Periodic Points in S–Integer Dynamical Systems

Vijay Chothi

A thesis submitted at the University of East Anglia
in partial fulfilment of the requirements for the degree of
Doctor of Philosophy.

June 1996

To my mother and father, Sunil and Veena.

Acknowledgements

I would like to thank Graham Everest and Tom Ward, under the kind supervision of whom this thesis has ebbed and flowed towards fruition. The former, for sharing his technical expertise and eternal optimism, the latter, for his 'never say die' attitude towards research not to mention meticulous proof–reading. I acknowledge the financial support of the S.E.R.C. for the first three years of this research.

Abstract

This thesis is a study of the dynamical system associated to the ring of S–integers in an $\mathbf{A}$–field. Arithmetic examples of such systems interpolate between the well–documented toral endomorphisms and automorphisms of the full d–dimensional solenoid $\hat{\mathbf{Q}}^d$. The geometric analogue is an original class of examples, subsuming certain cellular automata, which it is natural to investigate simultaneously. We compute the topological entropy of these systems and give criteria for ergodicity and expansiveness, appealing to results by Bowen, Eisenberg, Lind/Ward and Tate. This leads to a strengthening of the interplay between arithmetic and geometric dynamics.

In Chapter 4 we try to understand how the cardinality of the set of points of period n grows with n. There are non–expansive examples in this class of algebraic systems which have logarithmic growth rate of periodic points equal to the entropy, but possess irrational zeta functions. We enter the realm of recurrence sequences and the question of the existence of intermediate limit points comes under scrutiny. Waddington's idea for proving that the periodic points of an ergodic toral automorphism are uniformly distributed is given an arithmetic generalisation to the special class of ergodic S–integer systems (Chapter 5). Using a deep result of Heath–Brown on the Artin problem, we construct an example that on the one hand mimics expansive behaviour (in that the upper growth rate of periodic points is positive) and on the other hand is highly non–expansive (in that it locally has infinitely many isometric directions). We then present examples inspired by conjectures of Artin and Mersenne which yield (conjectorial) examples with other behaviour.

In the arithmetic case, it is well–known that the entropy is equal to the logarithmic Mahler measure of an integral polynomial associated with the action. The final Chapter uses methods of Everest to generalise the classical Mahler measure to $\mathbf{A}$–fields. We deduce that the entropy in the geometric case is also equal to its geometric Mahler measure.

The Appendix is a paper written with Graham Everest and Thomas Ward in which the notion of oriented local entropy is introduced, and it is shown how the global entropy of a $\mathbf{Z}^2$–action on a compact connected metrisable group may be decomposed into a sum of such local contributions. In this paper also, periodic points are used to analyse a class of dynamical systems.

Contents

Chapter 1

Introduction

1.1 Measure Theory

A *measurable space* is a set X with a collection of subsets $\mathcal{B}$ of X such that

1. $X \in \mathcal{B}$,
2. if $B \in \mathcal{B}$ then $X \setminus B \in \mathcal{B}$,
3. if $B_n \in \mathcal{B}$ then $\bigcup_{n=1}^{\infty} B_n \in \mathcal{B}$.

Such a collection $\mathcal{B}$ is called a *σ–algebra* of subsets and the elements of $\mathcal{B}$ are the *measurable sets.*

A *finite measure* on the space $(X, \mathcal{B})$ is a map $m : \mathcal{B} \to \mathbf{R}_{>0}$ satisfying $m(\emptyset) = 0$ and $m(\bigcup_{n=1}^{\infty} B_n) = \sum_{n=1}^{\infty} m(B_n)$ if $\{B_n\}$ is a pairwise disjoint collection of measurable sets. If, in addition, $m(X) = 1$, then $(X, \mathcal{B}, m)$ is a *probability space.*

If X is a topological space, then the *Borel σ–algebra* is the smallest σ–algebra defined on X that contains all the open sets, and a measure on X is a *Borel measure* if it is defined on the Borel σ–algebra.

1.2 Haar Measure

Haar measure is a generalisation of Lebesgue measure on the real line to locally compact groups and was first introduced by A. Haar [14] in 1933. Indeed, on the real line Haar measure coincides with Lebesgue measure (up to normalisation). The measure is defined on any locally compact (Hausdorff) topological group X and is the unique translation invariant Borel measure (up to a positive multiplicative constant). A proof of this can be found in either Weil [60] or Cartan [8], whose elegant proof of existence and uniqueness avoids Tychonoff's Theorem. The translation invariance of Haar measure μ on X means that $\mu(Bx) = \mu(B)$ for all $x \in X$ and $B \in \mathcal{B}$, the collection of measurable sets.

Furthermore, if X has the structure of a compact group, then the Haar measure μ can be normalised to give a Borel probability measure on X. The existence of Haar measure means that we can define $L^p(\mu)$ spaces and integration.

Examples

1. $X = \mathbf{T}$ the additive circle, μ is normalised Lebesgue measure.

2. X is a finite group, $\mu(B) = \frac{1}{|X|} \times |B|$ for any $B \subseteq X$.

3. $X = \mathbf{Z}_p$ (p–adic integers), $\mu\left(a + p^n \mathbf{Z}_p\right) = \frac{1}{p^n}$ for all $a \in \mathbf{Z}_p, n \in \mathbf{N}$.

1.3 Duality Theory

Definition 1.1 A *topological group* G is a topological space carrying a group structure and satisfying the following conditions:

1. the mapping $(x, y) \to xy$ of $G \times G$ onto G is a continuous mapping of the Cartesian product $G \times G$ onto G;

2. the mapping $x \to x^{-1}$ of G onto G is continuous.

We will use the term *LCA group* to mean a locally compact Hausdorff abelian topological group.

Definition 1.2 A *character* χ of a LCA group G is a continuous homomorphism from G into the unit circle $\mathbf{T}$. The collection of all characters is called the *dual group* of G, and is denoted by $\hat{G}$. Sometimes we write $< g, \chi >$ for $\chi(g)$ to emphasise that it is a pairing between G and $\hat{G}$.

We can topologise $\hat{G}$ as follows. For $K \subset X$ compact and $r > 0$ let

$$N_{K,r} = \{\chi : |\chi(g) - 1| < r \text{ for all } g \in K\}.$$

Then these sets form a base for a topology on $\hat{G}$. This topology is called the topology of uniform convergence on compact subsets, and is denoted by UCC.

Theorem 1.1 *If G is any LCA group then $\hat{G}$, endowed with the UCC–topology, is also a LCA group.*

Proof. See Theorem 10 in [33].

□

We quote the following results which can be found in [16].

1. (Pontryagin–van Kampen Duality Theorem). Let Γ denote the dual group of a LCA group G. For fixed $g \in G$, let $\chi : \Gamma \to \mathbf{T}$ be given by $\chi(\gamma) = \gamma(g)$ for all $\gamma \in \Gamma$. Then the map defined by $\alpha(g)(\gamma) = \chi(\gamma)$ for all $\gamma \in \Gamma$ is a topological group isomorphism between G and $\hat{\Gamma}$. A proof can be found in [16], Theorem 24.8.

2. G is compact if and only if $\hat{G}$ is discrete.

3. If G is compact, then G is connected if and only if $\hat{G}$ is torsion free, and G is zero–dimensional if and only if $\hat{G}$ is torsion.

4. If $H \subset G$ is a closed subgroup then G/H is a LCA group in the quotient topology. The *annihilator* of H, defined as

   $$H^{\perp} = \{\chi \in \hat{G} : \chi(h) = 1 \text{ for all } h \in H\},$$

   is a closed subgroup of $\hat{G}$. We have

(i) $\widehat{G/H} \cong H^{\perp}$.

(ii) $\hat{G}/H^{\perp} \cong \hat{H}$.

(iii) $H^{\perp\perp} \cong H$.

5. A homomorphism $T : G \to H$ of LCA groups induces a dual homomorphism $\hat{T} : \hat{H} \to \hat{G}$ defined by $(\hat{T}\gamma)(x) = \gamma(T(x))$. The map $\hat{T}$ is injective (resp. surjective) if and only if T is surjective (resp. injective).

6. If G is compact then the elements of $\hat{G}$ form an orthonormal basis for $L^2(G)$. As a consequence, each $f \in L^2(G)$ has a *Fourier series* representation

$$f = \sum_{\gamma \in \hat{G}} a_\gamma \gamma$$

where a_γ are uniquely determined complex numbers. Putting $G = \mathbf{T}$ yields the classical Fourier series.

7. The *Fourier transform* of any $f \in L^1(G)$ is the complex–valued function $\hat{f}$ on the dual group $\hat{G}$, defined by

$$\hat{f}(\chi) = \int_G f(g) < -g, \chi > dg$$

where the integration is with respect to Haar measure.

Definition 1.3 A *solenoid* is a finite dimensional, connected, compact abelian group. Equivalently, it is dual to a finite rank, torsion free, discrete abelian group, that is, to an additive subgroup of $\mathbf{Q}^d$ for some $d \geq 1$. For the *full solenoid* $\hat{\mathbf{Q}}$ there is a description in terms of quotients of adele rings, see Theorem 3 Section 4.2 in [59].

Lemma 1.1 *The dual of any endomorphism of a d–dimensional solenoid is an element of $GL(d, \mathbf{Q})$.*

1.4 Dynamical Systems

Let X be a compact topological space and $T : X \to X$ a continuous map. The pair (X, T) is a *topological dynamical system.* Continuous maps $T : X \to X$ and $S : Y \to$

Y are *topologically conjugate* if there exists a homeomorphism map $\phi : X \to Y$ such that $S \circ \phi = \phi \circ T$, so that the following diagram commutes:

$$\begin{array}{ccc} X & \stackrel{T}{\to} & X \\ \phi \downarrow & & \downarrow \phi \\ Y & \stackrel{S}{\to} & Y \end{array}$$

Topological conjugacy is an equivalence relation on the space of all continuous maps. If T is topologically conjugate to S then T^n is topologically conjugate to S^n for all $n \in \mathbf{Z}$, so T^n and S^n have the same number of fixed points. If a continuous map has the property that the set of points of period n,

$$Fix_n(T) = \{x \in X : T^n(x) = x\},$$

is finite for all $n \geq 1$, then we may encode the periodic point data into a single function, the *dynamical zeta function* of (X, T). This is defined (formally) as in [49] by

$$\zeta_T(z) = \exp\left(\sum_{n=1}^{\infty} |Fix_n(T)| \times \frac{z^n}{n}\right),$$

for any $z \in \mathbf{C}$ where this converges. The inspiration for this definition is the Weil zeta function of an algebraic variety over a finite field, the rationality of which was proved by Dwork (see Chapter V in [21]). The importance of a rational zeta function is that there exist algebraic complex numbers $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_u$ such that all conjugates of an α is an α, all conjugates of a β is a β, and we have

$$|Fix_n(\theta)| = \sum_{i=1}^{t} {\alpha_i}^n - \sum_{i=1}^{u} {\beta_i}^n \qquad (1)$$

for all $n \geq 1$. Thus $|Fix_n(\theta)|$ is completely determined for all $n \geq 1$ by a finite amount of data (the poles and zeros, with multiplicities, of ζ_T). Clearly ζ_T is an invariant of topological conjugacy.

1.5 Topological Entropy

The topological entropy of a dynamical system (X, T) was first introduced by Adler, Konheim and McAndrew in [2] as an invariant of topological conjugacy. It is a non–negative real number or ∞ denoted by $h(T)$. The original definition used open covers of a compact topological space X. Let α be an open cover of X and let $N(\alpha)$ denote the least cardinality of a finite subcover of α. The *join* of two open covers, $\alpha \vee \beta$, is defined to be the open cover by sets of the form $A \bigcap B$ where $A \in \alpha, B \in \beta$. The topological entropy with respect to α is defined by

$$h(T, \alpha) = \lim_{n \to \infty} \frac{1}{n} \log N \left(\bigvee_{i=0}^{n-1} T^{-i} \alpha \right)$$

and the topological entropy of T is given by

$$h(T) = \sup_{\alpha} h(T, \alpha)$$

where α ranges over all open covers of X.

Bowen [5] gave a new definition of topological entropy using (n, ϵ)–generators (or spanning sets) for X a metric space. His definition coincides with that of Adler, Konheim and McAndrew on compact metric spaces, and has the advantage of extending the concept of topological entropy to the class $UC(X, d)$ of uniformly continuous maps of spaces which are not necessarily compact. His definition will prove to be useful later on and we now present the details.

1.6 Bowen Entropy

Let (X, d) be a metric space and $T : X \to X$ be a uniformly continuous map. Let n be a natural number, $\epsilon > 0$ and $K \subset X$ compact. A set $F \subset X$ is called an (n, ϵ)–generator for K if for every $x \in K$ there exists $y \in F$ such that

$$d(T^j(x), T^j(y)) \leq \epsilon \text{ for all } 0 \leq j \leq n.$$

This means that every point of K stays ϵ-close to some point of F for at least n iterations of T. Let $r_n(\epsilon, K)$ denote the least cardinality of any (n, ϵ)–generator for K with respect to T. We claim that $r_n(\epsilon, K) < \infty$. Since K is compact there exists a finite covering $\{U_1, \ldots, U_m\}$ of K by sets with diameter less than or equal to ϵ. Now choose a point y in every non–empty set of the form

$$\bigcap_{j=0}^{n} T^{-j}(U_{i_j}), \tag{2}$$

where $1 \le i_j \le m,\ \ 0 \le j \le n$. We have selected at most m^n points and these form an (n, ϵ)–generator for K with respect to T. To see this, take $x \in K$, and for each $0 \le j \le n$ take i_j such that $T^j(x) \in U_{i_j}$, so x is an element of the set in (2). If $y \in K$ is chosen in accordance with (2) then $d(T^j(x), T^j(y)) \le \epsilon$ for $0 \le j \le n$ since $T^j(x),\ \ T^j(y) \in U_{i_j}$, which has diameter less than or equal to ϵ. Hence $r_n(\epsilon, K) \le m^n$. Thus

$$\limsup_{n\to\infty} \frac{1}{n} \log r_n(\epsilon, K) \tag{3}$$

is finite. The *topological entropy* of T is defined as

$$h(T) = \sup_K \left\{ \lim_{\epsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} \log r_n(\epsilon, K) \right\}, \tag{4}$$

where K runs over all compact subsets of X. This is the definition due to Bowen [5]. Since $r_n(\epsilon, K) \to \infty$ as $\epsilon \to 0$, the lim sup in (3) increases as $\epsilon \to 0$. So the limit in (4) exists, although it can be infinite. We need the lim sup in (4) because there are examples of maps for which $\{\frac{1}{n} \log r_n(\epsilon, K)\}_{n=1}^{\infty}$ diverges for arbitrarily small ϵ, see section 7.2 Remark (14) in [56]. If X is compact, then it can be shown that

$$h(T) = \lim_{\epsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} \log r_n(\epsilon, X).$$

See Corollary 7.5.2 in [56] for a proof of this. In a nutshell, $h(T)$ is a measure of the growth rate in n of the number of orbits of length n up to a small error.

1.7 Calculating Topological Entropy

The topological version of the Kolmogorov–Sinai Theorem (see Theorem 7.11 in [56]) allows us to compute $h(T)$ for some examples. An open cover α of X is a *topological generator* for T if for every sequence $\{A_k\}_{k\in\mathbf{Z}}$ where each A_k is an element of α, the intersection $\bigcap_{k\in\mathbf{Z}} T^{-k} A_k$ contains no more than one point of X. The topological version of Kolmogorov–Sinai is then: if α is a generator for T then, $h(T) = h(T, \alpha)$.

Examples

1. Let T be the shift action on $X = \{0, 1, \ldots, m-1\}^{\mathbf{Z}}$ given by

$$T(\{x_n\}) = \{x_{n+1}\} \text{ for all } n \in \mathbf{Z}.$$

We can easily construct a generator α for T by defining

$$A_j = \left\{ x = \{x_n\}_{-\infty}^{\infty} \in X : x_0 = j \right\}$$

and setting $\alpha = \{A_0, A_1, \ldots, A_{m-1}\}$. Then by the topological Kolmogorov–Sinai Theorem,

$$\begin{aligned} h(T) = h(T, \alpha) &= \lim_{n\to\infty} \frac{1}{n} \log N \left(\bigvee_{i=0}^{n-1} T^{-i}\alpha \right) \\ &= \lim_{n\to\infty} \frac{1}{n} \log m^n \\ &= \log m. \end{aligned}$$

2. If A is a toral endomorphism, then the dual endomorphism $\hat{A}$ is an element of $GL(d, \mathbf{Z})$ for some $d \geq 1$. It is well–known that the topological entropy is

$$h(A) = \sum_{i=1}^{d} \log^+ |\lambda_i|,$$

where $\lambda_1, \ldots, \lambda_d$ are the eigenvalues of $\hat{A}$ counted with multiplicity. See Section 8.4 in [56] for the details.

3. More generally, Yuzvinskii has shown in [63], using complicated linear algebra, that if A is an endomorphism of a solenoid then

$$h(A) = \log s + \sum_{i=1}^{d} \log^+ |\lambda_i|, \qquad (5)$$

where $\lambda_1, \ldots, \lambda_d$ are the eigenvalues of the rational matrix $\hat{A}$ (viewed as an element of $GL(d, \mathbf{Q})$) and s is the lowest common multiple of the denominators of the coefficients of the characteristic polynomial of $\hat{A}$. See [28] for an alternative adelic approach to proving (5).

4. Let $f = \sum_{k\in\mathbf{Z}} c_k u^k$ be a polynomial in $\mathbf{Z}[u^{\pm 1}]$ (with $c_k \neq 0$ for finitely many k), and consider the dynamical system (X, α) defined by

$$X = \left\{ x \in \mathbf{T}^{\mathbf{Z}} : \sum_{k\in\mathbf{Z}} c_k x_{k+n} = 0 (\mathrm{mod} 1) \text{ for all } n \in \mathbf{Z} \right\},$$

and by setting α equal to the shift action on X. Then

$$h(\alpha) = \log |c_m| + \sum_{i=1}^{m} \log^+ |\lambda_i|, \tag{6}$$

where c_m is the leading coefficient of f and $\lambda_1, \ldots, \lambda_m$ are the roots of f. The proof exploits a topological conjugacy between (X, α) and the automorphism of an m–dimensional solenoid determined by the companion matrix of f (see [20] Section 12 and [24]), so Yuzvinskii's formula may be applied to this rational matrix to compute the entropy.

Formula (6) has a very interesting generalisation to higher dimensions. Let X be a compact abelian group and $Aut(X)$ the group of continuous automorphisms of X. A $\mathbf{Z}^d$–action on X by automorphisms is a homomorphism $\alpha : \mathbf{Z}^d \to Aut(X)$. Such an action may be defined by specifying d commuting automorphisms of X, $U_1, \ldots, U_d$ say, and then setting the image $\alpha_{\mathbf{n}} = \alpha_{(n_1,\ldots,n_d)} = U_1^{n_1} \cdots U_d^{n_d}$ for $\mathbf{n} = (n_1, \ldots, n_d) \in \mathbf{Z}^d$. Kitchens and Schmidt [20] have shown that the $\mathbf{Z}^d$–action determines (and is determined by) a module M over the ring of Laurent polynomials $\mathcal{R}_d = \mathbf{Z}[u_1^{\pm 1}, \ldots, u_d^{\pm 1}]$. This correspondence is achieved by first defining the additive group M to be the dual group of X, then define automorphisms $\times u_1, \ldots, \times u_d$ to be the dual automorphisms of $\alpha_{(1,0,\ldots,0)}, \ldots, \alpha_{(0,\ldots,1)}$ respectively. Extending 'linearly' (by the structure of M as an additive group or $\mathbf{Z}$-module) makes M into an $\mathcal{R}_d$-module.

Conversely, if M is an $\mathcal{R}_d$-module, then multiplication by each of the u_j gives d commuting automorphisms of M. These correspond to a $\mathbf{Z}^d$–action α_M on the compact dual group X_M of M.

