

191
111
F
1
2
6-2-2

THE ENTROPY OF AUTOMORPHISMS OF
SOLENOIDAL GROUPS

T.Ward.

2
6-2-2
[scribble]

Submitted in partial fulfilment of the requirements for
the degree of Master of Science in the Department of
Mathematics at the University of Warwick.

September, 1986.

Acknowledgements

I would like to thank Doug Lind for suggesting this topic and my supervisor, Klaus Schmidt, for his continual help. Thanks also to Mark Eyeington for many helpful conversations.

I acknowledge the financial support of the Science and Engineering Research Council.

Introduction

S.A.Yuzvinskii calculated the Haar measure theoretic entropy of an endomorphism of a solenoidal group in (9). D.Lind stated without proof the equivalence of Yuzvinskii's formula to one involving Bowen entropies of the induced endomorphisms on vector spaces over all inequivalent completions of the rationals as stated in (5). The proof of this was outlined in a lecture by D.Lind at the L.M.S. conference on Ergodic Theory at the University of Durham in 1980.

In this dissertation we follow through the suggestion implicit in (5). In the first section the solenoid is described explicitly (Theorem 1.3) and is identified with a quotient group of the group of adeles Q_A .

In the second section the Haar measure theoretic entropy of an automorphism of the one-dimensional full solenoid is calculated directly using finite partitions (Theorem 2.3). This result is shown to be equivalent to that of Abramov (1). The direct calculation is included largely to show how the maps considered act on the solenoid, and in particular to show why they are bijections.

In the third section an automorphism of the d -dimensional solenoid $(Q^*)^d$ is considered. The Haar measure theoretic entropy of this is shown to be equivalent to the Bowen entropy of the induced map on the adèle space, and this is calculated. This gives the result of D.Lind. We then show the equivalence of this formula to that of Yuzvinskii. Throughout we use relationships between the zeros and the coefficients of a polynomial over a non-archimedean field

The fourth section is a direct generalisation of the third. Here, the Haar measure theoretic entropy of an auto-

morphism of the solenoid obtained from an algebraic number field, k , is found. We also give an abstract derivation of the solenoid k^* in terms of the group of adeles k_A .

Throughout we wish to describe the solenoids in such a way that the intuitive view of entropy in terms of stretching along axes gives the correct result.

The description of the solenoid as a quotient of the group of adeles can be found in (8) and in a rather different form in (2). The result of section two is proved by different methods in (1). The result of section three is stated in (5) and is derived using different methods in (9). The result in section four is formally original but is a very direct extension of the preceding sections.

I would like to express my thanks to Doug Lind for several very helpful conversations at Warwick during July 1986.

Notation

K is the additive group $[0,1)$. When G is a locally compact abelian group G^* is the Pontryagin dual of G . We use the following results without comment:-

$$G^{**} = G ; \quad G^*/H^\perp = H^*$$

when H is a closed subgroup of G . (See Hewitt and Ross, (2)).

When $k(Q)$ is an algebraic number field, $k_v(Q_p)$ is the completion at a finite place $v(p)$, and $r_v(Z_p)$ is the unique maximal compact subring of $k_v(Q_p)$. $k_A(Q_A)$ is the group of adeles and $k(Q)$ is always considered to be embedded diagonally in the group of adeles. Following Weil(8) we call a given k_v a quasi-factor of the group of adeles.

Section One: The Solenoid Q^*

Lemma 1.1:-The groups Z_p^* and $Q^{(p)}/Z$ are isomorphic as topological groups.

Proof.

Let e_p^k be the character on a cyclic group of order p^k defined by:-

$$e_p^k(1) = \exp(2\pi i/p^k)$$

and call the group generated by this character C_p^k . Then:-

$$Z_p^* = \varinjlim (C_p^k, \text{'raising to } p^{\text{th}} \text{ power' })$$

Similarly, if we write $Q(p,k) = \{p^{-k}a : a \in \mathbb{Z}\}$, then:-

$$Q^{(p)}/Z = \varinjlim (Q(p,k)/Z, \text{'multiplication by } p \text{'})$$

and notice that each $Q(p,k)$ is cyclic of order p^k .

Define a map from Z_p^* into $Q^{(p)}/Z$ in the natural way - if $\chi \in Z_p^*$ appears first in C_p^k so that $\chi = (e_p^k)^n$ and the kernel is $p^{k+1}Z_p$, then map this character to the rational n/p^k . This map is clearly an epimorphism and is injective since an image can be written in only one way as n/p^k with $n = 0, \dots, p^k-1$. This map is also a homeomorphism since both the groups are discrete. ■

Lemma 1.2:-The groups $(\prod_p \mathbb{Z}_p)^*$ and Q/Z are isomorphic as topological groups.

Proof.

We claim that any $x \in Q/Z$ can be written uniquely in the form:-

$$x = \sum_{p \in P} n_p / p^{(k_p)} \quad (1)$$

where $0 \leq n_p \leq p^{k_p}-1$ and P is a finite set of primes.

The existence of the decomposition (1) is equivalent to a solution in integers for the equation:-

$$\sum_i y_i (p_1^{\alpha_i} \dots \hat{p}_i^{\alpha_i} \dots p_n^{\alpha_n}) = N$$

where $x = N/p_1^{\alpha_1} \dots p_n^{\alpha_n}$, and this is always possible since Z is a principal ideal domain. We can then add or subtract multiples of $p_i^{\alpha_i}$ from y_i to make all the coefficients lie in the correct range.

