznelson, *Ergodic automorphisms of T^n are Bernoulli*, Israel J. Math. **10** (1971), 186–195.

6. L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **53** (1857), 173–175.

7. D. H. Lehmer, *Factorization of cyclotomic polynomials*, Ann. of Math. **34** (1933), 461–479.

8. D. S. Ornstein, *Two Bernoulli shifts with infinite entropy are isomorphic*, Advances in Math. **5** (1970), 339–348.

9. D. S. Ornstein, *Factors of Bernoulli shifts are Bernoulli shifts*, Advances in Math. **5** (1970), 349–364.

10. V. A. Rokhlin, *Metric properties of endomorphisms of compact commutative groups*, Amer. Math. Soc. (2) **64** (1967), 244–252.

11. C. L. Siegel, *Alegbraic integers whose conjugates lie in the unit circle*, Duke Math. J. **11** (1944), 597–602.

Department of Mathematics
University of California
Berkeley, California, U. S. A.