Now fix $d \geq 1$ and choose a non–zero polynomial $f \in \mathcal{R}_d$. From the above, setting $M = \mathcal{R}_d / < f >$ induces a $\mathbf{Z}^d$–action α_M on the compact group $X = X_M$. It has been proved in [29] that

$$h(\alpha) = \log M(f),$$

where

$$M(f) = \exp \left\{ \int_0^1 \cdots \int_0^1 \log |f(e^{2\pi i \theta_1}, \ldots, e^{2\pi i \theta_n})| d\theta_1 \ldots \theta_n \right\}$$

is the Mahler measure of f.

Chapter 2

S–Integer Dynamical Systems

2.1 Places of an A–Field

In [28], Yuzvinskii's formula (5) is decomposed into a sum of archimedean and p–adic contributions to give,

$$h(A) = \sum_{p \leq \infty} \sum_{i=1}^{d} \log^+ |\lambda_i{}^{(p)}|_p, \tag{7}$$

where $\lambda_1{}^{(p)}, \ldots, \lambda_d{}^{(p)}$ are the roots of the characteristic polynomial of $\hat{A}$ in some finite extension of $\mathbf{Q}_p$. Thus the $\log s$ term is actually just the sum over the non–archimedean primes. The framework for the proof of (7) is in Chapter IV of [59]. An analogous formula for an automorphism of k^d, k a number field, is obtained in [58].

Let k denote either the rational numbers $\mathbf{Q}$ or the field of rational functions in one variable over a finite field of constants, $\mathbf{F}_p(T)$, where p is a fixed rational prime. The p–adic absolute value on $\mathbf{Q}$ has a natural geometric analogue: the monic irreducible polynomials $\nu(T)$ of $\mathbf{F}_p(T)$ play the role of the finite primes in the arithmetic case, and the polynomial corresponding to the usual absolute value $|.|_\infty$ is conventionally chosen to be T^{-1}. The ν–adic absolute value on $\mathbf{F}_p(T)$ is defined as

$$|f|_\nu = p^{-ord_\nu(f) \cdot deg(\nu)}$$

where $ord_\nu(f)$ is the signed multiplicity with which ν divides the rational function $f(T)$. If $f(T) = \prod \nu(T)^{ord_\nu(f)}$ then define $deg(f) := \sum ord_\nu(f) \cdot deg(\nu)$. For the distinguished polynomial T^{-1}, $|f|_{T^{-1}} = p^{deg(f)}$. It is conventional to denote the distinguished metric on k by $|.|_\infty$ and if $\nu \neq \infty$ we write $\nu < \infty$. Analogously to the Artin–Whaples product formula we have

$$\prod_{\nu \leq \infty} |f|_\nu = 1.$$

This product formula extends to finite algebraic extensions of k, or **A**–fields in the terminology of Weil, which we now formalise.

The details for the following description of places of **A**–fields can be found in Chapter III Section 1 in [59]. Let M_L be the set of *places* on an **A**–field L (that is, equivalence classes of multiplicative valuations on L). A place ω is called *finite* if ω contains only non–archimedean valuations and *infinite* otherwise. The extension field L has only finitely many infinite places. The rational number field $\mathbf{Q}$ has only one infinite place, containing the usual absolute value, and a finite place for each prime p. In the infinite place we choose a representative $|.|_\infty$ equal to the usual absolute value. In the place corresponding to p (which we also denote by p) we choose the valuation $|.|_p$ such that $|p|_p = p^{-1}$. In the function field case $\mathbf{F}_p(T)$, there are no infinite places. There are finite places for each monic irreducible polynomial $\nu(T)$ in $\mathbf{F}_p(T)$ and also for the distinguished polynomial T^{-1}. We choose for each place corresponding to $\nu(T)$ (which we also denote by ν) the valuation $|.|_\nu$ as described above. In each place $\omega \in M_L$ we choose a valuation as follows. Let ν be an element of M_k such $\omega \mid \nu$ (that is, the restrictions to k of the valuations in ω belong to ν; in particular ω is infinite if and only if $\omega \mid \infty$). The *local degree* is the number defined by $d_\omega = [L_\omega : k_\nu]$ where L_ω and k_ν denote the completions of L at ω and k at ν, respectively. Choose the valuation satisfying

$$|\alpha|_\omega = |\alpha|_\nu^{d_\omega/d} \text{ for each } \alpha \in k,$$

where d is the degree of the extension $k \subset L$. Then the Artin–Whaples product formula holds for all valuations on L,

$$\prod_{\omega \in M_L} |\alpha|_\omega = 1 \text{ for all } \alpha \in L^*. \tag{8}$$

2.2 An Adelic Construction

Let k be an $\mathbf{A}$–field and let k_ν denote the completion of k with respect to the ν–adic metric $|.|_\nu$. For every finite place ν let $r_\nu = \{x \in k : |x|_\nu \leq 1\}$ denote the ring of ν–adic integers in k_ν – this is the maximal compact subring of k_ν, and let $r_\nu^* = \{x \in k : |x|_\nu = 1\}$ – this is the group of invertible elements of r_ν. Let S be any set of places of k not containing P_∞, the set of infinite places. For any such set S we define the following product,

$$k_{\mathbf{A}}(S) = \left\{ x = (x_\nu) \in \prod_{\nu \in S \cup P_\infty} k_\nu : |x_\nu|_\nu \leq 1 \text{ for almost every } \nu \right\},$$

where the phrase "almost every ν" means "all but a finite number of ν". Since each factor r_ν is compact and k_ν is locally compact, $k_{\mathbf{A}}(S)$ is locally compact under the product topology. This is an example of a *restricted direct product* first exhibited in this context in Tate's thesis [53]. We make $k_{\mathbf{A}}(S)$ into a ring by defining addition and multiplication component wise. Define the subring R_S of k by

$$R_S = \{x \in k : |x|_\nu \leq 1 \text{ for all } \nu \notin S \cup P_\infty\}.$$

Classically R_S is known as the ring of S*–integers*.

Examples

1. If $k = \mathbf{Q}$ and $S = \emptyset$, then $R_S = \mathbf{Z}$.
2. If $k = \mathbf{F}_p(T)$ and $S = \emptyset$, then $R_S = \mathbf{F}_p[T]$.
3. If $k = \mathbf{Q}$ and $S = \{2, 3\}$, then $R_S = \mathbf{Z}[\frac{1}{6}]$.
4. If $k = \mathbf{F}_p(T)$ and $S = \{T\}$, then $R_S = \mathbf{F}_p[T^{\pm 1}]$.

Let ξ be a non–zero element of R_S and let $\theta = \theta_\xi$ be the surjective endomorphism of the compact group $\hat{R}_S$, dual to multiplication by ξ on R_S. The pair $(\hat{R}_S, \theta)$ forms a dynamical system. Note that if we consider k to be a d–dimensional vector space over $\mathbf{Q}$ or $\mathbf{F}_p(T)$, where d is the degree of the extension, then $(\hat{R}_S, \theta)$ is isomorphic to a system of the form $(\hat{R}^d_{S^*}, \hat{\xi}^*)$, where

$$S^* = \{\nu : \omega \mid \nu \text{ for each } \omega \in S\}$$

and $\xi^* \in M_d(R_{S^*})$, the set of $d \times d$ matrices over the ring R_{S^*}. Thus the number field situation gives rise to an endomorphism of a finite–dimensional solenoid.

Examples

1. Let $k = \mathbf{Q}, S = \emptyset$ and $\xi = 2$. Then $R_S = \mathbf{Z}, \hat{R}_S = \mathbf{T}$ and θ is the circle doubling map.

2. Let $k = \mathbf{Q}, S = \{2\}$ and $\xi = 2$. Then $R_S = \mathbf{Z}[\frac{1}{2}]$, $\hat{R}_S$ is the solenoid $\widehat{\mathbf{Z}[\frac{1}{2}]}$ and θ is the automorphism of $\hat{R}_S$ dual to the automorphism $x \mapsto 2x$ of R_S.

3. Let $k = \mathbf{Q}, S = \{2, 3, 5, 7, 11, \dots\}$ and $\xi = \frac{3}{2}$. Then $R_S = \mathbf{Q}$ and θ is the automorphism of the full solenoid $\hat{\mathbf{Q}}$ dual to multiplication by $\frac{3}{2}$ on $\mathbf{Q}$.

4. Let ξ be an algebraic integer, $k = \mathbf{Q}(\xi)$ and $S = \emptyset$. Then R_S is the ring of integers in k. Taking $\xi = \sqrt{2}-1+i\sqrt{2\sqrt{2}-2}$ gives a non–expansive quasihyperbolic automorphism of the 4-torus (see Section 3 in [27]).

5. Let $k = \mathbf{F}_p(T), S = \emptyset$ and $\xi = T$. Then $R_S = \mathbf{F}_p[T], \hat{R}_S = \prod_{i=0}^{\infty}\{0, 1, \dots, p-1\}$ and θ is the one–sided shift on p symbols.

6. Let $k = \mathbf{F}_p(T), S = \{T\}$ and $\xi = T$. Then $R_S = \mathbf{F}_p[T^{\pm 1}]$, $\hat{R}_S = \prod_{-\infty}^{\infty}\{0, 1, \dots, p-1\}$ and θ is the two–sided shift automorphism on p symbols.

7. Let $k = \mathbf{F}_p(T), S = \{T\}$ and $\xi = T+1$. Then $\hat{R}_S$ is the two–sided shift space on p symbols, and θ is the cellular automaton defined by
$$(\theta(x))_m = x_m + x_{m+1} (\mathrm{mod} p).$$

Let φ be the diagonal embedding of R_S into $k_{\mathbf{A}}(S)$ given by $(\varphi(x))_\nu = x$ for all $x \in R_S, \nu \in S \cup P_\infty$. This map is well–defined since any $r \in R_S$ has $|r|_\nu \leq 1$ for almost every ν (see Theorem III.1.3 of [59]). The main result of this Chapter is the following theorem.

Theorem 2.1

$$h(\theta; \hat{R}_S) = \sum_\nu \log^+ |\xi|_\nu .$$

The arithmetic version of this quantity is the logarithmic height of an algebraic number. Abromov [1] proved Theorem 2.1 in the case $k = \mathbf{Q}$ where the map ξ is specified by a rational number m/n in lowest terms, so

$$h(\theta; \hat{\mathbf{Q}}) = \max\{\log|m|, \log|n|\}.$$

The following preliminary results give us information about R_S by identifying it with its natural image in $k_{\mathbf{A}}(S)$. The proofs are a straightforward extension of Weil's in [59] where he considers the case in which S comprises all finite places and embeds k in the adele ring $k_{\mathbf{A}}$.

Theorem 2.2 *$\varphi(R_S)$ is a discrete subgroup of $k_{\mathbf{A}}(S)$ and $k_{\mathbf{A}}(S)/\varphi(R_S)$ is compact.*

Proof. We first prove the Theorem for the case $k = \mathbf{Q}$ or $\mathbf{F}_p(T)$ and resolve later the generalisation to $\mathbf{A}$–fields.

Definition 2.1 For each $\nu \in S$ define a subring of R_S by

$$R_S^{(\nu)} = \{\alpha \in R_S : |\alpha|_\omega \leq 1 \text{ for all places } \omega \neq \nu\}.$$

Clearly $R_S^{(\nu)}$ is a subring of R_S for each $\nu \in S$. For example, if $k = \mathbf{Q}$ and $S = \{2, 3\}$, then $R_S^{(2)} = \mathbf{Z}[\frac{1}{2}], R_S^{(3)} = \mathbf{Z}[\frac{1}{3}]$ are both subrings of $R_S = \mathbf{Z}[\frac{1}{6}]$. If $k = \mathbf{F}_p(T)$ and $S = \{T\}$, then $R_S^{(T)} = \mathbf{F}_p[T^{\pm 1}] = R_S$.

Lemma 2.1 *For each $\nu \in S$ we have*

$$k_\nu = R_S^{(\nu)} + r_\nu \text{ and } R_S^{(\nu)} \bigcap r_\nu = \begin{cases} \mathbf{Z} & \text{if } k = \mathbf{Q}, \\ \mathbf{F}_p & \text{if } k = \mathbf{F}_p(T). \end{cases}$$

Proof. The first assertion follows easily by examining the ν–adic expansion of an element of k_ν and the second is obvious.

□

Lemma 2.2 *In the case $k = \mathbf{Q}$ we have*

$$\mathbf{Q}_{\mathbf{A}}(S) = \varphi(R_S) + A_\infty \text{ and } \varphi(R_S) \bigcap A_\infty = \varphi(\mathbf{Z})$$

where $A_\infty = \mathbf{R} \times \prod_{p \in S} \mathbf{Z}_p$ is an open subring of $\mathbf{Q}_{\mathbf{A}}(S)$.

Proof. The second assertion is actually obvious. Let $x = (x_p)$ be any element in $\mathbf{Q}_{\mathbf{A}}(S)$ and define S^* to be the set of primes $p \in S$ such that $x_p \notin \mathbf{Z}_p$; so S^* is finite. By Lemma 2.1, for each $p \in S^*$ we may write

$$x_p = \alpha_p + x'_p \text{ with } \alpha_p \in R_S^{(p)}, x'_p \in \mathbf{Z}_p.$$

For $p \in S \setminus \{S^*\}$ put $\alpha_p = 0$ and $x'_p = x_p$. Set $\alpha = \sum_{p \in S \cup \infty} \alpha_p$, so that $\alpha \in R_S$, and $y = x - \varphi(\alpha)$. If $y = (y_p)$ then we have for every $p \in S$,

$$y_p = x_p - \alpha_p - \sum_{p' \in S \setminus \{p\}} \alpha_{p'} = x'_p - \sum_{p' \in S \setminus \{p\}} \alpha_{p'}.$$

By the definition of $R_S^{(p)}$, all the terms on the right–hand side are in $\mathbf{Z}_p$. So y is in A_∞, hence x is in $\varphi(R_S) + A_\infty$. This proves the first assertion of the lemma.

□

Since A_∞ is open in $\mathbf{Q}_{\mathbf{A}}(S)$ it suffices to show that $\varphi(R_S) \bigcap A_\infty$, that is $\varphi(\mathbf{Z})$, is discrete in A_∞; this is clear since its projection onto the factor $\mathbf{R}$ of the product A_∞ is $\mathbf{Z}$, which is discrete in $\mathbf{R}$. Hence $\varphi(R_S)$ is discrete in $\mathbf{Q}_{\mathbf{A}}(S)$. Now let I be the closed interval $[-\frac{1}{2}, \frac{1}{2}]$ in $\mathbf{R}$, and put $C = I \times \prod_{p \in S} \mathbf{Z}_p$. Obviously $A_\infty = \varphi(\mathbf{Z}) + C$, so $\mathbf{Q}_{\mathbf{A}}(S) = \varphi(R_S) + C$. Hence $\mathbf{Q}_{\mathbf{A}}(S)/\varphi(R_S)$ is compact since C is. This completes the proof of Theorem 2.2 for $k = \mathbf{Q}$.

□

Lemma 2.3 *In the case $k = \mathbf{F}_p(T)$ we have*

$$k_{\mathbf{A}}(S) = \varphi(R_S) + A_0 \textit{ and } \varphi(R_S) \bigcap A_0 = \varphi(\mathbf{F}_p)$$

where $A_0 = \prod_{\nu \in S \cup \infty} r_\nu$ is a compact open subring of $k_{\mathbf{A}}(S)$.

Proof. The second assertion is again obvious. In a fashion similar to the arithmetic proof, take any $x = (x_\nu)$ in $k_{\mathbf{A}}(S)$. By Lemma 2.1, for each $\nu \in S$ satisfying $|x_\nu|_\nu > 1$ we may write

$$x_\nu = \alpha_\nu + x'_\nu \text{ with } \alpha_\nu \in R_S^{(\nu)}, x'_\nu \in r_\nu.$$

For the remaining valuations in S put $\alpha_\nu = 0$ and $x'_\nu = x_\nu$. Set $\alpha = \sum_{\nu \in S \cup \infty} \alpha_\nu$, so that $\alpha \in R_S$, and $y = x - \varphi(\alpha)$. Then, just as in Lemma 2.2, y is in A_0 implies that x is in $\varphi(R_S) + A_0$. This proves the first assertion of the lemma.

□

Now since A_0 is open in $k_{\mathbf{A}}(S)$ and $\mathbf{F}_p$ is finite, it is clear that $\varphi(R_S)\bigcap A_0 = \varphi(\mathbf{F}_p)$ is discrete in A_0 and so $\varphi(R_S)$ is discrete in $k_{\mathbf{A}}(S)$. Finally, $k_{\mathbf{A}}(S)/\varphi(R_S)$ is compact since A_0 is compact. This completes the proof of Theorem 2.2 for $k = \mathbf{F}_p(T)$.

□

From [59] Chapter I, Theorem 5 and Theorem 8, we have that the collection of completions of $\mathbf{A}$–fields coincides with the collection of all non–discrete locally compact fields.

Proposition 2.1 *Let K be a non–discrete locally compact field and let χ_0 be a fixed, non–trivial character. Then any non–trivial character χ of the additive group of K can be uniquely written as $t \mapsto \chi_0(tx)$ for all $t \in K$ and some fixed $x \in K^*$.*

In other words $K \cong \hat{K}$, both topologically and algebraically, via the mapping

$$t \mapsto \chi_t(x) := \chi(tx).$$

For example, $\mathbf{R}$ and $\mathbf{Q}_p$ are self–dual. In general, the construction of a non–trivial character of k may take some doing.

Proposition 2.2 *Let χ be any character of $k_{\mathbf{A}}(S)$. Then χ induces a character χ_ν on the quasifactor k_ν for each $\nu \in S \cup P_\infty$ via the projection mapping $x = (x_\nu) \mapsto x_\nu$ of $k_{\mathbf{A}}(S)$ onto k_ν. A character of an infinite product of compact groups must induce the trivial character 1 on almost all the factors. Since x_ν is in r_ν for almost every $\nu \in S$ then χ_ν is trivial on r_ν for almost all ν and for each $x = (x_\nu)$ in $k_{\mathbf{A}}(S)$,*

$$\chi(x) = \prod_{\nu \in S \cup P_\infty} \chi_\nu(x_\nu), \tag{9}$$

where almost all the factors are equal to 1.

Proof. See Theorem 23.21 in [16]. Suppose $\{H_i : i \in I\}$ is a family of compact groups. Using the notation in [16], let $\prod^*_{i\in I} H_i$ be the subgroup of the compact group $\prod_{i\in I} H_i$ consisting of all $x = (x_i) \in \prod_{i\in I} H_i$ such that $x_i = e_i$ for all but finitely many indices i. For any element (χ_i) in $\prod^*_{i\in I} \hat{H}_i$ define the function $\chi : \prod_{i\in I} H_i \to \mathbf{T}$ by

$$\chi(x) = \prod_{i\in I} \chi_i(x_i), \tag{10}$$

where all but a finite number of terms in the product are equal to 1.

The set of χ satisfying (10) is clearly a subgroup of the dual of $\prod_{i\in I} H_i$ that separates points of $\prod_{i\in I} H_i$. By Theorem 23.20 in [16] the set of such characters $\{\chi\}$ is dense in the dual group of $\prod_{i\in I} H_i$, which is itself discrete. Hence all characters on $\prod_{i\in I} H_i$ are of the form in (10).

□

Theorem 2.3

$$k_{\mathbf{A}}(S)/\varphi(R_S) \cong \hat{R}_S.$$

Proof. Once again we treat the case $k = \mathbf{Q}$ or $\mathbf{F}_p(T)$. Consider the former. We construct a non–trivial character χ on $\mathbf{Q}_{\mathbf{A}}(S)$ as follows. For each $p \in S$ let χ_p be trivial on $\mathbf{Z}_p$ and for $p = \infty$ define

$$\chi(x_\infty) = e^{-2\pi i x_\infty} \text{ for all } x_\infty \in \mathbf{R}.$$

By (9), any continuous character on $\mathbf{Q}_{\mathbf{A}}(S)$ must be trivial on $\mathbf{Z}_p$ for all but finitely many p in S since it must restrict to a continuous character on an infinite (if S is infinite) product of compact groups. We can calculate the character χ_p, induced on the quasifactor $\mathbf{Q}_p$, by considering again the ring $R_S^{(p)}$. We have,

$$1 = \chi(\varphi(x)) = \chi_\infty(x)\chi_p(x) \text{ for all } x \in R_S^{(p)},$$

since χ is trivial on $\varphi(R_S)$. So

$$\chi_p(x) = e^{2\pi i x} \text{ for all } x \in R_S^{(p)}$$

and by Lemma 2.1 this completely determines χ_p on $\mathbf{Q}_p$.