The expression (1) is unique:-

$$\sum_{p \in P'} m_p / p^{(j_p)} = \sum_{p \in P} n_p / p^{(k_p)} \quad \text{mod } 1$$

implies that the order of this element of Q/Z is uniquely

$$\prod_p p^{(k_p)}$$

so that $P = P'$ and $k_p = j_p$ for each $p \in P$. Thus:-

$$\sum (n_p - m_p) / p^{(k_p)} \in \mathbb{Z}$$

and $\sum_{p' \in P} (n_{p'} - m_{p'}) \prod_{p \in P \setminus \{p'\}} p^{(k_p)}$ is an integer divisible by $\prod_p p^{(k_p)}$

So p divides $(n_{p'} - m_{p'})$ and therefore $n_{p'} = m_{p'}$.

Define a character on $\prod_p \mathbb{Z}_p$ for each rational between zero and one, written as at (1), by $((e_p^{k_p})^{n_p})$. Notice this is the trivial character on all but finitely many places since P is finite. This assignment clearly defines a monomorphism. To see that this is surjective notice that any character trivial on all but finitely many places must take the above form and the set of such characters is dense in $(\prod_p \mathbb{Z}_p)^*$ since it separates points. Surjectivity follows since $(\prod_p \mathbb{Z}_p)^*$ is discrete.

The map is a homeomorphism since both of the groups are discrete. ■

By duality, lemma 1.2 shows that $(Q/Z)^*$ is isomorphic to $\prod Z_p$ and they will be identified below without comment.

Let $X = (Q/Z)^*$. This is a subgroup of Q^* with (Q^*/X) isomorphic to Z^* since $X = Z^\perp$ in Q^* . So there is a short exact sequence:-

$$\begin{array}{ccccccc} 0 & \longrightarrow & X & \longrightarrow & Q^* & \longrightarrow & Q^*/X \longrightarrow 0 \\ & & \downarrow \cong & & & & \downarrow \cong \\ & & \prod Z_p & & K & & \end{array}$$

Thus Q^* is a central extension of K (the dual of Z) defined by a symmetric cocycle $w: K \times K \longrightarrow \prod Z_p$.

Consider the cocycle $w(a,b) = -\text{Int}(a+b) \cdot \underline{1}$, where $\underline{1}$ is the multiplicative unit in $\prod Z_p$, $(1,1,\dots)$. Then the group $G = \text{Ext}_w(K,X)$ has binary operation:-

$$(a, \underline{x}) + (b, \underline{y}) = (a+b, \underline{x} + \underline{y} - \text{Int}(a+b) \cdot \underline{1})$$

and is therefore isomorphic to $(R \times X)/Y$ where $Y = \{(n, n \cdot \underline{1}) : n \in \mathbb{Z}\}$.

Make G into a topological group with the product topology from the usual topologies on K and on X .

Any continuous character on $R \times X$ has the form:-

$$(a, n) \cdot (b, \underline{x}) = \exp(2\pi i ab) \cdot \prod (e_p^k)^n (x_p) \quad (2)$$

where $a \in \mathbb{R}$, $\underline{x} = (x_2, x_3, x_5, \dots)$ is an element of X and n is a map from the set of all primes into the positive integers which is zero on all but finitely many primes.

In order for such a character to be trivial on Y , we need:-

$$(a, n) \cdot (1, 1 \cdot \underline{1}) = 1$$

Thus $a = -\sum \frac{n_p}{p^{k_p}}$ so a is rational and uniquely determines and is uniquely determined by (n_p, k_p) as before.

Thus G^* is isomorphic to Q and so by duality the solenoid Q^* is given by G . Notice that G is compact. A basis of open sets at the identity in $R \times X$ is given by all sets of the form:-

$$O(m, n) = (-1/m, 1/m) \times \prod p^{n_p} Z_p$$

where m is a positive integer and n is as at (2). Thus a basis of open sets at the identity in G is given by all the sets:-

$$U(m, n) \cup V(m, n)$$

where $U(m, n) = [0, 1/m) \times \prod p^{n_p} Z_p$ and $V(m, n) = (1-1/m, 1) \times \prod p^{n_p} Z_p$.

We have proved the following theorem.

Theorem 1.3:-The solenoid Q^* is isomorphic to $\text{Ext}_W(K, X)$. A basis of open sets at the identity is given by all sets of the form $U(m, n) \cup V(m, n)$.

Corollary 1.3:-The solenoid is isomorphic to Q_A/Q where Q is embedded in the adele diagonally.

Proof.

A fundamental set of Q_A modulo Q is:-

$$K \times \prod Z_p \quad (\text{Weil, p.65})$$

and the binary operation is precisely that given by the cocycle w when representatives are chosen to lie in this set. A basis of open sets at the identity in the adele takes the same form as $O(.,.)$ above. ■

Section Two: Entropy of an automorphism of Q^*

Let $S:Q \longrightarrow Q$ be an automorphism. Then $S(x) = r \cdot x$ for some rational r . S induces a dual automorphism T of the solenoid Q^* by translation:- $(T\chi)(x) = \chi(Sx)$.