Now let χ' be an arbitrary character of $\mathbf{Q}_{\mathbf{A}}(S)$ and denote the induced character on the quasifactor $\mathbf{Q}_p$ of $\mathbf{Q}_{\mathbf{A}}(S)$ by χ'_p for each $p \in S \cup \infty$. By Proposition 2.1, with $\mathbf{Q}_p$ non–discrete and χ_p non–trivial,

$$\chi'_p(x) = \chi_p(a_p x)$$

for some unique a_p in $\mathbf{Q}_p$. By (9) χ'_p must be trivial on $\mathbf{Z}_p$ for all but finitely many $p \in S$ if χ is to be continuous. Thus $\chi_p(a_p) = 1$ for all but finitely many $p \in S$ and so $a_p \in \mathbf{Z}_p$ for all but finitely many $p \in S$. Therefore $a = (a_p)$ is in $\mathbf{Q}_{\mathbf{A}}(S)$ and by (9) χ' is the character χ_a of $\mathbf{Q}_{\mathbf{A}}(S)$ given by $\chi_a(x) = \chi(ax)$ for all $x \in \mathbf{Q}_{\mathbf{A}}(S)$.

We have shown that the mapping $a \mapsto \chi_a$ of $\mathbf{Q}_{\mathbf{A}}(S) \to \widehat{\mathbf{Q}_{\mathbf{A}}(S)}$ is surjective. Since this mapping is clearly injective and continuous then $\mathbf{Q}_{\mathbf{A}}(S) \cong \widehat{\mathbf{Q}_{\mathbf{A}}(S)}$.

Now

$$\widehat{\varphi(R_S)} \cong \widehat{\mathbf{Q}_{\mathbf{A}}(S)}/\varphi(R_S)^{\perp} \cong \mathbf{Q}_{\mathbf{A}}(S)/\varphi(R_S)^{\perp}.$$

So in order to prove the Lemma for the case $k = \mathbf{Q}$ we must show that the mapping $a \mapsto \chi_a$ induces an isomorphism of $\varphi(R_S)$ onto $\varphi(R_S)^{\perp}$. The group $\varphi(R_S)^{\perp}$ consists of all characters of $\mathbf{Q}_{\mathbf{A}}(S)$ which are trivial on $\varphi(R_S)$, and χ has this property by construction, hence so does χ_a for all $a \in \varphi(R_S)$. Thus $a \mapsto \chi_a$ maps $\varphi(R_S)$ into $\varphi(R_S)^{\perp}$.

To obtain the converse, let $\chi_b \in \varphi(R_S)^{\perp}$ for some $b \in \mathbf{Q}_{\mathbf{A}}(S)$ and put $C = I \times \prod_{p \in S} \mathbf{Z}_p$ where $I = [-\frac{1}{2}, \frac{1}{2}]$. In the proof of Theorem 2.2 we showed that $\mathbf{Q}_{\mathbf{A}}(S) = \varphi(R_S) + C$, so we may write

$$b = \varphi(\alpha) + c \text{ with } \alpha \in R_S, c \in C.$$

Note that $\chi_c \in \varphi(R_S)^{\perp}$. Now write $c = (c_p)$, so $c_p \in \mathbf{Z}_p$ for all $p \in S$, then

$$1 = \chi_c(\varphi(1)) = \chi(c) = \chi_\infty(c_\infty) = e^{-2\pi i c_\infty}$$

where $c_\infty = 0$ since $c_\infty \in I$. Thus χ_c is trivial on A_∞ (as defined in Lemma 2.2). But as it is trivial on $\varphi(R_S)$, Lemma 2.2 shows that it is trivial on $\mathbf{Q}_{\mathbf{A}}(S)$, so $c = 0$ and hence $b \in \varphi(R_S)$. Therefore $a \mapsto \chi_a$ maps $\varphi(R_S)$ onto $\varphi(R_S)^{\perp}$ and induces a bijective morphism of $\widehat{\varphi(R_S)}$ onto $\mathbf{Q}_{\mathbf{A}}(S)/\varphi(R_S)$. This completes the proof in the arithmetic case.

Now let $k = \mathbf{F}_p(T)$ with p a fixed rational prime. Recall that ∞ corresponds to the valuation $|.|_{T^{-1}}$ on k, and is actually a finite place as are all the places on k. We identify an element $x \in k_\infty$ with its ν–adic expansion,

$$x = \sum_{i=n}^{\infty} a_i T^{-i}$$

where $n \in \mathbf{Z}$ and $a_i \in \mathbf{F}_p$ for all $i \geq n$. By analogy with $\mathbf{Q}$, we proceed to construct a non–trivial character χ on $k_{\mathbf{A}}(S)$ as follows: for each $\nu \in S$ let χ_ν be trivial on r_ν and for $\nu = \infty$ define

$$\chi_\infty(x_\infty) = e^{-2\pi i \frac{a_1}{p}} \text{ for all } x_\infty \in k_\infty.$$

As before χ must be trivial on r_ν for all but finitely many $\nu \in S$.

For each $\nu \in S$, let $B^{(\nu)}$ denote the subring of $R_S^{(\nu)}$ defined as

$$B^{(\nu)} = R_S^{(\nu)} \bigcap \left\{ \alpha \in R_S^{(\nu)} : |\alpha|_\infty < 1 \right\}.$$

So, as in Lemma 2.1, $k_\nu = B^{(\nu)} + r_\nu$ for all $\nu \in S$, and if we choose $\alpha \in B^{(\nu)} \setminus \{0\}$ then

$$\alpha = \nu(T)^{-n} g(T),$$

where $n \in \mathbf{N}$ and $g \in \mathbf{F}_p[T]$ with $deg(g) < ndeg(\nu)$. Let a_1 denote the leading coefficient of g. As $\nu(T)$ is monic, it can be written as $T^{deg(\nu)}u$ for some $u \in \mathbf{F}_p[T^{-1}]$ with constant term 1. Then

$$\alpha = \nu^{-n} g = u^{-n} T^{-ndeg(\nu)} g \equiv a_1 T^{-1} \left(\mathrm{mod} T^{-2}\right)$$

in the ring r_∞ and, since $\alpha \neq 0$,

$$\begin{aligned} \alpha T^{ndeg(\nu)-1-deg(g)} &\equiv a_1 T^{ndeg(\nu)-2-deg(g)} \left(\mathrm{mod} T^{-2}\right) \\ &\not\equiv 0 \left(\mathrm{mod} T^{-2}\right) \end{aligned}$$

because $ndeg(\nu) - deg(g) > 0$. We have now

$$1 = \chi(\varphi(\alpha)) = \chi_\infty(\alpha)\chi_\nu(\alpha)$$

since χ is trivial on $\varphi(R_S)$, and so

$$\chi_\nu(\alpha) = e^{2\pi i \frac{a_1}{p}} \neq 1 \text{ since } a_1 \neq 0.$$

The character χ_ν is completely determined by its values on $B^{(\nu)}$ since it is trivial on r_ν.

Continuing as in the arithmetic proof, let χ' be any character of $k_{\mathbf{A}}(S)$. For each $\nu \in S$, the induced characters χ'_ν on the quasifactors k_ν can be written as $\chi'_\nu(x) = \chi_\nu(a_\nu x)$ with $a_\nu \in k_\nu$. Since χ'_ν must be trivial for all but finitely many $\nu \in S$, we deduce that $a = (a_\nu) \in k_{\mathbf{A}}(S)$, so that χ' is the character given by

$$\chi_a(x) = \chi(ax) \text{ for all } x \in k_{\mathbf{A}}(S).$$

As before, by considering the continuous bijective morphism $a \mapsto \chi_a$, we conclude that $\widehat{k_{\mathbf{A}}(S)} \cong k_{\mathbf{A}}(S)$ and that this mapping takes $\varphi(R_S)$ into $\varphi(R_S)^\perp$.

Let $\chi_b \in \varphi(R_S)^\perp$ for some $b \in k_{\mathbf{A}}(S)$, then by Lemma 2.3 we may write $b = \varphi(\alpha) + c$ with $\alpha \in R_S, c \in A_0$; so χ_c is trivial on $\varphi(R_S)$. Put $c = (c_\nu)$ so that $c_\nu \in r_\nu$ for all $\nu \in S \cup \infty$. Clearly $c_\infty \equiv \gamma \,(\mathrm{mod} T^{-1})$ for some $\gamma \in \mathbf{F}_p$. Now substitute α by $\alpha + \gamma$ and c by $c - \varphi(\gamma)$, so that $c_\infty \equiv 0 \,(\mathrm{mod} T^{-1})$. Then we have

$$1 = \chi_c(\varphi(1)) = \chi(c) = \chi_\infty(c_\infty),$$

whence c_∞ is in $T^{-2} r_\infty$ because in the ν–adic expansion of c_∞ the coefficients a_0 and a_1 must be zero. It follows that $\chi_\infty(c_\infty t) = 1$ for all $t \in r_\infty$, so χ_c is trivial on A_0 and hence on $k_{\mathbf{A}}(S)$ by Lemma 2.3. So $c = 0$ and $b \in \varphi(R_S)$.

In conclusion, $a \mapsto \chi_a$ maps $\varphi(R_S)$ onto $\varphi(R_S)^\perp$ and $\widehat{\varphi(R_S)} \cong k_{\mathbf{A}}(S)/\varphi(R_S)$. This completes the proof for the geometric case.

□

2.3 Extension of Theorems 2.2 and 2.3 to A–Fields

These results have a natural generalisation to the case of k being an $\mathbf{A}$–field. Since S is an arbitrary set of finite places of k (as opposed to the classical case where S comprises all the finite places), it is not sufficient to quote Weil at our leisure. He uses the language of tensor–products and algebras to establish our Theorems for the case in which S comprises the set of all finite places. Instead we return to one of the sources of Weil's adelic machinery, namely Tate's elegant thesis [53].

In [53], Tate introduces the notion of an *abstract restricted direct product*, under the hypothesis that $\mathbf{P}$ $(= S \cup P_\infty)$ is an arbitrary set of indices (places). Let $G_{\mathcal{P}}$

$(= k_\nu)$ be a locally compact abelian group for $\mathcal{P} \in \mathbf{P}$, and for all but finitely many $\mathcal{P}$, let $H_\mathcal{P}$ $(= r_\nu)$ be an open compact subgroup of $G_\mathcal{P}$. The restricted direct product is defined as

$$G(\mathbf{P}) = \left\{ g = (g_\mathcal{P}) \in \prod_{\mathcal{P}\in\mathbf{P}} G_\mathcal{P} : g_\mathcal{P} \in H_\mathcal{P} \text{ for almost every } \mathcal{P} \right\},$$

a locally compact abelian topological group. We topologise $G(\mathbf{P})$ by choosing a fundamental system of neighbourhoods of 1 in $G(\mathbf{P})$ of the form $N = \prod_{\mathcal{P}\in\mathbf{P}} N_\mathcal{P}$, where each $N_\mathcal{P}$ is a neighbourhood of 1 in $G_\mathcal{P}$ and $N_\mathcal{P} = H_\mathcal{P}$ for all but finitely many $\mathcal{P}$.

The key results proved in Lemma 3.2.2 and Theorem 3.2.1 of [53] are:

1. $\varphi(R_S)$ is discrete in $k_\mathbf{A}(S)$ and $k_\mathbf{A}(S)/\varphi(R_S)$ is compact,

2. $R_S^\perp \cong R_S$, $\widehat{k_\mathbf{A}(S)} \cong k_\mathbf{A}(S)$ and so $k_\mathbf{A}(S)/\varphi(R_S) \cong \hat{R}_S$

where S is an arbitrary set of finite places of an $\mathbf{A}$–field k. This completes the generalisation of Theorems 2.2 and 2.3 to $\mathbf{A}$–fields.

2.4 The Entropy Formula

Identifying R_S with $\varphi(R_S) \subset k_\mathbf{A}(S)$, the action of ξ on R_S extends to $k_\mathbf{A}(S)$ by defining $(\xi x)_\nu = \xi(x_\nu)$ for $x \in k_\mathbf{A}(S)$ and $\nu \in S \cup P_\infty$. Equivalently, the extension can be defined locally via the embedding $R_S \subset \prod_{\nu\in S\cup P_\infty}(R_S \otimes_k k_\nu) \cong k_\mathbf{A}(S)$. Thus the endomorphism θ of $\hat{R}_S$ may be lifted to an automorphism $\tilde{\theta}$ of $k_\mathbf{A}(S)$,

$$\begin{array}{ccc} k_\mathbf{A}(S) & \xrightarrow{\tilde{\theta}} & k_\mathbf{A}(S) \\ \downarrow & & \downarrow \\ \hat{R}_S & \xrightarrow{\theta} & \hat{R}_S \end{array} \qquad (11)$$

where $\tilde{\theta}$ is the aforementioned extension. This lifting is analogous to the lifting of maps of the circle $\mathbf{T}$ to the universal cover $\mathbf{R}/\mathbf{Z}$. Following the work of Bowen we give a method for computing the entropy of a uniformly continuous map acting on a locally compact metric space, by using Haar measure to count orbits.

Definition 2.2 Suppose that (X, d) is a locally compact metric space and $T : X \to X$ is uniformly continuous. Set

$$D_n(x, \epsilon, T) = \bigcap_{j=0}^{n-1} T^{-j}(B_\epsilon(T^j(x))),$$

where $B_\epsilon(y) = \{z \in X : d(y, z) < \epsilon\}$. A Borel measure μ on X is called *T–homogeneous* if

(i) $\mu(K) < \infty$ for all $K \subset X$ compact,

(ii) $\mu(K) > 0$ for some compact K,

(iii) for each $\epsilon > 0$ there exist positive constants δ, c such that

$$\mu(D_n(y, \delta, T)) \le c\mu(D_n(x, \epsilon, T)) \text{ for all } n \ge 0 \text{ and } x, y \in X.$$

For such a μ, put

$$k(\mu, T) = \lim_{\epsilon \to 0} \limsup_{n \to \infty} -\frac{1}{n} \log \mu(D_n(x, \epsilon, T)).$$

By (iii) this is independent of x. Proposition 7 of [5] states that $h(T) = k(\mu, T)$ for any T–homogeneous measure μ. If T is a continuous endomorphism of a locally compact group, then Haar measure μ is T–homogeneous and $h(T) = k(\mu, T)$.

Lemma 2.4

$$h(\theta; \hat{R}_S) = h(\tilde{\theta}; k_{\mathbf{A}}(S)).$$

Proof. Since $k_{\mathbf{A}}(S)$ is a locally compact metric space and $\tilde{\theta}$ is uniformly continuous, Bowen's definition of topological entropy $h(\tilde{\theta}; k_{\mathbf{A}}(S))$ applies. From the second assertion of Section 2.3, $h(\theta; \hat{R}_S) = h\left(\tilde{\theta}; k_{\mathbf{A}}(S)/\varphi(R_S)\right)$. Theorem 20 in [5] shows that for ϵ small enough we have,

$$\hat{\varphi}\left(D_n(y, \epsilon, \tilde{\theta})\right) = D_n(y + \varphi(R_S), \epsilon, \tilde{\theta}),$$

for all $y \in k_{\mathbf{A}}(S)$. Thus the projection map $\hat{\varphi}$ is a local isometry of $k_{\mathbf{A}}(S)$ onto $k_{\mathbf{A}}(S)/\varphi(R_S)$. Hence the result.

□

Lemma 2.5

$$h(\tilde{\theta}; k_{\mathbf{A}}(S)) = h(\tilde{\theta}; k_{\mathbf{A}}(S_1)),$$

where $S_1 \subseteq S$ *is a finite set such that* $|\xi|_\nu > 1$ *if and only if* $\nu \in S_1$.

Proof. We write

$$k_{\mathbf{A}}(S) = k_{\mathbf{A}}(S_1) \times \prod_{\nu \notin S_1} r_\nu.$$

Since the second factor is compact, by Theorem 7.10 in [56] we have

$$h(\tilde{\theta}; k_{\mathbf{A}}(S)) = h(\tilde{\theta}; k_{\mathbf{A}}(S_1)) + h\left(\tilde{\theta}; \prod_{\nu \notin S_1} r_\nu\right).$$

The product $\prod_{\nu \notin S_1} r_\nu$ has a basis of open sets U_m given by,

$$U_m = \prod_{\nu \in F} \nu^m r_\nu \times \prod_{\nu \in S_1^c \setminus F} r_\nu,$$

where $m > 0$ and F is a finite subset of S_1^c. Since $\xi \in r_\nu$ for each $\nu \in S_1^c$, Proposition 7 in [5] with the $\tilde{\theta}$–homogeneous Haar measure implies that $h(\tilde{\theta}; \prod_{\nu \notin S_1} r_\nu) = 0$.

□

Lemma 2.6

$$h(\tilde{\theta}; k_{\mathbf{A}}(S_1)) = \sum_{\nu \in S_1 \cup P_\infty} h(\tilde{\theta}; k_\nu).$$

Proof. Unfortunately, in the absence of compactness, additivity of entropy is not a forgone conclusion (see Theorem 7.10 in [56] and Lind/Ward [28] where this occurs in a similar context). Let μ_ν denote Haar measure on k_ν for each $\nu \in S \cup P_\infty$, then μ_ν is $\tilde{\theta}$–homogeneous.

In the arithmetic case, if $\nu|\infty$ (that is, $|.|_\nu$ is the usual absolute value or it's square) then $k_\nu = \mathbf{R}$ or $\mathbf{C}$, and Theorem 8.14 in [56] shows that the Bowen entropy is $h(\tilde{\theta}; k_\nu) = \log^+ |\xi|_\nu$. For example, $h(\times 2; \mathbf{C}) = \log^+ |2|^2 = \log 4$. It remains to compute the Bowen entropy contributions from the ultrametric ν–adic absolute values.

Suppose ν corresponds to an ultrametric ν–adic absolute value on k. From Chapter I Section 2 in [59], $mod_{k_\nu}(\xi)$ is the number well–defined by $\mu_\nu(\xi E) = mod_{k_\nu}(\xi)\mu_\nu(E)$ for any measurable $E \subset k_\nu$ with $0 < \mu_\nu(E) < \infty$. This number is called the *module* of ξ. By Corollary 3 in Chapter I Section 2 of [59] and Theorem 11 in Chapter 3 Section 2 of [21], $mod_{k_\nu}(\xi) = |\xi|_\nu$.

If C is a compact ball centered at 0, then

$$\bigcap_{j=0}^{n-1} \tilde{\theta}^{-j}(C) = \bigcap_{j=0}^{n-1} \xi^{-j} C = \begin{cases} \xi^{-(n-1)} C & \text{if } |\xi|_\nu > 1, \\ C & \text{if } |\xi|_\nu \le 1. \end{cases}$$

It follows that

$$\begin{aligned} k(\mu_\nu, \tilde{\theta}) &= \lim_{n\to\infty} -\frac{1}{n} \log \mu_\nu \left(\bigcap_{j=0}^{n-1} \tilde{\theta}^{-j}(C) \right) \\ &= \log^+ mod_{k_\nu}(\xi) \\ &= \log^+ |\xi|_\nu \\ &= h(\tilde{\theta}; k_\nu) \end{aligned}$$

by [5] Proposition 7. Since the lim sup's are actually limits, additivity of entropy follows.