When Q^* is described as in Corollary 1.3 and r is a prime q say, then the action of T is:-

$$T(a, \underline{x}) = (qa - \text{Int}(qa), q\underline{x} - \text{Int}(qa) \cdot \underline{1})$$

In order to describe the action of T^{-1} , embed each Z_p into Q_p and use "Int" to describe the integer part of a p -adic number. Also write, for $\underline{x} \in \prod Z_p$, x_q^0 for the units digit in the q -adic component of \underline{x} . We now claim that:-

$$T^{-1}(a, \underline{x}) = ((q+a-x_q^0)/q, \text{Int}((\underline{x} + \text{Int}(qa) \cdot \underline{1})/q))$$

This is checked directly:-

$$\begin{aligned} T^{-1} \cdot T(a, \underline{x}) &= T^{-1}(qa - \text{Int}(qa), q\underline{x} - \text{Int}(qa) \cdot \underline{1}) \\ &= ((q+qa - \text{Int}(qa) - (T\underline{x})_q^0)/q, \text{Int}(q\underline{x}/q)) \\ &= (a+1 - (T\underline{x})_q^0 - (\text{Int}(qa))/q, \underline{x}) \end{aligned}$$

Now notice that $\text{Int}(qa) = 0, 1, \dots$, or $q-1$ so:-

$$\begin{aligned} (T\underline{x})_q &= q(x_q^0 + x_q^1 \cdot q + \dots) - \text{Int}(qa) \\ &= (q - \text{Int}(qa)) + (x_q^0 - 1) \cdot q + x_q^1 \cdot q^2 + \dots \end{aligned}$$

So even if $x_q^0 = 0$, $(x_q^0 - 1) \cdot q + \dots$ lies in qZ_q , and so the units component vanishes. Similarly, $T \cdot T^{-1}$ is the identity.

Remarks:-

(1) T is q -to-1 on K and '1-to- q ' on Z_q . The choice of image point in Z_q is made depending on the position in K , thus removing the ambiguity and making the map on the whole space bijective.

(2) Haar measure μ on Q^* is given by the product measure $m \times \prod m_p$ where m is normalised Haar measure on K and m_p is normalised Haar measure on Z_p . This is so because a translation on Q^* acts by a translation on each of the components.

Lemma 2.1:- The Haar measure theoretic entropy of T on Q^* is $\log q$, and a full entropy factor is $K \times Z_q$.

Proof.

Define the partition P^m of Q^* to be the product of the following partitions:-

- on K into the intervals $[i/m!, (i+1)/m!)$ for $i = 0, 1, \dots, m!-1$.
- on each Z_p into the p^m p -adic cylinders each defined by prescribing the first m digits. Each such set has m_p -measure $1/p^m$.

Notice that P^{m+1} is a refinement of P^m so that:-

$$\bigvee_{m=0}^{\infty} P^m = \lim_{m \rightarrow \infty} P^m$$

and this is clearly equal to the point partition modulo null sets. Thus (Walters, p.99):-

$$h_{\mu}(T) = \lim_{m \rightarrow \infty} h_{\mu}(T, P^m) \quad (3)$$

To calculate $h_\mu(T, P^m)$, observe that the partition $\bigvee_{i=0}^{n-1} T^{-i} P^m$ is the product of the partitions:-

- on K into the intervals $[i/(m!q^{n-1}), (i+1)/(m!q^{n-1}))$ when $m > q$. There are $m!q^{n-1}$ such sets, each of m -measure $1/m!q^{n-1}$.
- on each Z_p ($p \neq q$) into the sets of the original partition P^m . This is because each application of T^{-1} maps the partition on Z_p onto itself, merely permuting the elements.
- on Z_q into P^m again. This is because each application of T^{-1} maps the partition P^n onto P^{n-1} .

Thus $K \times Z_q$ is a full entropy factor for the system (T, Q^*) . That is, the entropy of T is equal to the entropy of T modulo the invariant factor $\prod_{p \neq q} Z_p$ acting on $Q^*/\prod_{p \neq q} Z_p$. With a minor abuse of notation use the same letters for maps and partitions and for their quotients by this invariant factor.

Then:-

$$\begin{aligned}
 h_\mu(T, P^m) &= \lim (1/n) H_\mu \left(\bigvee_{i=0}^{n-1} T^{-i} P^m \right) \\
 &= \lim (1/n) H_\mu (T^{-(n-1)} P^m) \\
 &= \lim (1/n) \sum_{i=0}^{m!q^{n-1}-1} (1/m!q^{n-1}) \log (m!q^{n-1}) \\
 &= \lim (1/n) \log (m!q^{n-1}) \\
 &= \log q
 \end{aligned}$$

Thus by (3):- $h_\mu(T) = \log q$

■

Lemma 2.2:-The Haar measure theoretic entropy of T^{-1} on Q^* is $\log q$, and a full entropy factor is KxZ_q .

Proof.

Use the same partition P^m and the result (3). Then $\bigvee_{i=0}^{n-1} T^i P^m$ is the partition:-

- on K into P^m itself. This is because each application of T maps P^m onto P^{m-1} so that if $n > \max(m!, q)$, $T^n P^m$ is the trivial partition.
- on Z_p ($p \neq q$) into P^m itself for the same reason as in Lemma 2.1; since q is prime to $p \neq q$, "multiplying" or "dividing" by q is an isometry fixing the lattice Z_p .
- on Z_q , TP^m is the natural partition into q^{m+1} sets (i.e. P^{m+1}) so that we obtain the natural partition by cylinders into q^{m+n-1} sets, each of m_q -measure $1/(q^{m+n-1})$.

So KxZ_q is a full entropy factor for T^{-1} and by the same abuse of notation as in Lemma 2.1:-

$$\begin{aligned}
 h_\mu(T^{-1}, P^m) &= \lim (1/n) H_\mu \left(\bigvee_{i=0}^{n-1} T^i P^m \right) \\
 &= \lim (1/n) \sum_{j=0}^{q^{n+m-1}-1} (1/q)^{n+m-1} \log(q^{n+m-1}) \\
 &= \lim (1/n) \log(q^{n+m-1}) \\
 &= \lim (1+(m-1)/n) \log q \\
 &= \log q
 \end{aligned}$$

Thus by (3):- $h_\mu(T^{-1}) = \log q$ ■

Now return to the map T induced by multiplication by a general rational r on Q .

Theorem 2.3:-The Haar measure theoretic entropy of T acting on Q^* is given by:-

$$h_\mu(T) = \sum \log|r|_p$$

where the sum is taken over all inequivalent places of Q at which the norm of r exceeds one. We include the real place and real norm formally as one of the places p .

Proof.

This follows immediately from the above lemmas: a full entropy factor is $Kx \prod_p Z_p$ where P is the set of primes appearing in the numerator or denominator of r . Since this is a finite product we have by the same abuse of notation as above:-

$$h_\mu(T) = h_m(T \text{ on } K) + \sum_p h_{m_p}(T \text{ on } Z_p)$$

and the result follows by noticing from the proofs of the two lemmas that on each Z_p only powers of the prime p appearing in r can do anything other than permute elements of a partition. ■

Remarks:-

(1)The "full entropy factors" chosen above are chosen so as to include all of the stretching and contracting parts of T and to ensure that the quotient map is well-defined. They therefore do contain some factors not contributing to the entropy.

(2)If we write $r=m/n$, with $(m,n)=1$ and n positive then the above formula becomes:-

$$h_{\mu}(T) = \max\{\log n, \log |m|\}$$

which is the result in Abramov's paper (1).

(3) The above calculations do not easily extend to higher dimensions so in the next section we find a full entropy factor for a map covering T in the form of a finite product of finite-dimensional vector spaces over completions of the rationals.

Section Three: Higher-dimensional Solenoids

Use the construction of Corollary 1.3 so that $(Q^*)^d$ is identified with $(Q_A/Q)^d$ and let T be an automorphism of $(Q^*)^d$ dual to some element (t_{ij}) of $GL_d(Q)$.

Let $\pi: Q_A \longrightarrow Q_A/Q$ be the canonical epimorphism. Then the following diagram commutes:-

$$\begin{array}{ccc} Q_A^d & \xrightarrow{T'} & Q_A^d \\ \pi \downarrow & & \downarrow \pi \\ (Q^*)^d & \xrightarrow{T} & (Q^*)^d \end{array}$$

where T' is the map on the covering space defined by the same matrix as was T .

Remarks:-

(1) The automorphism T on $(Q^*)^d$ is an affine transformation of a compact group so that (Walters, p.197) if μ is Haar measure on $(Q^*)^d$ then:-

$$h_\mu(T) = h(T)$$

where h with no suffix means topological entropy.

(2) Since Q_A^d has a countable basis of open sets at the identity, (see Section One or Weil, p.59) it is a metrizable topological group (Hewitt and Ross, p.70) and a translation invariant metric can be chosen. One such metric is:-

$$d'(\underline{x}, \underline{y}) = \|\underline{x} - \underline{y}\| + \sum_p \|\underline{x}_p - \underline{y}_p\| / 2^p$$

where $\|x_\omega - y_\omega\| = (\sum_{i=1}^d |x_\omega^i - y_\omega^i|^2)^{1/2}$ and $\|x_p - y_p\|_p = (\sum_{i=1}^d |x_p^i - y_p^i|^2)^{1/2}$.

Convergence is guaranteed since for all but finitely many places x_p and y_p both lie in \mathbb{Z}_p^d so that:-

$$\|x_p - y_p\|_p \leq \sqrt{d} \text{ for all but finitely many } p.$$

Then the quotient metric d induced on $(Q^*)^d$, given by:-

$$d(a, b) = \inf \{d'(\underline{x}, \underline{y}) : \pi(\underline{x}) = a, \pi(\underline{y}) = b\}$$

defines the topology of $(Q^*)^d$.

Also notice that $\pi: ((Q_A)^d, d') \longrightarrow ((Q^*)^d, d)$ is a local isometry since Q^d is discrete in Q_A^d .

(3) T is uniformly continuous on $(Q^*)^d$ by compactness. T' is uniformly continuous on Q_A^d since it is uniformly continuous on each quasi-component Q_p^d or \mathbb{R}^d and it is an isometry on all but finitely many places. This is because the elements of T' are rationals and for any rational r , $|r|_p = 1$ for all but finitely many p .

Thus, by (Walters, p.199), the topological entropy of T on $(Q^*)^d$ is identical to the topological entropy of T' on Q_A^d .

Putting all three remarks together we conclude:-

$$h_\mu(T) = h(T')$$

Lemma 3.1:- If P is the set of primes appearing in the numerator or denominator of elements of T , then $\mathbb{R}^d_x \prod_{p \in P} Q_p^d$ is a full entropy factor for T' .

Proof.

Similar to Lemmas 2.1 and 2.2. If $p \notin P$, then T' fixes the lattice Z_p^d in Q_p^d and can therefore not contribute to the entropy. Alternatively, notice as above that on such a Q_p^d , T' is an isometry. ■

So the problem is now reduced to finding the topological entropy of T' on the finite cartesian product $R^d \times \prod_p Q_p^d$, where T' acts as an automorphism of each component. Firstly, since P is finite:-

$$h(T') = h(T' \text{ on } R^d) + \sum_P h(T' \text{ on } Q_p^d)$$

Lemma 3.2:- $h(T' \text{ on } R^d) = \sum \log |s_i|$ where the sum is taken over all eigenvalues of T with modulus exceeding one.

Proof.

See Walters p.201. ■

In the sequel, write $\text{spec}_p(T')$ for the roots of the characteristic polynomial of T regarded as a polynomial over Q_p in some splitting extension of Q_p for this polynomial.

Let $p(x) = \det(T - x \cdot I_d)$ be the characteristic polynomial of T' and by the usual embedding $Q \subset Q_p$ regard p as a member of $Q_p[x]$.