□

Proof of Theorem 2.1

From Lemmas 2.4–2.6, we conclude that

$$h(\theta; \hat{R}_S) = \sum_{\nu \in S_1 \cup P_\infty} h(\tilde{\theta}; k_\nu) = \sum_\nu \log^+ |\xi|_\nu,$$

since an argument as in the proof of Lemma 2.5 shows that $h(\tilde{\theta}; k_\nu) = 0$ for $\nu \notin S_1$.

□

Thus the entropy of the geometric endomorphism θ of $\hat{R}_S$ admits a ν–adic decomposition exactly analogous to the p–adic decomposition of its arithmetic counterpart, shown in (7). Theorem 2.1 is a special case of [28] in the connected case. In the geometric case, it is an easy extension. Following Weil, we strive to treat both zero and positive characteristics on an even footing.

Chapter 3

Ergodicity and Expansiveness

Definition 3.1 Suppose $(X, \mathcal{B}, m)$ is a probability space. A map $T : X \to X$ is called a *measure–preserving transformation* if for every $B \in \mathcal{B}$ we have $T^{-1}(B) \in \mathcal{B}$ and $m(B) = m(T^{-1}(B))$.

Our main interest in such systems will be when $T : X \to X$ is a (continuous) surjective endomorphism of a compact abelian group preserving Haar measure μ. Halmos [15] first observed that such a transformation is measure preserving as follows: define a new measure m on X by setting $m(B) = \mu(T^{-1}(B))$ for all $B \in \mathcal{B}$. Then

$$m(T(x) + B) = \mu(T^{-1}(T(x) + B)) = \mu(x + T^{-1}(B)) = \mu(T^{-1}(B)) = m(B)$$

by the translation invariance property of μ. But μ is the unique probability measure with this property so $m = \mu$ since T is surjective.

Definition 3.2 Let $(X, \mathcal{B}, m)$ be a measure space. A measure preserving transformation $T : X \to X$ is said to be *ergodic* if whenever $m(T^{-1}(B) \triangle B) = 0$ for $B \in \mathcal{B}$ then either $m(B) = 0$ or $m(B) = 1$.

Ergodic maps are in a sense indecomposable ones. Ergodicity is equivalent to the following property:

$$\text{whenever } f \in L^2(G) \text{ and } (f \circ T)(x) = f(x) \text{ a.e. then } f \text{ is constant a.e.} \tag{12}$$

(See Theorem 1.6 in [56] for a proof of this.) The ergodicity condition for compact abelian groups is:

Theorem 3.1 *If X is a compact abelian group with normalised Haar measure and $T : X \to X$ is a surjective continuous endomorphism then T is ergodic if and only if the trivial character $\gamma \equiv 1$ is the only $\gamma \in \hat{X}$ satisfying $\gamma \circ T^n = \gamma$ for some $n > 0$.*

Proof. First suppose that whenever $\gamma \circ T^n = \gamma$ for some $n > 0$ we have $\gamma \equiv 1$. Let $f \circ T = f$ with $f \in L^2(X)$. Write f in its Fourier series expansion

$$f = \sum a_m \gamma_m$$

where

$$\sum |a_m|^2 < \infty. \tag{13}$$

The T–invariance of f implies that $\sum a_m \gamma_m(Tx) = \sum a_m \gamma_m(x)$, so that the coefficients of $\gamma_m, \gamma_m \circ T, \gamma_m \circ T^2, \ldots$ are all a_m. By (13) we must have $\gamma_m \circ T^n = \gamma_m \circ T^l$ for some $n > l \geq 0$, that is, $\gamma_m \circ T^{n-l} = \gamma_m$. By our assumption $\gamma_m \equiv 1$ and so f is constant a.e. Therefore T is ergodic by (12).

Conversely, let T be ergodic and $\gamma \circ T^n = \gamma$ for some $n > 0$ (n minimal). It follows that the function

$$f = \gamma + \gamma \circ T + \cdots + \gamma \circ T^{n-1}$$

is T–invariant and non–constant (since it is a sum of distinct elements of the orthornormal basis). By (12) T is not ergodic, a contradiction.

□

Corollary 3.1 *If $T : \mathbf{T}^n \to \mathbf{T}^n$ is a surjective continuous endomorphism of the n–torus then T is ergodic if and only if the dual map $\hat{T}$, which is an element in $GL(n, \mathbf{Z})$, has no roots of unity as eigenvalues.*

Proof. Suppose T is not ergodic, then by the characterisation of ergodicity above there exists a non–zero $q \in \mathbf{Z}^n$ and $m > 0$ such that $\hat{T}^m q = q$. So $\hat{T}^m$ has 1 as an eigenvalue and hence an m-th root of unity as an eigenvalue.

Conversely, if $\hat{T}$ has an m-th root of unity as an eigenvalue then $\hat{T}^m$ has 1 as an eigenvalue. So $(\hat{T}^m - I)$ is singular whence there exists a non–zero $y \in \mathbf{R}^n$ with $(\hat{T}^m - I)y = 0$. But the matrix $(\hat{T}^m - I)$ has integral entries so we can find such a y in $\mathbf{Z}^n$. Hence $\hat{T}^m y = y$ and T is not ergodic by the Theorem. □

The criteria for ergodicity in S–integer dynamical systems $(\hat{R}_S, \theta)$ is the following.

Theorem 3.2 *In the arithmetic case θ is ergodic if and only if the set of conjugates of ξ does not contain a root of unity. In the geometric case θ is ergodic if and only if $\xi \notin \mathbf{F}_p^*$.*

Proof. Recall that the dynamical system $(\hat{R}_S, \theta_\xi)$ has a matrix representation $(\hat{R}_{S^*}^d, \hat{\xi^*})$ where $S^* = \{\nu : \omega \mid \nu \text{ for each } \omega \in S\}$ and $\xi^* \in M_d(R_{S^*})$. Suppose that θ is not ergodic, then by Theorem 3.1 there exists a non–zero vector $q \in R_{S^*}^d$ and $m > 0$ such that $(\xi^*)^m q = q$. So $(\xi^*)^m$ has 1 as an eigenvalue. Therefore if k is a number field then ξ^* has an m-th root of unity as an eigenvalue. If k is a finite algebraic extension of $\mathbf{F}_p(T)$ then some eigenvalue of ξ^* must be constant, since $\mathbf{F}_p^*$ is a cyclic group, otherwise the degree of an eigenvalue as an algebraic function in T increases with m. Hence, in the arithmetic case some conjugate of ξ is a root of unity, and in the geometric case $\xi \in \mathbf{F}_p^*$.

Conversely, assume that either some conjugate of ξ is an m-th root of unity or $\xi \in \mathbf{F}_p^*$, so that ξ^* has either an m-th root of unity or a constant in $\mathbf{F}_p^*$ as an eigenvalue. Then either $(\xi^*)^m - I$ or $(\xi^*)^{p-1} - I$ is singular, respectively. Since the entries of these matrices lie in R_{S^*}, there exists a non–zero $y \in R_{S^*}^d$ such that either $(\xi^*)^m y = y$ or $(\xi^*)^{p-1} y = y$. By Theorem 3.1 $\hat{\xi^*}$ is not ergodic, hence θ is not ergodic.

□

Definition 3.3 A continuous map T of a metric space (X, d) is *forwardly expansive* if there exists an *expansive constant* $\delta > 0$ such that, for $x \neq y$ there exists $n \in \mathbf{N}$ with $d(T^n(x), T^n(y)) > \delta$.

Such maps allow the definition of topological entropy to be considerably refined as follows: for every $0 < \epsilon < \delta$ we have

$$h(T) = \sup_K \lim_{n \to \infty} \frac{1}{n} \log r_n(\epsilon, K)$$

rather than taking the double limit as in (4). This is proved in Proposition 7.3 of [32]. Hence $h(T)$ is always finite.

Definition 3.4 A homeomorphism T of a metric space (X, d) is expansive if there exists an *expansive constant* $\delta > 0$ such that, for $x \neq y$ there exists $n \in \mathbf{Z}$ with $d(T^n(x), T^n(y)) > \delta$.

It has been shown in [18] that if a homeomorphism $T : X \to X$ is forwardly expansive, then X is finite.

Lemma 3.1 *A continuous endomorphism T of a compact metrisable group X is expansive if there is a neighbourhood U of the identity 0_X of X such that*

$$\bigcap_{n \in \mathbf{N}} T^n U = \{0_X\}.$$

Proof. This is obvious from the definition of expansiveness because X is metrisable.

□

Expansiveness is a natural condition in topological dynamics. The algebraic analogue that eliminates certain complex behaviour is the following.

Definition 3.5 [Section 3 in [20]] Let X be a compact group and let $\Gamma \subset Aut(X)$ be a countable group. The pair (X, Γ) satisfies the *descending chain condition* if there exists, for every sequence $X \supset V_1 \supset V_2 \supset \cdots V_n \cdots$ of closed Γ–invariant subgroups, an integer $N \geq 1$ with $V_n = V_N$ for all $n \geq N$.

Theorem 3.3 *Let X be a compact group and $\Gamma \subset Aut(X)$ be a finitely generated, abelian group, and assume that (X, Γ) is expansive. Then (X, Γ) satisfies the descending chain condition. If X is zero–dimensional and (X, Γ) satisfies the descending chain condition then (X, Γ) is expansive.*

Proof. See Theorem 5.2 in [20].

□

It is well–known that if T is a surjective continuous endomorphism of the n–dimensional torus then T is expansive if and only if $\hat{T}$ has no eigenvalues of modulus 1 (this is Theorem 21 in [24]).

If $\alpha_{\mathcal{R}_d/<f>}$ is a $\mathbf{Z}^d$–action on a compact abelian group $X_{\mathcal{R}_d/<f>}$, then by [44], $\alpha_{\mathcal{R}_d/<f>}$ is expansive if and only if f has no zeros on the multiplicative d–torus. The criteria for expansiveness in S–integer dynamical systems $(\hat{R}_S, \theta)$ is a straightforward application of the following result by Eisenberg [9].

Lemma 3.2 *Let K be a complete non–discrete field with a valuation $|.|$, and let $\bar{K}$ denote the algebraic closure of K extending uniquely the absolute value on K. Let E be a finite dimensional vector space over K, and let u be an automorphism of E. Then u is expansive if and only if $|\lambda| \neq 1$ for each eigenvalue λ of u in $\bar{K}$.*

Theorem 3.4 *In the arithmetic case, θ is expansive if and only if the orbit of ξ under the action of the Galois group $\mathrm{Gal}[\bar{\mathbf{Q}} : \mathbf{Q}]$ on $\bar{\mathbf{Q}}^*$ does not intersect $\mathbf{T}$ and $S \subseteq \{\nu < \infty : |\xi|_\nu \neq 1\}$. In the geometric case, θ is expansive if and only if $S \cup P_\infty \subseteq \{\nu \leq \infty : |\xi|_\nu \neq 1\}$.*

Proof. Recall that by Bowen [5] there exists a local isometry between $k_{\mathbf{A}}(S)$ and $\hat{R}_S$, hence expansiveness on $\hat{R}_S$ is equivalent to expansiveness on $k_{\mathbf{A}}(S)$. Now set E equal to each of the quasifactors of $k_{\mathbf{A}}(S)$ in turn and fix u to be multiplication by ξ, then, bearing in mind that θ is not necessarily invertible, the result follows from Lemma 3.2. Note that the set S must be finite. Thus expansive actions are ones which behave hyperbolically in all directions k_ν such that $\nu \in S \cup P_\infty$.

□

This Theorem is a generalisation of Proposition 7.2 in [45] where Schmidt considers k to be a number field and $S = \{\nu < \infty : |\xi|_\nu \neq 1\}$.

Chapter 4

Periodic Points

Definition 4.1 Let $T : X \to X$ be a homeomorphism of a compact metric space. For $n \geq 1$, the set of points of period n is given by

$$Fix_n(T) = \{x \in X : T^n(x) = x\}.$$

Theorem 4.1 *If $T : X \to X$ is an expansive homeomorphism of a compact metric space then $|Fix_n(T)| < \infty$ for all $n \geq 1$ and*

$$\limsup_{n\to\infty} \frac{1}{n} \log |Fix_n(T)| \leq h(T).$$

Proof. Let δ be an expansive constant for T. Suppose $T^n(x) = x, T^n(y) = y$ and $x \neq y$. If $d(T^j(x), T^j(y)) \leq \delta$ for all $0 \leq j \leq n-1$, then by expansiveness we must have $d(T^j(x), T^j(y)) \leq \delta$ for all $j \in \mathbf{Z}$ and hence $x = y$. Therefore the set $Fix_n(T)$ is (n, δ)–separated (as defined in Section 7.2 of [56]) and so

$$|Fix_n(T)| \leq s_n(\delta, X) < \infty,$$

where $s_n(\delta, X)$ denotes the maximal cardinality of any (n, δ)–separated set for X with respect to T. Hence

$$\limsup_{n\to\infty} \frac{1}{n}|Fix_n(T)| \leq \limsup_{n\to\infty} \frac{1}{n} s_n(\delta, X) \leq h(T).$$

□

Example 4.1 If T is an expansive endomorphism of the d–torus then

$$|Fix_n(T)| = |det(\hat{T}^n - I)| = \prod_{i=1}^{d} |\lambda_i^n - 1|$$

where $\lambda_1, \ldots, \lambda_d$ are the eigenvalues of $\hat{T}$ and

$$h(T) = \lim_{n\to\infty} \frac{1}{n} \log |Fix_n(T)|.$$

(This growth rate also holds when T is merely ergodic, but the proof involves deep Diophantine estimates. See [26] for details.)

4.1 Periodic Points Counting Formula

We propose to extend the computation of $|Fix_n(T)|$ in the above example to the S–integer dynamical systems $(\hat{R}_S, \theta)$ defined in Chapter 2 and shall be investigating their periodic–point growth rates in both zero and positive characteristic. We begin by proving a general result concerning discrete subgroups of a locally compact abelian group.

Let Γ be a discrete subgroup of a locally compact abelian group X such that X/Γ is compact. A *fundamental domain* F of X modulo Γ is a full (measurable) set of coset representatives of Γ in X. Denote by μ the Haar measure on X normalised to give $\mu(F) = 1$. Let $\tilde{A} : X \to X$ be a continuous surjective mapping with $\tilde{A}(\Gamma) \subset \Gamma$, then this induces a continuous surjective endomorphism $A : X/\Gamma \to X/\Gamma$ by defining $A(x + \Gamma) = \tilde{A}(x) + \Gamma$ for all $x \in X$. Let $c : X/\Gamma \to X$ be a Borel section of the canonical epimorphism $\pi : X \to X/\Gamma$, so $\pi \circ c$ is the identity on X/Γ. Such a map c always exists, see for instance Appendix A in Zimmer [64]. The measure μ induces via this Borel section a probability measure μ^* on X/Γ by defining

$$\mu^*(\pi(E)) = \mu(E)$$

whenever $E \subset X$ is a measurable set and $\pi|_E = c|_E$ is a bijection. Also, the following diagram commutes:

$$\begin{array}{ccc} X & \stackrel{\tilde{A}}{\to} & X \\ \pi\downarrow & & \downarrow\pi \\ X/\Gamma & \stackrel{A}{\to} & X/\Gamma \end{array}$$

Recall the module function introduced in the proof of Lemma 2.6.

Theorem 4.2 *If* $\ker A$ *is discrete, then*

$$mod_X(\tilde{A}) = |\ker A|.$$

Proof. Since Γ is discrete in X, a fundamental domain F may be chosen so that there exists a neighbourhood $U(0_X)$ of the identity $0_X \in X$ with $U(0_X) \subset F$. The finiteness of $|\ker A|$ follows from the fact that it is discrete and X/Γ is compact. So for a sufficiently small neighbourhood $V(0_{X/\Gamma})$ of the identity $0_{X/\Gamma} \in X/\Gamma$,

$$A^{-1}V(0_{X/\Gamma}) = \bigcup_{i=1,\ldots,|\ker A|} V_i,$$

where each V_i is a neighbourhood of a point in the set $A^{-1}(0_{X/\Gamma})$ and their union is disjoint. Since A is measure–preserving

$$\mu\left(A^{-1}V(0_{X/\Gamma})\right) = \mu\left(V(0_{X/\Gamma})\right).$$

Once again using the discreteness of Γ in X we have that X is locally isomorphic to X/Γ. This means that, assuming the neighbourhoods $U(0_X)$ and $V(0_{X/\Gamma})$ are small enough, $\pi|_{U(0_X)}$ is a homeomorphism between $U(0_X)$ and $V(0_{X/\Gamma})$. Thus we have

$$\begin{aligned} \mu\left(\tilde{A}U(0_X)\right) &= \mu\left(AV(0_{X/\Gamma})\right) \\ &= |\ker A|\mu\left(V(0_{X/\Gamma})\right) \\ &= |\ker A|\mu\left(U(0_X)\right) \end{aligned}$$

which proves the Theorem. Furthermore, since $U(0_X) \subset F$,

$$\mu(\tilde{A}F) = |\ker A|.$$

□

Corollary 4.1 *If $(\hat{R}_S, \theta)$ is an ergodic S–integer dynamical system, then the number of points of period $n \geq 1$ is*

$$|Fix_n(\theta)| = \prod_{\nu \in S \cup P_\infty} |\xi^n - 1|_\nu.$$

Proof. A fundamental domain of $k_{\mathbf{A}}(S)$ modulo k is a set

$$F = \begin{cases} [0,1)^d \times \prod_{\nu \in S} r_\nu & \text{if } k \text{ is a number field with } d = [k : \mathbf{Q}]. \\ \prod_{\nu \in S \cup P_\infty} r_\nu & \text{otherwise.} \end{cases}$$

The set F is measurable. For each $\nu \in S \cup P_\infty$, let μ_ν denote a Haar measure on k_ν normalised to have $\mu_\nu(r_\nu) = 1$ for all but finitely many ν. Then the product measure $\mu = \prod_{\nu \in S \cup P_\infty} \mu_\nu$ is well defined and is a Haar measure on $k_{\mathbf{A}}(S)$. Recall the map $\tilde{\theta}$, the linear lift of θ, in (11). Set $A = \theta^n - I, X = k_{\mathbf{A}}(S)$ and $\Gamma = \varphi(R_S)$, then ergodicity implies that $\ker A$ is discrete in $\hat{R}_S$ and by the Theorem we have,

$$\begin{aligned} |Fix_n(\theta)| &= |\ker(\theta^n - 1)| \\ &= \mu\left((\tilde{\theta}^n - 1)F\right) \\ &= \prod_{\nu \in S \cup P_\infty} |\xi^n - 1|_\nu. \end{aligned}$$

□

(Theorem 4.2 for the case $\mathbf{Z}^d \subset \mathbf{R}^d$ amounts to a version of Pick's Theorem for parallelipipeds.)

4.2 Growth Rates

We shall be investigating the following growth rates in ergodic S–integer dynamical systems,

$$p^+(\theta) = \limsup_{n \to \infty} \frac{1}{n} \log |Fix_n(\theta)| \text{ and } p^-(\theta) = \liminf_{n \to \infty} \frac{1}{n} \log |Fix_n(\theta)|. \tag{14}$$

Observe the following easy inequality,

$$\frac{1}{n} \log \prod_{\nu \in S \cup P_\infty} |\xi^n - 1|_\nu \leq \sum_{\nu \in S \cup P_\infty} \log^+ |\xi|_\nu \leq h(\theta)$$

so that

$$p^{-}(\theta) \leq p^{+}(\theta) \leq h(\theta). \tag{15}$$

In general, for a continuous map T of a metric space (X, d), we need expansiveness to deduce that $p^{+}(T) \leq h(T)$. For these algebraic systems, we always have (15).

Lemma 4.1 (Baker's Theorem) *Let ξ be an algebraic number on the unit circle which is not a root of unity. Then there are effectively computable constants $A = A(\xi)$ and $B = B(\xi)$ such that*

$$|\xi^n - 1| > \frac{A}{n^B} \text{ for all } n \geq 1.$$

Proof. A discussion of bounds for linear forms in logarithms can be found in [4].