Define the following metrics on Q_p^d :-

$$d(x, y) = \max_i \{ |x_i - y_i|_p \}$$

$$d_n(x, y) = \max_o \{ d(T'^i x, T'^i y) \}$$

Let $p(x) = p_1^{m_1}(x)p_2^{m_2}(x)\dots p_s^{m_s}(x)$ where each p_i is irreducible over Q_p . Then T' is similar to a matrix M in primary rational canonical form (Hungerford, p.360).

Remarks:-

(1) M has the form:-

$$M = \begin{bmatrix} \boxed{M_1} & & \\ & \boxed{M_2} & \\ & & \ddots \\ & & & \boxed{M_t} \end{bmatrix}$$

where each M_i is the companion matrix to $p_i^{m_i}(x) = x^{r_i} + a_{r_i-1}x^{r_i-1} + \dots + a_0$ so that:-

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ & & \ddots & & \\ & & & \ddots & \\ & & & & 1 \\ -a_0 & \dots & \dots & \dots & -a_{r-1} \end{bmatrix}$$

$$\text{Thus } h(M, Q_p^d) = \sum_i h(M_i, Q_p^{r_i})$$

Also notice that $r_1 + r_2 + \dots + r_t = d = m_1 \deg(p_1) + \dots + m_t \deg(p_t)$.

(2) Notice that $h(M) = h(T')$ since if $M = S(T')S^{-1}$ where S is in $GL_d(Q)$ then $M^n = S^1(T')^n S^{-1}$ so that the metrics d_n defined by T' and the corresponding metrics defined by M are uniformly equivalent.

(3) Let the solutions of p_i be $s_1, \dots, s_{r_i/m}$ in F , the splitting field for p_i over Q_p . So, counted according to multiplicity, each s appears m_i times in $\text{spec}_p(T')$ or $\text{spec}_p(M)$. For brevity,

call a given M_i and p_i M and p .

The unique norm on F that extends the usual p -adic norm on Q_p is:-

$$|x|_p = |N_{F/Q_p}(x)|^{1/\deg(x)}$$

where $\deg(x)$ is the degree of the minimal monic polynomial over Q_p that has x as a zero.

Notice that $|s_i|_p = |s_1|_p$ for all i since there is an isometric member of $\text{Gal}(F:Q_p)$ interchanging any two roots of p .
(see Koblitz, p.60 ff.)

In this case we have:-

$$p^m(x) = x^r + a_{r-1}x^{r-1} + \dots + a_0$$

and so:- $p(x) = x^{r/m} + \dots + (a_0)^{1/m}$

and hence:- $|s_i|_p = |a_0|_p^{1/r}$

Since each coefficient of p^m is a symmetric polynomial in the roots s_j this gives an upper bound on the size of the coefficients:-

$$|a_{r-i}|_p \leq |a_0|_p^{(r/m^2) - (i/m)}$$

(4) The bound on the coefficients in (3) now gives an easy description of the metrics d_n .

The action of M is as follows:-

$$M(x-y) = \begin{bmatrix} x_1 - y_1 \\ \vdots \\ a_0(x_0 - y_0) - \dots - a_{r-1}(x_{r-1} - y_{r-1}) \end{bmatrix}$$

and so:-

$$d_n(x, y) = \max_0^{r-1} \{ |x_i - y_i|_p, |a_i|_p |x_i - y_i|_p, \dots, |a_i|_p^{n-1} |x_i - y_i|_p \}$$

Then if $|a_0|_p \leq 1$, $d_n = d$ and we get $h(M, Q_p^r) = 0$.

Lemma 3.3:- $h(M, Q_p^r) = \sum_{|s_i|_p > 1} m \cdot \log s_i$

$$= \begin{cases} 0 & \text{if } |s_i|_p \leq 1 \\ r \cdot \log s_1 & \text{by remarks.} \end{cases}$$

Proof.

From (4) above, assume without loss of generality that $|s_1|_p > 1$ so that $|a_0|_p^{1/m} > 1$.

We then have:-

$$d_n(x, y) = |a_0|_p^{n-1} \cdot \max \{ |x_i - y_i|_p \}$$

by the remarks.

Thus a minimal (n, ε) -spanning set for the compact set Z_p^r is:-

$$S = \{x \in Z_p^r : \text{the first } m \text{ co-ordinates of each } x_i \text{ are fixed}\}$$

where m is the smallest positive integer satisfying:-

$$p^{-m} < \varepsilon/2 \cdot |a_0|_p^{n-1}$$

The cardinality of S is $r \cdot p^m$.

So, to within a factor $\mu \in (1/p, p]$, we have the equality:-

$$r_n(\varepsilon, Z_p^r) = \mu r \cdot (2|a_0|_p^{n-1})/\varepsilon$$

Then:-

$$r(\varepsilon, Z_p^r) = \limsup (1/n) \log r_n(\varepsilon, Z_p^r)$$

$$= \limsup (1/n) \log (\mu r \cdot 2 \cdot |a_0|_p^{n-1} / \varepsilon)$$

$$= \limsup (1-1/n) \log (2(\mu r)^{(1/(n-1))} |a_0|_p / \varepsilon^{1/(n-1)})$$

$$= \log |a_0|_p$$

Hence:-

$$h(M, Z_p^r) = \log |a_0|_p$$

$$= r \cdot \log |s_1|_p$$

$$= \sum_{i=1}^{r/m} m \log |s_i|_p$$

Now notice that $h(M, p^{-N} Z_p^r) = h(M, Z_p^r)$ where $p^{-N} Z_p^r = (p^{-N} Z_p^r)^r$ for any integer N by a similar calculation:-

$$r_n(\varepsilon, p^{-N} Z_p^r) = \mu r \cdot (2 |a_0|_p^{n+N-1})/\varepsilon$$

so as n tends to infinity in the expression for $r(\varepsilon, p^{-N} Z_p^r)$ we get:-

$$r(\varepsilon, p^{-N} Z_p^r) = r(\varepsilon, Z_p^r)$$

Lastly, let K be any compact set in Q_p^r . Then there exists an N such that $p^{-N} Z_p^r \supset K$ so (Walters, p.172) we have:-

$$h(M, p^{-N} Z_p^r) \geq h(M, K)$$

Thus:-

$$\begin{aligned} h(M) &= \lim h(M, p^{-N} Z_p^r) \\ &= h(M, Z_p^r) \\ &= \begin{cases} 0 & \text{if } |s_1|_p < 1 \\ r \cdot \log |s_1|_p & \text{otherwise} \end{cases} \end{aligned}$$

Theorem 3.4:-The Haar measure theoretic entropy of T on $(Q^*)^d$ is given by:-

$$h_\mu(T) = \sum \log |s_{i,p}|_p$$

where $\{s_{i,p}\} = \text{spec}_p(T)$ and the sum is taken over all places and all eigenvalues with p -adic norm exceeding one. Here we formally include the real place as the "infinite" place.

Proof.

This is all shown above:-

$$h_\mu(T) = h(T') \quad \text{by the end of the remarks}$$

$$= h(T' \text{ on a finite full entropy factor})$$

$$= \sum_{p \in \mathcal{P} \cup \{\infty\}} h(T', Q_p^d)$$

$$= \sum_{|s_i| > 1} \log |s_i| + \sum_p \sum_i^t h(M_i \cdot Q_p^r)$$

$$= \sum_{|s_i| > 1} \log |s_i| + \sum_j \sum_p \log |s_{j,p}|_p$$

Remarks.

(1) Yuzvinskii's formula for the Haar measure theoretic entropy of T is:-

$$h_{\mu}(T) = \log s + h(T \text{ on } \mathbb{R}^d) \quad (1)$$

where s is the least common denominator of the coefficients of the characteristic polynomial of T .

Lind states in (5) that this is equivalent to the sum of the entropies of the induced maps on all the inequivalent places of Q . He also has the expression in 3.4.

In order to show the equivalence of Theorem 3.4 and (1) above, we will use the following facts about Newton polygons from Koblitz.

Let $f(x) = x^d + b_{d-1}x^{d-1} + \dots + b_0$ be a polynomial over Q_p and let F be a splitting field with p -adic norm extending that on Q_p as used above. The Newton polygon of f is defined to be the convex hull of the points $(i, \text{ord}_p b_i)$ with the convention that $\text{ord}_p 0 = \infty$. Then if a segment of the polygon has slope μ and horizontal length N then f has exactly N zeroes s_i with $\text{ord}_p(s_i) = -\mu$. The converse is clearly true.

Let f as above be the characteristic polynomial of T . Notice that:-

$$\log s = \sum_r \log |1/s|_p$$

-this is true of any positive integer.

At a given prime p where $\text{ord}_p(s)$ is strictly positive so that this place contributes to the above sum, we can assume by the arguments used in the remarks of this section that f is

irreducible over \mathbb{Q}_p . Then:-

$$|b_{d-i}|_p \leq |b_0|_p^i$$

$$\text{so that:-} \quad \text{ord}_p(b_{d-i}) \geq i \cdot \text{ord}_p(b_0) \quad (a)$$

Let $\text{ord}_p s = n = -\text{ord}_p(b_{d-i})$ for some i . We then have:-

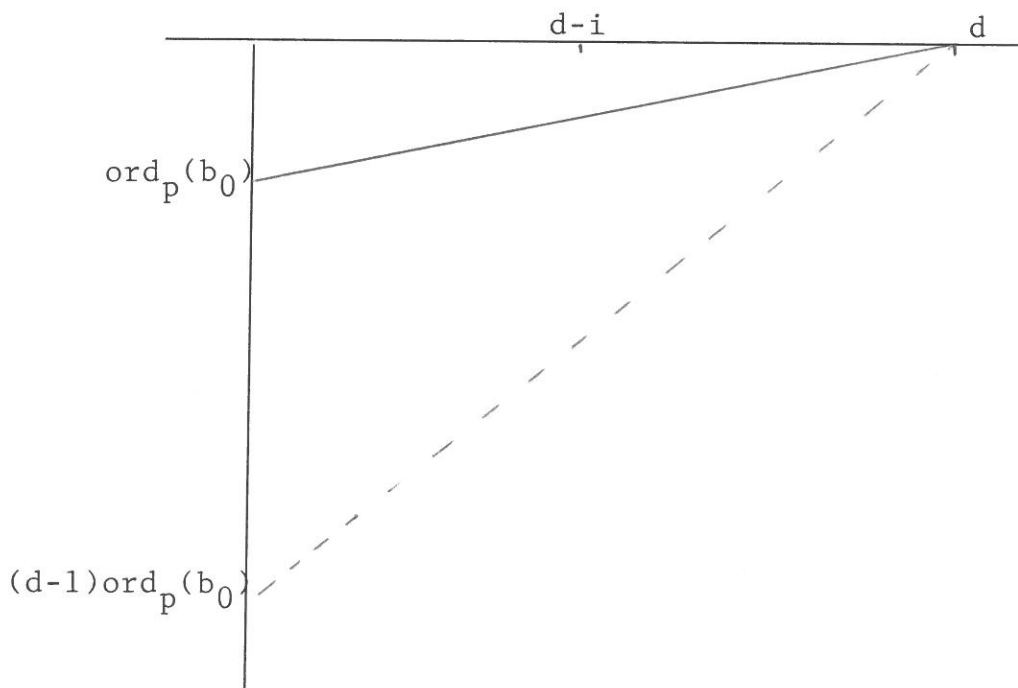
$$\text{ord}_p(b_j) \geq \text{ord}_p(b_{d-i}) \text{ for all } j. \quad (b)$$