□

A weaker (earlier) result is sufficient to give convergence in the quasihyperbolic toral case (see [26]).

Lemma 4.2 (Gelfond's Lower Bound) *Let ξ be an algebraic number on the unit circle which is not a root of unity. Then given $\epsilon > 0$, there exists M such that $|\xi^n - 1| > e^{-\epsilon n}$ for all $n \geq M$.*

Proof. See [13].

□

Theorem 4.3 *Let $(\hat{R}_S, \theta)$ be an ergodic arithmetic S–integer dynamical system with S finite. Then the growth rate of the number of periodic points exists and is given by*

$$p^{+}(\theta) = p^{-}(\theta) = h(\theta). \tag{16}$$

Proof. Note that

$$\begin{aligned}
\lim_{n\to\infty} \frac{1}{n} \log |Fix_n(\theta)| &= \lim_{n\to\infty} \frac{1}{n} \sum_{\nu \in S \cup P_\infty} \log |\xi^n - 1|_\nu \\
&= \lim_{n\to\infty} \frac{1}{n} \sum_{\nu \in P_\infty} \log |\xi^n - 1|_\nu + \sum_{\nu \in S : \xi \notin r_\nu^*} \log^+ |\xi|_\nu + \lim_{n\to\infty} D_n
\end{aligned}$$

where $D_n = \frac{1}{n}\sum_{\nu\in S:\xi\in r_\nu^*}\log|\xi^n-1|_\nu$. We first handle the archimedean contribution. Suppose $|\xi|=1$ for $\epsilon>0$, then by Lemma 4.1 we have

$$\frac{1}{n}\log A - \frac{B}{n}\log n < \frac{1}{n}\log|\xi^n-1| < \frac{1}{n}\log 2$$

So $\frac{1}{n}\log|\xi^n-1|\to 0$ as $n\to\infty$. If $|\xi|<1$ then clearly $\frac{1}{n}\log|\xi^n-1|\to 0$ as $n\to\infty$. Finally, if $|\xi|>1$ then

$$\frac{1}{n}\log|\xi^n-1| = \frac{1}{n}\Big(\log|\xi|^n + \log|1-\xi^{-n}|\Big) \to \log|\xi| \text{ as } n\to\infty.$$

Therefore for any algebraic number ξ,

$$\frac{1}{n}\log|\xi^n-1| \to \log^+|\xi|$$

and hence,

$$\frac{1}{n}\sum_{\nu\in P_\infty}\log|\xi^n-1|_\nu \to \sum_{\nu\in P_\infty}\log^+|\xi|_\nu.$$

We now show that $D_n\to 0$ by deriving the bound

$$n^{-1} \ll |\xi^n-1|_\nu \le 1 \tag{17}$$

for any finite place ν and $\xi\in {r^*}_\nu$. The upper bound is obvious. Suppose that the place ν of k lies above the place p of $\mathbf{Q}$ for some rational prime p. Using the Euclidean algorithm we may write $n = n_1(p-1)+r_1$ where $0\le r_1<p-1$.

Now, if $|\xi^n-1|_\nu = 1$ then there is no ν–adic contribution in the quantity D_n, so we may suppose that $|\xi^n-1|_\nu<1$. Let $\mathbf{\Omega}_\nu$ denote the smallest field which contains $\mathbf{Q}$ and is both algebraically closed and complete with respect to $|.|_\nu$. The ν–adic logarithm $\log_\nu$ is defined as

$$\log_\nu(1+x) = \sum_{i=1}^{\infty}\frac{(-1)^{i+1}x^i}{i} \tag{18}$$

and converges for all $x\in\mathbf{\Omega}_\nu$ such that $|x|_\nu<1$. Setting $x=\xi^n-1$ we get

$$\log_\nu(\xi^n) = (\xi^n-1) - \frac{(\xi^n-1)^2}{2} + \frac{(\xi^n-1)^3}{3} - \dots \tag{19}$$

and so $|\log_\nu(\xi^n)|_\nu = |\xi^n - 1|_\nu$. Now

$$\begin{aligned} |\xi^n - 1|_\nu &= \left|\log_\nu\left(\xi^{n_1(p-1)+r_1}\right)\right|_\nu \\ &= |(n_1(p-1)+r_1)\log_\nu(\xi)|_\nu \\ &= |n_1 + r_2|_\nu C \end{aligned}$$

where $C = |\log_\nu(\xi)|_\nu > 0$ and $r_2 = \frac{r_1}{p-1}$. The p–adic expansion of n_1 is $n_1 = a_0 + a_1 p + \ldots + a_m p^m$ where $a_0, \ldots, a_m \in \mathbf{F}_p$ for some $m \geq 0$. Clearly $p^m \leq n_1 < p^{m+1}$. Thus

$$\frac{C}{n_1} \leq \frac{C}{p^m} \leq |n_1 + r_2|_\nu C = |\xi^n - 1|_\nu < 1 \tag{20}$$

and (17) is established. Hence

$$\lim_{n\to\infty} \frac{1}{n} \log|Fix_n(\theta)| = \sum_\nu \log^+ |\xi|_\nu = h(\theta). \tag{21}$$

□

The case when $S = \emptyset$ and ξ is on the unit circle but not a root of unity is an example of a *quasihyperbolic* toral endomorphism. As shown in Lind's paper on quasihyperbolic toral automorphisms [26] Section 4, the existence of the limit

$$\lim_{n\to\infty} \frac{1}{n} \log|Fix_n(\theta)| = h(\theta)$$

is equivalent to the validity of Gelfond's lower bound, Lemma 4.2. The growth rate of $|Fix_n(\theta)|$ is exponential.

Remark

Let α be a $\mathbf{Z}^d$–action on a compact group X (as defined in Chapter 1). For a finite–index subgroup Λ in $\mathbf{Z}^d$ put

$$Fix_\Lambda(\alpha) = \{x \in X : \alpha^{\mathbf{n}}(x) = x \text{ for all } \mathbf{n} \in \Lambda\},$$

the subgroup of Λ-periodic points. We measure the size of the period Λ by setting $\|\Lambda\| = dist(\mathbf{0}, \Lambda \setminus \{\mathbf{0}\})$ with $dist$ the usual metric on $\mathbf{Z}^d$. In analogy with (14), the growth rates considered are

$$p^+(\alpha) = \limsup_{\|\Lambda\|\to\infty} \frac{1}{|\mathbf{Z}/\Lambda|} \log|Fix_\Lambda(\alpha)|, \;\; p^-(\alpha) = \liminf_{\|\Lambda\|\to\infty} \frac{1}{|\mathbf{Z}/\Lambda|} \log|Fix_\Lambda(\alpha)|.$$

Theorem 7.1 in [29] states that if α is expansive on X then

$$p^+(\alpha) = p^-(\alpha) = h(\alpha).$$

Theorem 4.3 is of particular interest because it provides us with non–expansive, non–toral examples for which (16) holds, and, as we shall see later, they may have irrational zeta functions.

□

Theorem 4.4 *Let $(\hat{R}_S, \theta)$ be an ergodic geometric S–integer dynamical system with S finite. Then*

$$p^+(\theta) = h(\theta). \tag{22}$$

Proof. The periodic points formula in Corollary 4.1 gives

$$\frac{1}{n}\log|Fix_n(\theta)| = \sum_{\nu\in S\cup P_\infty:\xi\notin r_\nu^*} \log^+|\xi|_\nu + \frac{1}{n}\sum_{\nu\in S'}\log|\xi^n - 1|_\nu,$$

where $S' \subseteq S$ for which $\xi \in r_\nu^*$ for all $\nu \in S'$. It will be convenient to split S' into sets A and B defined as,

$$A = \{\nu \in S' : |\xi - 1|_\nu = 1\} \text{ and}$$

$$B = \{\nu \in S' : |\xi - 1|_\nu < 1\}.$$

Let $\nu \in A$, then the general theory of valuations shows that ξ admits a convergent series expansion,

$$\xi = \sum_{i=0}^{\infty} a_i \pi^i, \tag{23}$$

where π is an element of k satisfying $ord_\nu(\pi) = \frac{1}{e}$, the index of ramification is denoted by e and the coefficients come from the residue class field L. The field L is isomorphic to a finite extension of $\mathbf{F}_p$ with $[L : \mathbf{F}_p] \le [k_\nu : (\mathbf{F}_p(T))_\nu]$ and $a_0 \ne 0, 1$ since $|\xi|_\nu = |\xi - 1|_\nu = 1$. Note that in the special case $k = \mathbf{F}_p(T)$, the field L is taken as the set of polynomials $g \in \mathbf{F}_p[T]$ with $deg(g) < deg(\nu)$, so $L \cong \mathbf{F}_{p^{deg(\nu)}}$. Let d denote the order of a_0 in the multiplicative group L^*, so $d \ge 2$. Then $|\xi^n - 1|_\nu = 1$ if and only if $d \not| n$. For each $\nu_1, \ldots, \nu_m \in A$ we can associate integers $d_1, \ldots, d_m \geq 2$ such that $|\xi^n - 1|_{\nu_j} = 1$ if and only if $d_j \not| n$.

Now consider the valuations $\nu_1, \ldots, \nu_l \in B$. If $\nu \in B$ we may write

$$\xi = 1 + \sum_{i=1}^{\infty} a_i \pi^i,$$

where a_i and π are as above, and $|\xi - 1|_\nu = |\pi|_\nu^t$ where $t = \min\{i : a_i \neq 0\} > 0$. For each $\nu_j \in B$ label such t by t_j, the coefficients a_i by $a_i(j)$ and π by π_j. Then we have,

$$\begin{aligned} \frac{1}{n} \sum_{\nu \in B} \log |\xi^n - 1|_\nu &= \frac{1}{n} \sum_{\nu \in B} \log |\xi - 1|_\nu + \frac{1}{n} \sum_{\nu \in B} \log |\xi^{n-1} + \cdots + \xi + 1|_\nu \\ &= \frac{1}{n} \sum_{j=1}^{l} \log |\pi_j|_{\nu_j}^{t_j} + \frac{1}{n} \sum_{j=1}^{l} \log \left| n + \sum_{i=1}^{\infty} b_i(j) {\pi_j}^i \right|_{\nu_j}, \end{aligned}$$

for computable coefficients $b_i(j) \in r_{\nu_j}^*$ and $j = 1, \ldots, l$. Clearly this expression tends to zero if $p \not| n$. Hence

$$\frac{1}{n} \sum_{\nu \in S'} \log |\xi^n - 1|_\nu \to 0 \text{ as } n \to \infty$$

through the set

$$\{n \geq 1 : p \not| n, d_j \not| n \text{ for } j = 1, \ldots, m\}.$$

It follows that $p^+(\theta) = h(\theta)$.

□

4.3 Zeta Functions

Theorem 4.5 *Let X be a compact, connected group (necessarily abelian) and let α be an expansive automorphism of X, then ζ_α is rational.*

Proof. By Theorem 6.1 in [20], X is isomorphic to

$$Y_{H(A)} = \left\{ x = \{x_i\}_{-\infty}^{\infty} \in (\mathbf{T}^d)^{\mathbf{Z}} : (x_i, x_{i+1}) \in H(A) \text{ for all } i \in \mathbf{Z} \right\},$$

where $H(A) \subset \mathbf{T}^d \times \mathbf{T}^d$ is defined by

$$H(A) = \tau\left(\{(y, Ay) : y \in \mathbf{R}^d\}\right)$$

for some $d \geq 1$, $A \in GL(d, \mathbf{Q})$ and τ is the quotient map $\mathbf{R}^d \times \mathbf{R}^d \to \mathbf{T}^d \times \mathbf{T}^d$. The isomorphism carries α to T^A, the shift on $Y_{H(A)}$. The group $Y_{H(A)}$ is a *generalised solenoidal group* as studied by Lawton in [24]. Let m be the least positive integer for which mA has integer entries. Then the number of periodic points is given by

$$|Fix_n(\alpha)| = m^n \prod |\lambda_i^n - 1|$$

where $\lambda_1, \ldots, \lambda_t$ are the eigenvalues of mA. Finally, since α is expansive, Theorem 21 in [24] shows that the eigenvalues of mA are not of modulus 1, hence expanding the finite product shows that the zeta function is rational.

□

For example, if $A = [3/2]$ then $(Y_{H(A)}, T^A)$ is homeomorphic to the one–dimensional solenoidal automorphism dual to multiplication by $3/2$ on $\mathbf{Z}[\frac{1}{6}]$ and the number of points of period n is $3^n - 2^n$.

Theorem 4.6 *Let X be a compact, zero–dimensional topological group and α be an expansive automorphism, then ζ_α is rational if and only if α is ergodic.*

Proof. By Kitchens Theorem 1(ii) in [19], (X, α) is homeomorphic to $(F, \psi) \times (G^{\mathbf{Z}}, \sigma)$ where F is a finite group, ψ is an automorphism, G is a finite group and σ is the shift. For $n \geq 1$,

$$|Fix_n(\alpha)| = |Fix_n(\psi \times \sigma)| = |Fix_n(\psi)| \cdot |G|^n,$$

which is finite. So the zeta function is given by

$$\zeta_\alpha(z) = \exp\left(\sum_{n=1}^{\infty} \frac{|Fix_n(\alpha)|}{n} z^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{|Fix_n(\psi)| \cdot |G|^n}{n} z^n\right).$$

Since ψ is an automorphism of a finite group there exists $m > 0$ such that $\psi^m \equiv Id$ for all $x \in F$. Therefore,

$$|Fix_n(\alpha)| = \begin{cases} a|G|^n & \text{if } n \in m\mathbf{Z}+1, \\ a_2|G|^n & \text{if } n \in m\mathbf{Z}+2, \\ \vdots & \\ a_{m-1}|G|^n & \text{if } n \in m\mathbf{Z}+(m-1), \\ a_m|G|^n & \text{if } n \in m\mathbf{Z}, \end{cases}$$

where $a_1, a_2 \ldots, a_m = |F|$ are positive constants. We can capture the numbers $\{|Fix_n(\alpha)| : n \in \mathbf{N}\}$ in a recurrence sequence as follows. Set $f_n = |Fix_n(\alpha)|$ and define the relation

$$f_{n+m} = f_n|G|^m$$

for $n = 1, 2, \ldots$ together with the initial conditions

$$f_1 = a_1|G|, f_2 = a_2|G|^2, \ldots, f_m = a_m|G|^m. \tag{24}$$

So $\sum_{n=1}^{\infty} f_n z^n$ represents the rational function

$$\frac{\sum_{j=1}^{m} a_j(|G|z)^j}{1-(|G|z)^m}.$$

Now, by Theorem 1.12 in [56], $(G^{\mathbf{Z}}, \sigma)$ is ergodic, so α is ergodic if and only if $F = \{e\}$. Clearly the ergodic systems have rational zeta functions of the form $\frac{1}{1-|G|z}$.

Suppose that $|F| > 1$, then the sequence f_n has a *power sum* representation (as shown in [38]),

$$f_n = \sum_{i=1}^{m} \alpha_i \beta_i^n,$$

where each β_i is of the form $|G| \times \eta_i$, where $\{\eta_1, \ldots, \eta_m\}$ is a complete set of m-th unit roots, and the α_i's are constant algebraic numbers. We claim that the α_i's cannot all be ± 1. To see this, notice that the initial conditions (24) require that

$$f_k = (\alpha_1 \eta_1^k + \cdots + \alpha_m \eta_m^k)|G|^k = a_k|G|^k$$

for $k = 1, \ldots, m$. One of the η_i's is equal to 1; let it be η_j. Summing over k, we find that

$$a_1 + a_2 + \cdots + a_m = m\alpha_j.$$

Recall that $a_i \geq 1$ for all i, so if $\alpha_j = \pm 1$, then $\alpha_j = 1$ and $a_k = 1$ for $k = 1, \ldots, m$, which is impossible since $a_m = |F| > 1$. It follows (see, for example, Exercise 6, Section V.1 of [21]) that ζ_α is irrational.

□

Theorem 4.7 *If $(\hat{R}_S, \theta)$ is expansive, then the zeta function ζ_θ is rational.*

Proof. By the criteria for expansiveness in Theorem 3.4 we have for all $n \geq 1$,

$$|Fix_n(\theta)| = \begin{cases} \left(\prod_{\nu \in P_\infty} |\xi^n - 1|_\nu\right) {C_1}^n & \text{in the arithmetic case,} \\ {C_2}^n & \text{in the geometric case,} \end{cases}$$

where $C_1 = \prod_{\nu \in S} |\xi|_\nu$ and $C_2 = \prod_{\nu \in S \cup P_\infty} |\xi|_\nu$ are positive constants. In the former, the Galois conjugates of ξ are not of modulus 1 so we may derive a rational expression for ζ_θ. The geometric result is obvious.

□

Example 4.2 Let θ be the expansive action of $\widehat{\mathbf{Z}[\frac{1}{6}]}$ dual to $\times\frac{2}{3}$ on $\mathbf{Z}[\frac{1}{6}]$. The entropy of θ is $\log 3$ and for each $n \geq 1$,

$$\begin{aligned} |Fix_n(\theta)| &= \left|\left(\frac{2}{3}\right)^n - 1\right|_\infty \left|\left(\frac{2}{3}\right)^n - 1\right|_2 \left|\left(\frac{2}{3}\right)^n - 1\right|_3 \\ &= 3^n - 2^n. \end{aligned}$$

The zeta function is given by

$$\begin{aligned} \zeta_\theta(z) &= \exp\left(\sum_{n=1}^{\infty} \frac{(3^n - 2^n) z^n}{n}\right) \\ &= \frac{1 - 2z}{1 - 3z}. \end{aligned}$$

Example 4.3 Let θ be the endomorphism of $\widehat{\mathbf{Z}[\frac{1}{30}]}$ dual to $\times\frac{3}{2}$ on $\mathbf{Z}[\frac{1}{30}]$. By Theorem 3.4 θ is non–expansive (since $|\frac{3}{2}|_5 = 1$). The number of points of period n is given by

$$\begin{aligned} |Fix_n(\theta)| &= \left|\left(\frac{3}{2}\right)^n - 1\right|_\infty \left|\left(\frac{3}{2}\right)^n - 1\right|_2 \left|\left(\frac{3}{2}\right)^n - 1\right|_3 \left|\left(\frac{3}{2}\right)^n - 1\right|_5 \\ &= (3^n - 2^n)\, |3^n - 2^n|_5 \end{aligned}$$

and its first few values are

$$1, 1, 19, 13, 211, 133, 2059, 1261, 19171, 2321, 175099, \ldots$$

By Theorem 4.3 the logarithmic growth rate of this sequence is equal to $\log 3$, the entropy of θ. We claim that ζ_θ is irrational and we shall use the following results on rational functions and recurrence sequences to prove this:

Theorem 4.8 (Hadamard Quotient Theorem) *Let* $\mathbf{F}$ *be a field of characteristic zero and* (a'_n) *a sequence of elements of a subring* R *of* $\mathbf{F}$ *which is finitely generated over* $\mathbf{Z}$*. Let* $\sum b_n X^n$ *and* $\sum c_n X^n$ *be formal series over* $\mathbf{F}$ *representing rational functions. Denote by* J *the set of integers* $n \geq 0$ *such that* $b_n \neq 0$*. Suppose that* $a'_n = c_n / b_n$ *for all* $n \in J$*. Then there is a sequence* (a_n) *with* $a_n = a'_n$ *for* $n \in J$*, such that the series* $\sum a_n X^n$ *represents a rational function.*

Proof. See [37] and the lecture notes of [41] for a proof, and [38] for a general discussion.

$\square$

Proposition 4.1 *The number of values that a recurrence sequence can take on infinitely often is bounded by some integer* l *that depends only on the poles of its generating rational function.*

Proof. See Proposition 2 in [35].