By the remark (3) all the zeros of f have:-

$$|s_i|_p = |s_1|_p = |b_0|_p^{1/d}$$

$$\text{so that:-} \quad \text{ord}_p(s_i) = \text{ord}_p(b_0)/d$$

So the Newton polygon has the shape:-



(a) requires that all the points lie above the dotted line. (b) requires all the points to lie above the horizontal line through $(d-i, \text{ord}_p(d-i))$. However, all the roots have the same order so all the points must lie above the solid line also. These three conditions can only be satisfied if $i=d$. That is:-

$$\text{ord}_p s = -\text{ord}_p(b_0)$$

Thus, $|1/s|_p = |b_0|_p = |s_1|_p^d$. This means that:-

$$\log|1/s|_p = \sum \log|s_i|_p$$

This shows the equivalence of Theorem 3.4 and Yuzvinskii's formula (1).

(2) The above results show that the action of T on the solenoid locally is very simple. At a neighbourhood of the origin, the solenoid looks like a cartesian product of real lines and p -adic Cantor sets and the entropy agrees with the "stretching" done by T in each of the "directions" associated with eigenvectors.

Section Four: Solenoids from Algebraic Number Fields

In this section we check that nothing goes wrong when Q is replaced by k in the preceding sections, where k is an algebraic extension of the rationals. We also explain the observation made in Corollary 1.3.

Lemma 4.1:-The group of adeles of an algebraic number field is isomorphic to its dual. The isomorphism is determined by any character on k_A which vanishes on k but is not trivial.

Proof.(See Weil,p.60ff)

Consider the case $k = Q$ first. We can define non-trivial characters on Q_A which are trivial on Q since Q is discrete in the group of adeles. One such character μ can be obtained by setting:-

$$\mu_{\infty}(x_{\infty}) = \exp(-2\pi i x_{\infty})$$

and letting μ_p be trivial on each Z_p . Notice that any continuous character on Q_A must be trivial on all but finitely many of the Z_p since it must restrict to a continuous character on an infinite product of compact groups.

The character induced on a given quasi-factor by μ can be found as follows. If $x \in Q^{(p)}$ then $x \in Z_q$ for all primes $q \neq p$ so that:-

$$\mu(x) = \mu_{\infty}(x) \mu_p(x) = 1$$

since the character is trivial on Q . Thus:-

$$\mu_p(x) = \exp(2\pi i x)$$

This determines μ_p completely since Q is dense in Q_p and μ is continuous.

Notice from the above that we can write:-

$$\mu = \prod_p \mu_p$$

including the real place as one of the p 's and with convergence guaranteed since the μ_p are trivial on all but finitely many Z_p and when evaluated on a given adele, the adele will be in Z_p for all but finitely many places.

Now let μ' be any element of Q_A^* . Then, since each Q_p is a non-discrete field, and each μ_p is non-trivial we have:-

$$\mu'_p(x) = \mu_p(a_p x)$$

for some a_p in Q_p , and this a_p is uniquely determined by the above equation.

As usual, μ'_p must be trivial on all but finitely many Z_p . Now notice that 1 is the topological generator of each Z_p so this condition is exactly equivalent to requiring that $\mu_p(a_p) = 1$ for all but finitely many p . Thus $\underline{a} = (a_p)$ is itself an adele and we can write:-

$$\mu'(\underline{x}) = \mu(\underline{a} \cdot \underline{x})$$

This mapping from Q_A^* into Q_A is therefore surjective. It is easily seen to be a monomorphism and continuous. Duality then shows this map to be a homeomorphism.

For the case where k is an algebraic extension of Q , we simply identify k with Q^n as additive groups and notice that $(Q^n)_A$ - the adele group of a vector space - is still isomorphic to k_A (see Weil, p.62) and this isomorphism sends $(Z_p)^n$ to r_v in all but finitely many places, where v is a place above p . What this means is that we can find a character on k_A by which to do the same construction as we did for Q_A . If w_1, \dots, w_n is a Q -basis for k then we could choose the character:-

$$\bar{\mu}(\underline{x}_1 w_1 + \dots + \underline{x}_n w_n) = \mu(\underline{x}_1 + \dots + \underline{x}_n)$$

Notice also that the kernel of the character induced by μ on Q_p (and hence by $\bar{\mu}$ on k_v) is exactly $Z_p(r_v)$ for all but finitely many p (v). ■

Lemma 4.2:-The solenoid k^* is isomorphic to k_A/k .

Proof.

We are done if we can show that the mapping in 4.1 sends k^\perp to k . This is clear:- if $\bar{\mu}'(x) = 1$ for all $x \in k$ and $\bar{\mu}'(x) = \bar{\mu}(\underline{a}x)$ then $\underline{a}x \in k$ for all $x \in k$ so that $\underline{a} \in k$. ■

Let w_1, \dots, w_n be an integral basis for k over Q . Then if v is a place of k lying above the place p of Q we have:-

$$r_v = w_1 Z_p + \dots + w_n Z_p$$

Put $F_\omega = \{t_1 w_1 + \dots + t_n w_n : 0 \leq t_i < 1\}$. Then:-

$$k_A/k = F_\omega \times \prod_v r_v$$

Now consider an automorphism of $(k^*)^S$ given by a matrix T in $GL_S(k)$. We have $(k^*)^S = F_{\infty}^S \times \prod_V r_V^S$.

As in section three, $(k^*)^S$ is a compact metrizable group and T is an affine transformation so that the Haar measure theoretical entropy of T is equal to the topological entropy. Further, we have a commuting diagram with a locally isometric projection π :-

$$\begin{array}{ccc} (k_A)^S & \xrightarrow{T'} & (k_A)^S \\ \pi \downarrow & & \downarrow \pi \\ (k_A/k)^S & \xrightarrow{T} & (k_A/k)^S \end{array}$$

Thus the problem is reduced to finding the topological entropy in the sense of Bowen of the lifted automorphism T' acting on the adèle space $(k_A)^S$.

Lemma 4.3:-A full entropy factor for T' on $(k_A)^S$ is:-

$$(\bigoplus_i w_i R)^S \times \prod_V k_V^S$$

where V is the finite set of places at which any one of $|t_{ij}|_V$, $|\det T|_V$ takes on a value not equal to one.

Proof.

Section three, mutatis mutandis. The lattice r_V^S is clearly fixed at any place not in V and therefore such a quasi-factor cannot contribute to the entropy. ■

Thus we have reduced the problem to that of finding the Bowen entropy of T' acting on k_V^S for a given v .

Consider first a finite place v . As in section three, we can assume without loss of generality that T is in primary- k_v rational canonical form. So T is the direct sum of block matrices of the form:-

$$M = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & & & & \vdots \\ \vdots & & & & 1 \\ -b_0 & \dots & \dots & \dots & -b_{r-1} \end{bmatrix}$$

where $p(x) = x^r + b_{r-1}x^{r-1} + \dots + b_0$ is the characteristic polynomial of M and is an irreducible element of $k_v[x]$.

So we only need to find the Bowen entropy of M on k_v^r .

Lemma 4.4:- On a finite place v , we have:-

$$h(M \text{ on } k_v^r) = \begin{cases} \log |b_0|_v & \text{if } |b_0|_v > 1 \\ 0 & \text{if } |b_0|_v \leq 1 \end{cases}$$

Proof.

We observe that the metric d_n is given by:-

$$\begin{aligned} d_n(\underline{x}, \underline{y}) &= \max_{j=0}^{n-1} \{ |T^j x_i - T^j y_i|_v \} \\ &= \max \{ |b_0|_v^n \cdot d_1(\underline{x}, \underline{y}), d_1(\underline{x}, \underline{y}) \} \end{aligned}$$

Then on the compact set $r_v = w_1 Z_p + \dots + w_n Z_p$ the same calculation as in section three yields:-

$$h(T, r_v^r) = \begin{cases} \log |b_0|_v & \text{if } |b_0|_v > 1 \\ 0 & \text{if } |b_0|_v \leq 1 \end{cases}$$

and hence the required formula. ■

We now sum the entropies over all the blocks at this place to obtain:-

$$h(T \text{ on } k_v^S) = \sum \log |s_i|_v$$

where $\{s_i\} = \text{spec}_v(T)$ and the sum is taken over all eigenvalues with norm exceeding one.

The entropy of T' on an infinite place is clearly given by the same formula with v replaced by an infinite place.

Summing the above results over the finite full entropy factor we obtain the following analogue of Theorem 3.4:-

Theorem 4.5:-The Haar measure theoretic entropy of T on the solenoid $(k^*)^S$ is given by:-

$$h_\mu(T) = \sum \log |s_{i,v}|_v$$

where $\{s_{i,v}\} = \text{spec}_v(T)$ and the sum is taken over all places and all eigenvalues with norm at the place v exceeding one. Here we include the infinite places as some of the v 's.

Remark.

We can also easily describe the analogue of section one. An element of k^X is an automorphism of k and induces an automorphism of k^* . Notice that $t \in k^X$ has $|t|_v = 1$ for all but finitely many places and t is therefore an element of the group of ideles when embedded. (That is, t has a multiplicative inverse in the group of adeles).

As usual, the Haar measure theoretic entropy of the action of t is equal to the topological entropy of t acting as an idele on the group of adeles. Here there is a finite full entropy factor and we obtain:-

$$h_{\mu}(t \text{ on } k^*) = \sum \log |t|_v$$

where the sum is taken over all finite and infinite places at which the norm of t exceeds one.

Bibliography

- (1) L.M.Abramov; "The entropy of an automorphism of a solenoidal group". Theory of Probability and its Applications 4, 231-236. (1959)
- (2) E.Hewitt and K.Ross; "Abstract Harmonic Analysis", Volume I. Springer-Verlag (1963).
- (3) T.W.Hungerford; "Algebra". Springer-Verlag (1974).
- (4) N.Koblitz; "p-adic numbers, p-adic analysis, and Zeta-functions" Springer-Verlag (1977).
- (5) D.Lind; "p-adic entropy", in L.M.S. Conference on Ergodic Theory University of Durham.(List of abstracts). (1980)
- (6) J.Tate; "Fourier Analysis in Number Fields and the Hecke Zeta-function", PhD. Thesis, Princeton (1950) = Chapter XV in "Algebraic Number Theory", ed. Cassels and Frohlich, Academic Press (1967).
- (7) P.Walters; "An Introduction to Ergodic Theory", Springer-Verlag (1982).
- (8) A.Weil; "Basic Number Theory", Springer-Verlag (1974).
- (9) S.A.Yuzvinskii; "Computing the Entropy of a group of endomorphisms", Siberian Maths Journal, 8, 172-178, (1967).