$\square$

Returning to Example 4.3 suppose, for a contradicton, that ζ_θ is rational. Then by differentiating ζ_θ, $\sum_{n=1}^{\infty} |Fix_n(\theta)| z^n$ is also rational. The sequence defined by $a_n = 3^n - 2^n$ is a recurrence sequence since it satisfies the linear, homogeneous recurrence relation

$$a_{n+2} = 5a_{n+1} - 6a_n,$$

together with the initial conditions $a_0 = 0, a_1 = 1$. Hence $\sum_{n=1}^{\infty} a_n z^n$ represents the rational function

$$\frac{z}{1 - 5z + 6z^2}.$$

By the Hadamard Quotient Theorem, with $|Fix_n(\theta)| \neq 0$,

$$\sum_{n=1}^{\infty} \frac{z^n}{|3^n - 2^n|_5}$$

is a rational function $P(z)/Q(z)$ and hence $b_n = |3^n - 2^n|_5^{-1}$ is a recurrence sequence. The Taylor series coefficients are given by,

$$b_n = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 5^{1+ord_5(n)} & \text{if } n \text{ is even.} \end{cases}$$

By the above Proposition the number of values that b_n can take on infinitely often is bounded by some integer depending on the roots of $Q(z)$. However, the set $\{1, 5, 5^2, \ldots\}$ is infinite, giving a contradiction. Hence ζ_θ is irrational.

Example 4.4 Let $k = \mathbf{F}_p(T)$ and $S = \{T\}$. Define θ to be the endomorphism of $\hat{R}_S = \widehat{\mathbf{F}[T^{\pm 1}]}$ dual to multiplication by T on $\mathbf{F}_p[T^{\pm 1}]$. The entropy of θ is

$$h(\theta) = \sum_{\nu \leq \infty} \log^+ |T|_\nu = \log p$$

and the number of periodic points is given by

$$\begin{aligned} |Fix_n(\theta)| &= |T^n - 1|_\infty |T^n - 1|_T \\ &= p^n. \end{aligned}$$

Alternatively, we may note that $\hat{R}_S \cong \widehat{\oplus_{\mathbf{Z}} \mathbf{F}_p} \cong {\mathbf{F}_p}^{\mathbf{Z}}$ and that θ is the one–sided (expansive) shift action on p symbols. Thus the entropy and the number of periodic points is as expected. Clearly $\zeta_\theta(z) = \frac{1}{1-pz}$.

Example 4.5 Let $k = \mathbf{F}_p(T)$ and $S = \{T - 1\}$. Define θ to be the endomorphism of $\hat{R}_S = \widehat{\mathbf{F}_p[T][\frac{1}{T-1}]}$ dual to multiplication by T on $\mathbf{F}_p[T][\frac{1}{T-1}]$. The entropy of θ is once again $\log p$ and the number of periodic points is given by

$$\begin{aligned} |Fix_n(\theta)| &= |T^n - 1|_\infty |T^n - 1|_{T-1} \\ &= p^{n - p^{ord_p(n)}}. \end{aligned}$$

Suppose, if possible, that ζ_θ is rational, then $\sum_{n=1}^{\infty} |Fix_n(\theta)| z^n$ is also rational. We already know that $\sum_{n=1}^{\infty} p^n z^n = \frac{1}{1-pz}$ is rational. Proceeding in the manner previously described we see that

$$\frac{p^n}{|Fix_n(\theta)|} = p^{p^{ord_p(n)}}$$

is a sequence in $\mathbf{Z}$, and by the Hadamard Quotient Theorem

$$\sum_{n=1}^{\infty} p^{p^{ord_p(n)}} z^n$$

is a rational function. However the recurrence sequence $p^{p^{ord_p(n)}}$ has an infinite number of values that it takes on infinitely often, namely $\{p, p^p, p^{p^2}, \ldots\}$. This contradicts Proposition 4.1 and means that ζ_θ is irrational, and so θ is non–expansive.

Furthermore, writing $n = qp^{ord_p(n)}$ where $p \not| q$, we have

$$\begin{aligned} |Fix_n(\theta)| &= |T^n - 1|_\infty \, |T^q - 1|_{T-1}^{p^{ord_p(n)}} \\ &= p^n p^{-p^{ord_p(n)}} \text{ since } p \not| q \\ &= p^{n\left(1-\frac{1}{q}\right)}. \end{aligned}$$

So for a sequence $n_j \to \infty$ with $n_j / p^{ord_p(n_j)} = q$ for a fixed $q, p \not| q$,

$$\lim_{ord_p(n_j) \to \infty} \frac{1}{n_j} \log |Fix_{n_j}(\theta)| = \left(1 - \frac{1}{q}\right) \log p.$$

Also, $p^+(\theta) = h(\theta)$ is obtained by letting $n \to \infty$ through numbers coprime with p. Hence the set of limit points of $\left\{\frac{1}{n} \log |Fix_n(\theta)|\right\}_{n=1}^{\infty}$ is

$$\left\{ \left(1 - \frac{1}{q}\right) h(\theta) : q \in \mathbf{N}, p \not| q \right\} \cup \{h(\theta)\}.$$

Chapter 5

The Distribution of Periodic Points

5.1 Invariant Measures on Compact Spaces

Let X be a compact metric space and let $\mathcal{B}$ denote its Borel σ–algebra. We define $\mathcal{M}(X)$ to be the collection of all Borel probability measures on X. If $T : X \to X$ is a continuous transformation, let $\mathcal{M}_T(X)$ denote the set of measures μ in $\mathcal{M}(X)$ which are T–invariant (those for which T is a measure–preserving transformation of $(X, \mathcal{B}, \mu)$).

We now introduce the *weak* topology* on $\mathcal{M}(X)$. Let $C(X)$ be the space of all continuous complex–valued functions $f : X \to \mathbf{C}$, endowed with the norm

$$\|f\| = \sup_{x \in X} |f(x)|.$$

Let $J : C(X) \to \mathbf{C}$ be a continuous, positive linear functional (positive means if $f \geq 0$ then $J(f) \geq 0$) with $J(1) = 1$, where $1 \in C(X)$ is the constant function 1. By the Riesz Representation Theorem there exists a unique $\mu \in \mathcal{M}(X)$ such that

$$\int_X f d\mu = J(f) \text{ for all } f \in C(X).$$

For the proof see [36]. The map $\mu \mapsto J_\mu (= J(f))$ is therefore surjective. Theorem 6.2 in [56] shows that if $\mu \neq \nu$ then $J_\mu \neq J_\nu$, showing that this assignment is injective.

Finally, since $\mu \in \mathcal{M}(X)$ is a probability measure the map $\mu \mapsto J_\mu$ is a bijective correspondence between $\mathcal{M}(X)$ and its image in the unit ball $B = \{f \in C(X) : \|f\| \leq 1\}$ in $C(X)$.

Now the set of continuous, positive linear functionals E on the Banach space $C(X)$ can be endowed with several topologies, one of which is known as the weak* topology. The bijection between B and $\mathcal{M}(X)$ allows us to impose this particular topology on $\mathcal{M}(X)$. It is the coarsest topology with respect to which the mapping $\mu \mapsto J_\mu$ is continuous. A topological base for $\mathcal{M}(X)$ is given by the sets

$$V_{f,\epsilon}(\mu) = \left\{\nu \in \mathcal{M}(X) : \left|\int_X f d\nu - \int_X f d\mu\right| < \epsilon\right\},$$

where $\epsilon > 0$ and $f \in C(X)$. Furthermore, since X is compact, there exists a dense subset $\{f_n\}_{n=1}^\infty$ of $C(X)$ which is dense in B. The weak* topology can be induced by the metric $D : \mathcal{M}(X) \times \mathcal{M}(X) \to \mathbf{R}$ defined by

$$D(\mu,\nu) = \sum_{n=1}^\infty \frac{1}{2^n}\left|\int_X f_n d\mu - \int_X f_n d\nu\right|. \tag{25}$$

It follows that $(\mathcal{M}(X), D)$ (and so too $(B, \|.\|)$) is a compact metric space – see Theorem 6.5 in [56] for a direct proof using sequential compactness. An immediate consequence of (25) is that in the weak* topology,

$$\mu_n \to \mu \text{ in } \mathcal{M}(X) \text{ if and only if } \int_X f d\mu_n \to \int_X f d_\mu \text{ for any } f \in C(X). \tag{26}$$

For instance, suppose $X = [0,1)$, the additive circle, and $\mu_n = \frac{1}{n}\sum_{j=1}^n \delta_{\frac{j}{n}}$ where $\delta_{\frac{j}{n}}$ is the point mass at j/n. Because continuous functions are Riemann integrable, $\int_X f d\mu_n$ is exactly a Riemann sum approximation to $\int_X f d\mu$. Hence μ_n converges weakly to Lebesgue measure on the circle.

The set $\mathcal{M}_T(X)$ is non–empty since invariant measures can always be constructed. For example, if ν is any element in $\mathcal{M}(X)$ then define a sequence $\{\mu_n\}_{n=1}^\infty$ in $\mathcal{M}(X)$ by $\mu_n = \frac{1}{n}\sum_{j=0}^{n-1} T^j\nu$. Clearly any limit point μ of $\{\mu_n\}$ (which exists by compactness of $\mathcal{M}(X)$) is T–invariant. Also $\mathcal{M}_T(X)$ is a compact subset of $\mathcal{M}(X)$.

5.2 Uniform Distribution of Periodic Points

Let T be an ergodic endomorphism of a solenoid and

$$Fix_n(T) = \{x \in X : T^n(x) = x\}$$

denote the set of points of period n. Since T is continuous, $Fix_n(T)$ is a closed subgroup of X for any $n \geq 1$ carrying normalised Haar measure μ_n. If $Fix_n(T)$ is finite, then normalised Haar measure μ_n on $Fix_n(T)$ is defined by,

$$\mu_n(x) = \frac{1}{|Fix_n(T)|} \sum_{x \in Fix_n(T)} \delta_x, \tag{27}$$

where δ_x is the point mass at x. The measures μ_n are in $\mathcal{M}_T(X)$. The dual group of $Fix_n(T)$ is given by

$$\widehat{Fix_n(T)} \cong \Gamma/(\hat{T}^n - 1)\Gamma, \tag{28}$$

where $\Gamma = \hat{X}$, and the Fourier transform of μ_n is given by

$$\begin{aligned}
\hat{\mu}_n(\gamma) &= \int_{Fix_n(T)} \mu_n(x)\gamma(-x)dx \\
&= \frac{1}{|Fix_n(T)|} \sum_{x \in Fix_n(T)} \gamma(x) \\
&= \begin{cases} 1, \text{ if } \gamma \in (\hat{T}^n - 1)\Gamma & (\gamma \text{ is trivial on } Fix_n(T)) \\ 0, \text{ otherwise} & (\gamma \text{ is non–trivial on } Fix_n(T)) \end{cases}
\end{aligned}$$

We say that the periodic points are uniformly distributed with respect to Haar measure $\mu \in \mathcal{M}_T(X)$, or that Haar measure describes the distribution of the periodic points of T, if $\mu_n \to \mu$ weakly in $\mathcal{M}(X)$. In order to prove this weak* convergence it suffices to establish (26) for all non–trivial characters in $\hat{X}$. This is because finite linear combinations of such functions are dense in $C(X)$ by the Stone–Weierstrass Theorem. Thus $\mu_n \to \mu$ weakly if and only if $\hat{\mu}_n \to \hat{\mu}$ pointwise on $\Gamma = \hat{X}$, that is, there exists $N(\gamma) > 0$ such that $\gamma \notin (\hat{T}^n - 1)\Gamma$ for all $n \geq N(\gamma)$.

Lind first proved the uniform distribution of periodic points for ergodic toral automorphisms in [26]. Waddington has given an alternative proof in [54] which, as shall be seen, applies to ergodic arithmetic S–integer systems. We shall prove that if $|Fix_{n_j}(\theta)| \to \infty$ as $j \to \infty$ along some subsequence then $\mu_{n_j} \to \mu$ in the weak* topology.

Ward has shown in [57] that the periodic points of an expansive $\mathbf{Z}^d$–action on a compact abelian group are uniformly distributed with respect to Haar measure if the action has completely positive entropy. The methods of [57] do not extend to the non–expansive case because they rely on an exponential growth rate. All the steps of Waddington's proof extend to endomorphisms of solenoids. However, the result that $|Fix_{n_j}(T)| \to \infty$ as $j \to \infty$ along some subsequence implies $\mu_{n_j} \to \mu$ is not true for all solenoids.

Example 5.1 Let $\Gamma = \mathbf{Z} \times \mathbf{Q}$, $X = \hat{\Gamma}$ and $\hat{T} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$. Note that X is a product of S–integer systems and $|Fix_n(T)| = 2^n - 1$. Clearly the periodic point measures converge to Haar measure on $\mathbf{T} \times \{1\}$, a closed subgroup of X.

Finite products of S–integer dynamical systems with $S = \emptyset$ yield toral endomorphisms, but the converse does not hold as illustrated by the following example due to Williams [62].

Example 5.2 Let T_A and T_B be the automorphisms of the 2–torus $\mathbf{T}^2$ defined by the unimodular matrices,

$$A = \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}.$$

Then the matrices A and B have the same characteristic polynomial $\chi_A(x) = \chi_B(x) = x^2 - 4x - 1$. The system $(T_A, \mathbf{T}^2)$ is isomorphic to the S–integer system with $k = \mathbf{Q}(\sqrt{5})$, $S = \emptyset$ and $\xi = 2 + \sqrt{5}$. So, if $(T_B, \mathbf{T}^2)$ were an S–integer system then k, S and ξ would be the same as above. We prove that this is not the case by making use of the following result found in Section 11, (3) of Williams [62].

Lemma 5.1 *Let C be an integer matrix with $AC = CB$. Then the determinant of C is even.*

Thus A and B cannot be conjugate elements of $GL(2, \mathbf{Z})$. So $(T_A, \mathbf{T}^2)$ and $(T_B, \mathbf{T}^2)$ are not even topologically conjugate.

Theorem 5.1 generalises (in an arithmetic direction) a specialisation of Waddington's result.

Theorem 5.1 *Let $(\hat{R}_S, \theta)$ be an ergodic arithmetic S–integer dynamical system. If*

$$|Fix_{n_j}(\theta)| \to \infty \text{ as } j \to \infty$$

along some subsequence then the points of period n_j are uniformly distributed with respect to Haar measure.

Proof. We need to prove that for any non–trivial character $\gamma \in \Gamma \setminus \{0\}$, $\hat{\mu}_{n_j}(\gamma) = 0$ for all n_j sufficiently large. Suppose, for a contradiction, that this is not the case. Then for some fixed j, there exists an infinite subsequence $\{n_{j(k)}\}$ of $\{n_j\}$ and some character $\gamma \in R_S \setminus \{0\}$ such that

$$\gamma \in (\xi^{n_{j(k)}} - 1)R_S \text{ for all } k.$$

Let $< \gamma >$ denote the ideal of R_S generated by γ. So $< \gamma > \subseteq (\xi^{n_{j(k)}} - 1)R_S$ and

$$\left|\frac{R_S}{< \gamma >}\right| \geq \left|\frac{R_S}{(\xi^{n_{j(k)}} - 1)R_S}\right| = |\widehat{Fix_{n_{j(k)}}}(\theta)|. \tag{29}$$

Since θ is ergodic, by Theorem 4.2,

$$\left|\frac{R_S}{< \gamma >}\right| = \prod_{\nu \in S \cup P_\infty} |\xi|_\nu$$

is a constant and $|\widehat{Fix_{n_{j(k)}}}(\theta)| = |Fix_{n_{j(k)}}(\theta)|$. However, our initial hypothesis $|Fix_{n_{j(k)}}(\theta)| \to \infty$ as $j \to \infty$ clearly contradicts (29).

□

Chapter 6

Examples

Example 6.1 Let $k = \mathbf{Q}$ and $S = \emptyset$, so $R_S = \mathbf{Z}$. Let θ be the toral endomorphism dual to multiplication by 2 on $\mathbf{Z}$. The periodic points formula in Corollary 4.1 gives $|Fix_n(\theta)| = 2^n - 1$ for all $n \geq 1$ and clearly

$$\frac{1}{n}\log|2^n - 1| \to \log 2,$$

which is equal to the entropy $h(\theta; \mathbf{T})$. The zeta function is $\zeta_\theta(z) = 1 - z/1 - 2z$.

Example 6.2 Let $k = \mathbf{Q}$ and S consist of all the finite places of $\mathbf{Q}$, then $R_S = \mathbf{Q}$. If θ is as above, acting on the full solenoid $\hat{\mathbf{Q}}$, then $|Fix_n(\theta)| = \prod_{p\leq\infty}|2^n - 1|_p = 1$ for all $n \geq 1$ and $h(\theta; \hat{\mathbf{Q}}) = \log 2$.

Example 6.3 Let k be an $\mathbf{A}$–field and $S = \emptyset$, then $R_S = O_k$ the ring of algebraic integers in k. If $k = \mathbf{Q}(\sqrt{2})$ and $\theta : \hat{O}_k \to \hat{O}_k$ is dual to multiplication by $\sqrt{2}$ on $O_k = \mathbf{Z}[\sqrt{2}]$, then the elements of P_∞ are the valuations induced by the embeddings of $k \to \mathbf{R}$ namely $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{2} \mapsto -\sqrt{2}$. By Corollary 4.1

$$\begin{aligned} |Fix_n(\theta)| &= \left|\left(\sqrt{2}\right)^n - 1\right|_\infty \left|\left(-\sqrt{2}\right)^n - 1\right|_\infty \text{ for all } n \geq 1 \\ &= \begin{cases} 2^n - 1 & \text{if } n \text{ is odd,} \\ \left(2^{n/2} - 1\right)^2 & \text{if } n \text{ is even.} \end{cases} \end{aligned}$$

Also,

$$h(\theta; \hat{O}_k) = \sum_\nu \log^+ \left|\sqrt{2}\right|_\nu$$

$$\begin{aligned} &= \sum_{\nu \in P_\infty} \log^+ \left|\sqrt{2}\right|_\nu \\ &= \log\left|\sqrt{2}\right|_\infty + \log\left|-\sqrt{2}\right|_\infty \\ &= \log 2. \end{aligned}$$

The system $\left(\widehat{\mathbf{Z}[\sqrt{2}]}, \widehat{\times\sqrt{2}}\right)$ is of course isomorphic to the endomorphism of $\mathbf{T}^2$ determined by the matrix $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$.

Example 6.4 Let $k = \mathbf{F}_p(T), S = \{T\}$ and $\xi = T + 1$. Then $\hat{R}_S$ is the two–sided shift space on p symbols, and θ is the non–expansive cellular automaton defined by

$$(\theta(x))_m = x_m + x_{m+1} (\mathrm{mod} p) \text{ for all } x_m \in \mathbf{F}_p, m \in \mathbf{Z}.$$

The entropy of θ is $\log p$ and

$$\begin{aligned} |Fix_n(\theta)| &= |(T+1)^n - 1|_\infty \, |(T+1)^n - 1|_T \\ &= p^n \left| T^n + \binom{n}{1} T^{n-1} + \ldots + \binom{n}{n-1} T \right|_T \\ &= \begin{cases} p^{n-1} & \text{if } p \not| n, \\ 1 & \text{if } p | n. \end{cases} \end{aligned}$$

We claim that the set of limit points of $\left\{\frac{1}{n}\log|Fix_n(\theta)|\right\}_{n=1}^{\infty}$ is

$$\left\{\left(1 - \frac{1}{q}\right) h(\theta) : q \in \mathbf{N}, p \not| q\right\} \cup \{h(\theta)\}.$$

This is easily seen as follows: write $n = qp^{ord_p(n)}$ where $p \not| q$ then,

$$\begin{aligned} |Fix_n(\theta)| &= |(T+1)^n - 1|_\infty |(T+1)^q - 1|_T^{p^{ord_p(n)}} \\ &= p^n p^{-p^{ord_p(n)}} \text{ since } p \not| q \\ &= p^{n\left(1 - \frac{1}{q}\right)}. \end{aligned}$$

So for a sequence $n_j \to \infty$ with $n_j / p^{ord_p(n_j)} = q$ for a fixed $q, p \not| q$,

$$\lim_{ord_p(n_j) \to \infty} \frac{1}{n_j} \log|Fix_{n_j}(\theta)| = \left(1 - \frac{1}{q}\right) \log p.$$

Also, $p^+(\theta) = h(\theta)$ is obtained by letting $n \to \infty$ through the numbers which are coprime with p. Hence the claim is proved.

We shall now restrict our attention to the case $k = \mathbf{Q}$ and S an infinite set. We seek examples where $p^-(\theta)$ and $p^+(\theta)$ can be computed. Such dynamical systems will of course be non–expansive, so examples where $p^+(\theta) = h(\theta)$ (as in the expansive case) will be particularly striking.

Example 6.5 Let k be an algebraic number field and S comprise all but a finite set F of non–archimedean places of k (degenerate situation). Using the Artin–Whaples product formula (8) we have,

$$\begin{aligned} \frac{1}{n}\log|Fix_n(\theta)| &= \frac{1}{n}\sum_{\nu\in P_\infty}\log|\xi^n-1|_\nu - \frac{1}{n}\sum_{\nu\in F\cup P_\infty}\log|\xi^n-1|_\nu \\ &\to 0, \end{aligned}$$

since $|\xi|_\nu \leq 1$ for all $\nu \in F$ and the estimate in (17) holds. Hence $p^+(\theta) = p^-(\theta) = 0$.

6.1 The Mersenne Dynamical System

Example 6.6 Let $k = \mathbf{Q}$ and fix $\xi = 2$. Define S to be the set of places $|.|_{M_p}$ for which the corresponding Mersenne number $M_p = 2^p - 1$ is prime. There are different heuristic theories giving strong evidence that M_p is prime for infinitely many values of p. Wagstaff has conjectured in [55] that the number of Mersenne primes less than x is about

$$\frac{e^\gamma}{\log 2}\log\log x = (2.5695\ldots)\log\log x.$$

We therefore conjecture that $S = \{3, 7, 31, 127, \ldots\}$ is infinite. Denote the elements of S by $p_1, p_2, \ldots$ where $p_i < p_j$ if and only if $i < j$.

Theorem 6.1 *If there are infinitely many Mersenne primes then $p^-(\theta) = 0$ and $p^+(\theta) = h(\theta)$.*

Proof. Define a sequence n_m such that $M_{n_m} = p_m$ for all $m > 0$, that is, the indices giving the Mersenne primes, then we have

$$\frac{1}{n_m}\log|Fix_{n_m}(\theta)| = \frac{1}{n_m}\log(2^{n_m}-1) + \frac{1}{n_m}\sum_{M_p\in S}\log|2^{n_m}-1|_{M_p}$$

$$
\begin{aligned}
&= \frac{1}{n_m}\log(2^{n_m}-1)+\frac{1}{n_m}\log|2^{n_m}-1|_{p_m} \\
&= \frac{1}{n_m}\log(2^{n_m}-1)-\frac{\log(2^{n_m}-1)}{n_m} \\
&= 0.
\end{aligned}
$$

Hence $p^-(\theta)=0$.

In order to compute the upper growth rate, define a sequence n_l^* by $(n_l^*, n_m)=1$ for all $l,m>0$. For example, we could set $n_l^*=11^l$ because 11 is coprime with the Mersenne indices $2,3,5,7,13,\ldots$ for all $l>0$. We claim that

$$2^{n_l^*}\equiv 1 \bmod M_{n_m} \text{ for some } l,m>0 \Rightarrow n_m|n_l^*.$$

Write $n_l^*=\alpha(M_{n_m}-1)+\beta$ where $0\le\beta<M_{n_m}-1$. Then by Fermat's Little Theorem,

$$2^{n_l^*}\equiv 1 \bmod M_{n_m} \Rightarrow 2^\beta\equiv 1 \bmod M_{n_m}.$$

Note that the order of 2 mod M_{n_m} is n_m, so $n_m|\beta$. Also $M_{n_m}-1=2^{n_m}-2\equiv 0 \bmod n_m$ by Fermat again. Therefore $n_m|M_{n_m}-1, n_m|\beta$ and so $n_m|n_l^*$. Hence the claim is proved and since it contradicts the definition of n_l^* we deduce that,

$$\frac{1}{n_l^*}\log|Fix_{n_l^*}(\theta)|=\frac{1}{n_l^*}\log|2^{n_l^*}-1|_\infty\to\log 2.$$

□

Theorem 6.2 *If there are infinitely many Mersenne primes, then the set of limit points of* $\left\{\frac{1}{n}\log|Fix_n(\theta)|\right\}_{n=1}^\infty$ *is*

$$\left\{\left(1-\frac{1}{q}\right)h(\theta):q\in\mathbf{N}\right\}\cup\{h(\theta)\}.$$

Proof. These limit points bear an elegant resemblance to Examples 4.5 and 6.4, suggesting, perhaps, a more general result.

We once again use the sequence of Mersenne indices n_m mentioned above. Observe that $2^{n_m}\equiv 1 \bmod M_{n_m}$ implies that $2^{qn_m}\equiv 1 \bmod M_{n_m}$, so

$$|2^{qn_m}-1|_{M_{n_m}}\le\frac{1}{M_{n_m}}.$$

We claim that equality holds for all n_m sufficiently large. To see this note that the order of 2 mod $M_{n_m}^2$ is $n_m M_{n_m}$ since

$$(2^{n_m})^{M_{n_m}} = (1 + M_{n_m})^{M_{n_m}} \equiv 1 \bmod M_{n_m}^2.$$

So if n_m is greater than the exponent of the largest Mersenne prime factor of q, say $M(q)$, then $|2^{qn_m} - 1|_{M_{n_m}} = \frac{1}{M_{n_m}}$. Thus we have

$$\begin{aligned}
\frac{1}{qn_m} \log |Fix_{qn_m}(\theta)| &= \frac{1}{qn_m} \log |2^{qn_m} - 1|_\infty + \frac{1}{qn_m} \sum_{M_p \in S} \log |2^{qn_m} - 1|_{M_p} \\
&= \frac{1}{qn_m} \log(2^{qn_m} - 1) + \frac{1}{qn_m} \log \left(\frac{1}{M_{n_m}} \right) \text{ for all } n_m > M(q) \\
&\to \left(1 - \frac{1}{q}\right) \log 2 \text{ as } m \to \infty.
\end{aligned}$$

To prove that no other limit points exist, write $n = ab$ and let $a \to \infty$ through the Mersenne indices. We have two possibilities. Firstly, if $(a, b) = 1$ for a, b sufficiently large then

$$\begin{aligned}
\frac{1}{n} \log |Fix_n(\theta)| &= \frac{1}{ab} \log(2^{ab} - 1) + \frac{1}{ab} \log(\frac{1}{2^a - 1}) \text{ for all } a, b \text{ sufficiently large} \\
&\to \log 2 \text{ as } a, b \to \infty.
\end{aligned}$$

Otherwise $b \to \infty$ through the set $\{qa^j : q, j \in \mathbf{N}\}$. Hence

$$\begin{aligned}
\frac{1}{n} \log |Fix_n(\theta)| &= \frac{1}{qa^{j+1}} \log \left(2^{qa^{j+1}} - 1\right) + \frac{1}{qa^{j+1}} \sum_{M_p \in S} \log \left|2^{qa^{j+1}} - 1\right|_{M_p} \\
&= \frac{1}{qa^{j+1}} \log \left(2^{qa^{j+1}} - 1\right) + \frac{1}{qa^{j+1}} \log \left(\frac{1}{(2^a - 1)^{j+1}} \right) \text{ for all } a > M(q) \\
&\to \left(1 - \frac{1}{q}\right) \log 2 \text{ as } a \to \infty.
\end{aligned}$$

□

For this example the zeta function would then have an infinite number of isolated singularities at $\frac{1}{2}, 1, 2^{\frac{1}{2}}, 2^{\frac{2}{3}}, 2^{\frac{3}{4}}, \ldots$. Also, assuming the conjecture holds, there are sequences along which the periodic point measures converge weakly to Haar measure on $\mathbf{Z}[\widehat{\frac{1}{3 \cdot 7 \cdot 31 \cdot 127 \cdots}}]$.

6.2 The Artin–Inspired Dynamical Systems

Example 6.7 Let $k = \mathbf{Q}$ and suppose ξ is a non–zero integer. Recall that ξ is said to be a *primitive root* modulo a prime p if and only if the residue classes modulo p of $\xi, \xi^2, \dots, \xi^{p-1} \equiv 1$ are all distinct. The number of primitive roots modulo p is $\phi(p-1)$, where ϕ is the Euler function. For example, 2 is not a primitive root modulo 7 since $2^3 \equiv 1 (\mathrm{mod}\ 7)$. In 1927 [3], Artin made the following conjecture: if a is neither a square nor -1, then there exist infinitely many primes such that a is a primitive root modulo p. The quantative version of Artin's conjecture is the following statement (see [17]): if $N_a(x)$ is the number of primes less than x for which a is a primitive root, then

$$N_a(x) \sim A \frac{x}{\ln x} \tag{30}$$

where A depends only on a. So, if we choose $\xi \in \mathbf{Z}$ to be neither a square nor -1 and define S to be the set of places $|.|_p$ for which ξ is a primitive root modulo p, then if Artin's conjecture holds S is an infinite set of places. Let θ be the endomorphism of $\hat{R}_S$ dual to multiplication by ξ on R_S.

Theorem 6.3 *If Artin's conjecture holds for ξ then $p^+(\theta) = h(\theta)$.*

Proof. Since $|\xi^n - 1|_p = 1$ if and only if $p - 1 \not| n$ for each $p \in S$, we have

$$\frac{1}{n} \log |Fix_n(\theta)| = \frac{1}{n} \log |\xi^n - 1|_\infty + \frac{1}{n} \sum_{p \in S: p-1|n} \log |\xi^n - 1|_p. \tag{31}$$

So by letting $n \to \infty$ through all the prime numbers, we get

$$\limsup_{n\to\infty} \frac{1}{n} \log |Fix_n(\theta)| = \log |\xi| = h(\theta). \tag{32}$$

□

Theorem 6.4 *There are infinitely many primes p with either 2 or 3 or 5 as a primitive root – but we do not know which one !*

Proof. See Heath–Brown's paper [7] in which he proves the ground–breaking theorem that, with the exception of at most two primes q_1, q_2 the following is true: For each prime q there are infinitely many primes p with q a primitive root modulo p.

□

Corollary 6.1 *There exist non–expansive systems* $(\hat{R}_S, \theta)$ *with* S *infinite and non–degenerate such that* $p^+(\theta) = h(\theta)$*, although we cannot explicitly identify them.*

These dynamical systems have the remarkable property that on the one hand they mimic hyperbolic behaviour ($p^+(\theta) = h(\theta)$), while on the other they have infinitely many directions in which they behave as isometries. For example, suppose that Artin's conjecture holds for 2 then the system determined by multiplication by 2 on $\mathbf{Z}[\frac{1}{3\cdot5\cdot11\cdots}]$ where the primes p are such that 2 is a primitive modulo p, has isometries given by the automorphism multiplication by 2 on $\mathbf{Q}_p$ for infinitely many p.

Conjecture 6.1 *If Artin's conjecture holds for* ξ *then* $p^-(\theta) = p^+(\theta) = h(\theta)$.

Evidence. The matter of $p^-(\theta)$ is immersed in the harder realms of prime number theory. We would guess that if S is sufficiently sparse but still infinite, then $\lim_{n\to\infty} \frac{1}{n} \log |Fix_n(\theta)|$ exists and equals the entropy of θ. Whilst the primitive root approach gives us *some* control over the n's for which $p|\xi^n - 1$, it seems difficult to control the size of $ord_p(\xi^n - 1)$. Indeed, for this example we have the following bound,

$$\inf_p \left\{ \frac{ord_p(\xi^{p-1} - 1)}{p} \right\} \ll \frac{1}{n} \sum_{p\in S: p-1|n} \log|\xi^n - 1|_p < 0.$$

Standard conjectures in prime number theory imply that

$$\liminf_{p\to\infty} \left\{ \frac{ord_p(\xi^{p-1} - 1)}{p} \right\} = 0$$

and so for these examples, $p^-(\theta) = p^+(\theta) = h(\theta)$ is expected. This is really all we can say about $p^-(\theta)$.

Example 6.8 The following example, though conjectorial, raises our hopes for the existence of dynamical systems satisfying

$$p^+(\theta) = p^-(\theta) = h(\theta) > 0,$$

with S infinite. It came about following a private communication with Heath–Brown.

Definition 6.1 For $m > 1$ an integer g is called a *primitive root* modulo m if the least positive integer t satisfying

$$g^t \equiv 1 (\bmod m)$$

is $\phi(m)$.

Let S be the set of places $|.|_p$ such that ξ is a primitive root modulo p^2, for some integer $\xi \neq 0, \pm 1$. The following assertions are equivalent as pointed out in Chapter 2 of [40]:

1. ξ is a primitive root modulo p and $\xi^{p-1} \not\equiv 1 (\bmod p^2)$;

2. ξ is a primitive root modulo p^2;

3. for every $m \geq 2$, ξ is a primitive root modulo p^m.

Now, the research into Wieferich primes and the Fermat quotient suggests that $\xi^{p-1} \not\equiv 1 (\bmod \ p^2)$ for infinitely many primes (see [39] and [40]), therefore, together with Artin's conjecture, it seems reasonable to conjecture that S is an infinite set.

Theorem 6.5 *If ξ is a primitive root modulo p^2 for infinitely many primes p, then*

$$p^+(\theta) = p^-(\theta) = h(\theta) > 0. \tag{33}$$

Proof. First observe that, given $l \geq 1$,

$$p^l | \xi^n - 1 \text{ if and only if } \phi(p^l) | n.$$

This is an easy consequence of Euler's Theorem: $(\xi, p) = 1$ implies that $\xi^{\phi(p^l)} \equiv 1 (\bmod \ p^l)$. So,

$$\frac{1}{n} \log |Fix_n(\theta)| = \frac{1}{n} \log |\xi^n - 1|_\infty - \frac{1}{n} \sum_{p \in S : p^{l-1}(p-1)|n, p^l(p-1) \nmid n} l \log p.$$

For terms with $l \geq 2$, $p^{l-1}|n$ whence

$$\sum_{p \in S : p^{l-1}|n} (l-1) \log p \leq \log n.$$

So for $l \geq 2$,

$$\frac{1}{n} \sum_{p \in S : p^{l-1} | n} l \log p \leq \frac{2}{n} \sum_{p \in S : p^{l-1} | n} (l-1) \log p \leq \frac{2}{n} \log n. \tag{34}$$

For the case $l = 1$ we need an estimate for $\sum_{p \in S : p-1|n} \log p$. This is achieved as follows: if $p - 1|n$ then $p \leq n + 1$ and $\log p = O(\log n)$. The number of possible p is at most $d(n)$ (the number of divisors of n), and following from standard results in number theory $d(n) = O(n^c)$ for any $c > 0$. Thus, choosing $0 < c < 1$,

$$\frac{1}{n} \sum_{p \in S : p-1 | n} \log p = O(n^{c-1} \log n). \tag{35}$$

From (34) and (35) we deduce that

$$\lim_{n \to \infty} \frac{1}{n} \log |Fix_n(\theta)| = \log |\xi|,$$

and so (33) is established.

□

Note that for both of these Artin systems, the conjectures imply that the periodic points are uniformly distributed.

6.3 The Periodic Points Realisation Problem

In this section we begin to seek answers to the following problem: given periodic point data, that is a sequence $\{a_n\}_{n=1}^{\infty}$ of natural numbers, can we reconstruct a suitable S–integer dynamical system $(\hat{R}_S, \theta)$ with that periodic point data ? An initial observation is that the sequence $\{a_n\}$ must be a *divisibility sequence*; if $m|n$ then $a_m|a_n$. A tractable starting point to the problem is to answer the following question: given $m \geq 0$ and a prime p, can we construct a map, multiplication by ξ, and a set S of non–archimedean places whose corresponding dynamical system has periodic points of the shape,

$$1, 1, \ldots, 1, p, 1, 1, \ldots, 1, p, \ldots$$

where the 1's occur in blocks of m each time ? By taking products of these 'building block' systems we can tackle the much harder general problem. As a prelude to Theorem 6.6 we recall some facts about Wieferich primes.

A prime p is called a *Wieferich prime* if it satisfies the congruence

$$2^{p-1} \equiv 1 (\text{mod } p^2). \tag{36}$$

In his 1909 paper [61], Wieferich proved the following theorem: suppose there exist integers x, y, z, not multiples of an odd prime p, such that $x^p + y^p + z^p = 0$ (we say that the *first* case of Fermat's last theorem fails for p), then p satisfies (36). The Wieferich congruence is satisfied very rarely, in fact the only known solutions less than 6×10^9 are 1093 and 3511. See [39] for a discussion on the history of (36). More generally, if $a \geq 2$ and p is a prime not dividing a, then

$$q_p(a) = \frac{a^{p-1} - 1}{p}$$

is called the *Fermat quotient* of p with base a. Thus

$$q_p(a) \equiv 0 (\text{mod } p) \text{ if and only if } a^{p-1} \equiv 1 (\text{mod } p^2).$$

Chapter 6 of [40] gives a heuristic reason to expect that there exist infinitely many primes p such that $q_p(a) \equiv 0 (\text{mod } p)$; it would follow that the number of Wieferich primes is infinite. Such primes should be extremely sparse.

Theorem 6.6 *Suppose that a prime p and an integer $m > 0$ satisfies $p - 1 = md$. Choose ξ a primitive root modulo p. If $q_p(\xi) \not\equiv 0 (\text{mod } p)$ then there exists a dynamical system $(\hat{R}_S, \theta)$ whose periodic point data has the shape,*

$$1, 1, \ldots, 1, p, 1, 1, \ldots, 1, p^{ord_p(2)+1}, \ldots, 1, 1, \ldots, 1, p^{ord_p(r)+1}, \ldots$$

where the 1's occur in blocks of $m - 1$ each time.

Proof. Let $k = \mathbf{Q}$ and S comprise all non–archimedean places except $|.|_p$. Define θ as the endomorphism of $\hat{R}_S$ dual to multiplication by ξ^d on R_S. The number of periodic points is given by

$$|Fix_n(\theta)| = |\xi^{dn} - 1|_p^{-1} \text{ for all } n \geq 1.$$

Since ξ is a primitive root modulo p, $|Fix_n(\theta)| = 1$ if and only if $p-1 \not| dn$, and this occurs if and only if $m \not| n$. So clearly the 1's are correctly positioned. Finally, the congruence condition gives $|Fix_n(\theta)| = |\xi^{r(p-1)} - 1|_p^{-1} = p^{ord_p(r)+1}$ if and only if $n = mr$.

□

Corollary 6.2 *The zeta function ζ_θ is irrational.*

Proof. Inspecting the periodic point data, we see that $|Fix_n(\theta)|$ has an infinite number of values that it takes on infinitely often, namely $\{1, p, p^2, \ldots\}$. By Proposition 4.1, $|Fix_n(\theta)|$ cannot be a recurrence sequence and so does not represent a rational function. Hence the result.

□

Example 6.9 The periodic point data

$$1,3,1,3,1,3^2,1,3,1,3,1,3^2,1,3,1,3,1,3^3,1,3,1,3,1,3^2,1,3,1,3,\ldots,1,3^{ord_3(r)+1},\ldots$$

where $n = 2r$, comes from the system $(\hat{R}_{S_1}, \theta_1)$, where S_1 comprise all finite places except $|.|_3$ and θ_1 is dual to multiplication by 2. The data

$$1,1,1,5,1,1,1,5,1,1,1,5,1,1,1,5,1,1,1,5^2,1,1,1,5,1,1,1,5,\ldots,1,1,1,5^{ord_5(r)+1},\ldots$$

where $n = 4r$, comes from the system $(\hat{R}_{S_2}, \theta_2)$, where S_2 comprise all finite places except $|.|_5$ and θ_2 is dual to multiplication by 3.

Hence the product dynamical system $(\hat{R}_{S_1}, \theta_1) \times (\hat{R}_{S_2}, \theta_2)$ has periodic point data

$$1,3,1,15,1,9,1,15,1,3,1,45,1,3,1,15,1,27,1,75,1,3,1,45,1,3,1,15,\ldots$$

Example 6.10 Let α be an algebraic number of degree d and let $\alpha_1, \ldots, \alpha_d$ denote its conjugates. Suppose we are given periodic point data determined by the recurrence sequence $\prod_{i=1}^{d}({\alpha_i}^n - 1)$, that is,

$$|Fix_n(\theta)| = \left|\prod_{i=1}^{d}({\alpha_i}^n - 1)\right| \text{ for all } n \geq 1.$$

Then the dynamical system $(\mathbf{T}^n, \theta)$, where θ is dual to the companion matrix of the minimum polynomial of α, recovers the given periodic point data. The system $(\mathbf{T}^n, \theta)$ is isomorphic to the S–integer system $(\hat{O}_k, \widehat{\times\alpha})$ where $k = \mathbf{Q}(\alpha)$ and $S = \emptyset$.

Problem 6.1 The archetypal example of a recurrence sequence is of course the celebrated Fibonacci sequence $\{f_n\}$ defined by

$$f_{n+2} = f_{n+1} + f_n \text{ for } n = 0, 1, 2, \dots \text{ with } f_0 = 0, f_1 = 1;$$

and generated by

$$\frac{z}{1 - z - z^2} = \sum_{n=1}^{\infty} f_n z^n.$$

This sequence satisfies the divisibility property, so a natural question is whether we can construct an S–integer dynamical system which has Fibonacci periodic point data. A first step to a solution might be the observation that ζ_θ is irrational and is given by

$$\zeta_\theta(z) = \exp\{\frac{1}{\sqrt{5}} \log\left(\frac{1-\beta_2 z}{1-\beta_1 z}\right)\},$$

where $\beta_1 = (1+\sqrt{5})/2$ and $\beta_2 = (1-\sqrt{5})/2$.

As a motivation to resolving Problem 6.1, we give an alternative criteria for classifying expansive arithmetic S–integer systems in terms of the periodic point data, rather than the action.

Theorem 6.7 *Let $(\hat{R}_S, \theta)$ be an arithmetic S–integer dynamical system. If $(\hat{R}_S, \theta)$ is expansive then $\lim_{n\to\infty} |Fix_n(\theta)/Fix_{n+1}(\theta)|$ exists. The converse holds if S is finite.*

Proof. Suppose $(\hat{R}_S, \theta)$ is expansive, then by Theorem 3.4 and the estimates in Lemma 4.1 and (17) we have,

$$\lim_{n\to\infty} \left|\frac{Fix_n(\theta)}{Fix_{n+1}(\theta)}\right| = \lim_{n\to\infty} \prod_{\nu\in S\cup P_\infty} \left|\frac{\xi^n - 1}{\xi^{n+1} - 1}\right|_\nu = \exp\{-h(\theta)\}.$$

For a partial converse, we assume S to be finite and prove that non–expansiveness implies that $|Fix_n(\theta)/Fix_{n+1}(\theta)|$ can be made arbitrarily large as well as small, for suitably chosen infinite sequences. Since

$$\widehat{Fix_n}(\theta) \cong R_S/(\xi^n - 1)R_S,$$

it is clear that in non–ergodic systems there exist sequences along which $|Fix_n(\theta)/Fix_{n+1}(\theta)|$ fails to converge. So we might as well assume ergodicity. We shall treat the archimedean and non–archimedean cases separately before determining their combined influence.

Firstly, suppose all the non–expansive behaviour is archimedean in nature. So the ratio $|Fix_n(\theta)/Fix_{n+1}(\theta)|$ contains a factor of the form,

$$\prod_{j=1}^{m}\left|\frac{\xi_j^n-1}{\xi_j^{n+1}-1}\right|,$$

where $\xi_1,\ldots,\xi_m$ are the conjugates of ξ which are not unit roots but are on the unit circle. For each j, write $\xi_j=e^{i\rho_j}$ where $\rho_j\in(0,2\pi)$ is irrational. Then by Dirichlet's Theorem on simultaneous approximation (see for instance [46]), there exist infinitely many integers $l_1,\ldots,l_m$ and infinitely many $n\in\mathbf{N}$ with

$$|n\rho_j+2\pi l_j|\ll\frac{1}{n^{1/m}}\text{ for }j=1,\ldots,m.$$

Hence, denoting the set of all such n by A, we have,

$$|\xi_j^n-1|=|e^{i(n\rho_j+2\pi l_j)}-1|\ll\frac{1}{n^{1/m}}\text{ for }j=1,\ldots,m\text{ and for all }n\in A.$$

Also observe that for any $1\leq j\leq m$ and $n\in A$,

$$|\xi_j^{n+1}-1|=|\xi_j^n-1+1-\xi_j^{-1}|\gg\left|\frac{1}{n^{1/m}}-|\xi_j-1|\right|\geq|1-|\xi_j-1||\geq 1,$$

and similarly $|\xi_j^{n-1}-1|\gg 1$. Thus for all $n\in A$ we have,

$$\left|\frac{\xi_j^n-1}{\xi_j^{n+1}-1}\right|\ll\frac{1}{n^{1/m}}$$

and

$$n^{1/m}\ll\left|\frac{\xi_j^{n-1}-1}{\xi_j^n-1}\right|,$$

which implies that

$$\prod_{j=1}^{m}\left|\frac{\xi_j^n-1}{\xi_j^{n+1}-1}\right|$$

is either arbitrarily small or arbitrarily large depending on whether n tends to infinity through A or $A-1=\{n-1:n\in A\}$.

Now consider the case when the non–expansive behaviour is solely non–archimedean. So the ratio $|Fixn(\theta)/Fix_{n+1}(\theta)|$ contains a factor of the form,

$$\prod_{j=1}^{m}\left|\frac{\xi^n-1}{\xi^{n+1}-1}\right|_{\nu_j},$$

where $\nu_j|p_j$ and $|\xi|_{\nu_j}=1$. As in (23), the ν_j–adic expansion of ξ has a non–zero constant term, so there exist positive integers $d_1,\dots,d_m$ such that $|\xi^n-1|_{\nu_j}=1$ if and only if $d_j\not|n$. Define an infinite subset $B\subset\mathbf{N}$ by

$$B=\{d_1\cdots d_m(p_1\cdots p_m)^r : r\in\mathbf{N}\}.$$

Then for each $j=1,\dots,m$ and $n\in B$ we have,

$$|\xi^n-1|_{\nu_j}\le|n|_{p_j}=\frac{1}{p_j^r}\text{ for all } r\in\mathbf{N}\text{ and } |\xi^{n+1}-1|_{\nu_j}=|\xi^{n-1}-1|_{\nu_j}=1.$$

Hence for all $r\in\mathbf{N}$

$$\prod_{j=1}^{m}\left|\frac{\xi^n-1}{\xi^{n+1}-1}\right|_{\nu_j}\le\prod_{j=1}^{m}|n|_{p_j}=\frac{1}{(p_1\cdots p_m)^r}$$

and

$$(p_1\cdots p_m)^r\le\prod_{j=1}^{m}\left|\frac{\xi^{n-1}-1}{\xi^n-1}\right|_{\nu_j}.$$

So once again $|Fix_n(\theta)/Fix_{n+1}(\theta)|$ fails to converge.

Finally, suppose non–expansiveness is a hybrid of archimedean and non–archimedean contributions. Then the ratio $|Fix_n(\theta)/Fix_{n+1}(\theta)|$ contains a factor of the form,

$$\prod_{j=1}^{m_1}\left|\frac{\xi_j^n-1}{\xi_j^{n+1}-1}\right|\prod_{j=1}^{m_2}\left|\frac{\xi^n-1}{\xi^{n+1}-1}\right|_{\nu_j},$$

where $\xi_1,\dots,\xi_{m_1}$ are those conjugates of ξ which are not unit roots but are on the unit circle and $|\xi|_{\nu_j}=1$ for $j=1,\dots,m_2$. This time we can afford to be more generous with the definition of $B\subset\mathbf{N}$, let

$$B=\{rd_1\cdots d_{m_2} : r\in\mathbf{N}\},$$

where the d_j's are those positive integers for which $|\xi^n-1|_{\nu_j}=1$ if and only if $d_j\not|n$.

Since $n'\rho_j$ is irrational for each $j = 1, \ldots, m_1$ and for all $n' \in B$, applying Dirichlet's Theorem again, there exist infinitely many integers $l_1, \ldots, l_{m_1}$ and infinitely many $n \in \mathbf{N}$ with

$$|nn'\rho_j + 2\pi l_j| \ll \frac{1}{n^{1/m_1}} \text{ for } j = 1, \ldots, m_1.$$

Hence, denoting the set of all such n by A and defining an infinite subset $E \subset \mathbf{N}$ by

$$E = \{n_1 n_2 : n_1 \in A, n_2 \in B\},$$

we have,

$$|\xi_j^n - 1| = |e^{i(n_1 n_2 \rho_j + 2\pi l_j)} - 1| \ll \frac{1}{n^{1/m_1}} \text{ for } j = 1, \ldots, m_1 \text{ and for all } n \in E.$$

As before, both $|\xi_j^{n+1} - 1|$ and $|\xi_j^{n-1} - 1|$ are bounded below by some positive constant, for $j = 1, \ldots, m_1$ and for all $n \in E$. Thus for all $n \in E$,

$$\prod_{j=1}^{m_1} \left| \frac{\xi_j^n - 1}{\xi_j^{n+1} - 1} \right| \prod_{j=1}^{m_2} \left| \frac{\xi_j^n - 1}{\xi_j^{n+1} - 1} \right| \ll \frac{1}{n}$$

and

$$n \ll \prod_{j=1}^{m_1} \left| \frac{\xi_j^{n-1} - 1}{\xi_j^n - 1} \right| \prod_{j=1}^{m_2} \left| \frac{\xi_j^{n-1} - 1}{\xi_j^n - 1} \right|.$$

Hence $\lim_{n\to\infty} |Fix_n(\theta)/Fix_{n+1}(\theta)|$ does not exist.

□

Let S be degenerate, that is, comprise all but a finite set F of non–archimedean places of k. Then

$$\left| \frac{Fix_n(\theta)}{Fix_{n+1}(\theta)} \right| = \prod_{\nu \in F} \left| \frac{\xi^{n+1} - 1}{\xi^n - 1} \right|_\nu,$$

where $|\xi|_\nu| \le 1$ for all $\nu \in F$. If $|\xi|_\nu = 1$ for some $\nu \in F$ then, by Theorem 6.7, $|Fix_n(\theta)/Fix_{n+1}(\theta)|$ does not converge. The other possibility is that $|\xi|_\nu < 1$ for all $\nu \in F$, in which case $|Fix_n(\theta)| = 1$ for all $n \ge 1$ and trivially $|Fix_n(\theta)/Fix_{n+1}(\theta)| = 1$.

Conjecture 6.2 *Let $(\hat{R}_S, \theta)$ be an arithmetic S–integer dynamical system. If S is infinite and non–degenerate, then $|Fix_n(\theta)/Fix_{n+1}(\theta)|$ does not converge.*

Returning to Problem 6.1, suppose, if possible, that $\{f_n\}$ arises as periodic point data in an arithmetic S–integer system $(\hat{R}_S, \theta)$. Then θ must be non–expansive because ζ_θ is irrational. Furthermore, the existence of the limit

$$\lim_{n\to\infty} \left| \frac{f_n}{f_{n+1}} \right| = \frac{1}{\beta_1} = \frac{\sqrt{5}-1}{2}, \tag{37}$$

means that S cannot be finite. Clearly S must be non–degenerate and, if Conjecture 6.2 holds, (37) is contradicted.

Chapter 7

Mahler Measure and Entropy

7.1 Historical Background

Let $F(x) \in \mathbf{Z}[x]$ denote a non–zero polynomial with rational integer coefficients. There are several ways to measure the height of $F(x)$. The definition proposed by Mahler in [30] has proved to be important,

$$m(F) = \int_0^1 \log |F(e^{2\pi i\theta})| d\theta. \tag{38}$$

We shall denote the exponential version of this definition by $M(F)$. Suppose $F(x)$ has the factorisation

$$F(x) = a \prod_i (x - \alpha_i), \quad a \in \mathbf{Z}, \quad \alpha_i \in \mathbf{C}. \tag{39}$$

Then an alternative form for (38) is

$$m(F) = \log |a| + \sum_i \log^+ |\alpha_i|. \tag{40}$$

The proof of this is an immediate application of Jensen's formula

$$\int_0^1 \log |e^{2\pi i\theta} - \alpha| = \log^+ |\alpha|. \tag{41}$$

So $m(F)$ is the non–negative logarithm of an algebraic number. Given the nature of the logarithm, we might as well assume that F is irreducible and that $F(0) \neq 0$.

In 1857, Kronecker [23] proved the following result.

Theorem 7.1 *If $\theta_1, \ldots, \theta_n$ are the roots of the polynomial $P(x) = x^n + c_1 x^{n-1} + \cdots + c_n$, where $c_1, \ldots, c_n$ are integers with $P(0) \neq 0$, and if all the roots lie inside the unit disk, then they must all be roots of unity.*

Corollary 7.1 *If $\alpha_{\mathcal{R}_1/<f>}$ is a $\mathbf{Z}$–action of a compact abelian group X_M, then $h(\alpha_{\mathcal{R}_1/<f>}) = 0$ if and only if f is cyclotomic.*

The proof of Theorem 7.1 is very slick: consider the polynomials $P_m(x)$ whose roots are $\theta_1^m, \ldots, \theta_n^m$ for $m = 1, 2, \ldots$. The condition on the size of the roots and the fact that the c_i are integers implies that there can only be a finite number of different P_m. Thus two distinct powers of each root must coincide and this means that each root is a root of unity.

This classical theorem makes it obvious that $m(F) = 0$ if and only if F is a cyclotomic (literally 'circle dividing') polynomial. Many results exist concerning the values of this measure and there are some fascinating conjectures. For example, Lehmer's question [25] asks how small $M(F)$ can be if F is not cyclotomic. Specifically, he asks whether, given $\epsilon > 0$, there exist polynomials F with integer coefficients such that $1 < M(F) < 1 + \epsilon$? To this day, no smaller positive measure has been found than Lehmer's example:

$$M(F) = \sigma_1 = 1.1762808\ldots \tag{42}$$

where $F(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$. In 1962 Mahler [31] extended his measure, in the obvious way, to polynomials $F(x_1, \ldots, x_n)$ in n variables with integer coefficients,

$$M(F) = \exp\left\{\int_0^1 \cdots \int_0^1 \log|F(e^{2\pi i\theta_1}, \ldots, e^{2\pi i\theta_n})| d\theta_1 \ldots \theta_n\right\} \tag{43}$$

Smyth has proved in [50] that $M(F) = 1$ if and only if F is a generalised cyclotomic polynomial. (Basically, this means that F is a cyclotomic polynomial evaluated on a monomial.) His method was to associate to F a convex hull (or exponent polytope of F) $\mathcal{C}(F)$ in $\mathbf{R}^n$, and to show how the faces of $\mathcal{C}(\mathcal{F})$ correspond to factors of F. This feature is the basis for an inductive argument. He has also obtained some exotic formulae for non–zero values of $M(F)$ (see [51]), for example,

$$M(1 + x_1 + x_2) = \exp\left\{\frac{3\sqrt{3}}{4\pi} L(2, \chi_3)\right\} = 1.38135\ldots, \tag{44}$$

$$M(1+x_1+x_2+x_3) = \exp\left\{\frac{7}{2\pi^2}\zeta(3)\right\} = 1.53154\ldots \tag{45}$$

Here $L(2,\chi_3)$ denotes the Dirichlet L–function with quadratic character mod3, that is,

$$L(2,\chi_3) = \sum_{n=1}^{\infty}\left(\frac{n}{3}\right)\frac{1}{n^2}$$

where $\left(\frac{n}{3}\right)$ denotes the Legendre symbol mod3. Also, ζ denotes the Riemann zeta function. The proofs basically use an extended version of Jensen's formula. Using the same technique Boyd [6] proved that

$$\lim_{n\to\infty} M(F(x,x^n)) = M(F(x_1,x_2)) \tag{46}$$

leading him on to make conjectures concerning the closure of the set $L = \{M(F) : F \text{ has integer coefficients}\}$ in the several variable case. For example, he considers a certain class of algebraic integers $S \subset L$ called the set of Pisot–Vijayaraghavan numbers, whose elements comprise the set $\theta > 1$ such that θ is a root of a monic irreducible polynomial with integer coefficients all of whose remaining roots lie in the unit disk $|z| < 1$. Such a polynomial must be *non–reciprocal* (bar a few easily handled exceptions). The *reciprocal* of a polynomial $F(x)$ of degree d is defined as $F^*(x) = x^d F(x^{-1})$. In order to appreciate the rich structure of S, consult Salem [42], [43] and Siegel [48]. Smyth has shown in [52] that if we define

$$L_0 = \{M(F) : F \text{ is non–reciprocal}\} \subset L$$

then

$$\inf L_0 = \min L_0 = \theta_0 = \min S = \inf S, \tag{47}$$

where $\theta_0 = 1.32471\ldots$ is the real zero of $x^3 - x - 1$, thus answering Lehmer's question for the class L_0. The set of Salem numbers $T \subset L$ is another set of algebraic integers consisting of all $\theta > 1$ such that θ is a root of a monic irreducible polynomial $P(x)$ with integer coefficients all of whose other roots lie in $|z| \leq 1$ with at least one on $|z| = 1$. This last condition forces $P(x)$ to be reciprocal. Boyd conjectures that

$$\min L = \sigma_1 = \min T. \tag{48}$$

The recent work of Everest [10] may also give insight into the closure of L. He proves that it is possible to realise $M(F)$, where $F(x_1,\dots,x_n)\in \mathbf{Z}[x_1,\dots,x_n]$, as an effective limit of Riemann sums. His technique is to parametrise the n–torus via algebraic numbers $\theta_i,\psi_i,\ 1\le i\le n$ chosen in such a way that $\{1,\theta_i,\psi_i\}$ are multiplicatively independent for each $1\le i\le n$ and involves an application of Baker's theorem on linear forms in logarithms of algebraic numbers.

Another candidate for the measure of polynomials in several variables has been propounded by Myerson in [34]. Taking (40) as a starting point, rather than (38), his measure for $F(x_1,\dots,x_n)\in \mathbf{Z}[x_1,\dots,x_n]$ is

$$\Omega(F)=\exp\left\{\int_{\mathbf{S}}\log|F|d\sigma\right\} \tag{49}$$

where σ is normalised Haar measure on the unit sphere $\mathbf{S}$ in $\mathbf{C}^n$. Note that $\Omega(F)=M(F)$ in the one variable case. In short, where $M(F)$ is the geometric mean of F on the torus, $\Omega(F)$ is the geometric mean of F on the sphere. Once again, calculations and conjectures abound, and there is even a Kronecker–inspired theorem.

7.2 The Mahler Measure Associated to an A–Field

In this section we construct a geometric analogue of the classical Mahler measure. The techniques applied were first introduced in constructing the elliptic Mahler measure in [12] and [11].

Suppose $F(x)$ is a non–zero irreducible polynomial with integral coefficients such that $F(0)\ne 0$, and let $F(x)$ have the factorisation as in (39). We first establish a third definition of $m(F)$ equivalent to (38) and (40), which shows that $m(F)$ is locally the sum of an archimedean component and p–adic components for each rational prime p. The key step will be to prove a p–adic analogue of Jensen's formula (41). We shall call these components *local measures* and define them as Shnirelman integrals. This corrects an error in [12] where the Haar integral was used to define the local measure.

Let K be a splitting field for F and let ν denote any valuation of K which lies above the valuation p of $\mathbf{Q}$. The field $\mathbf{\Omega}_\nu$ is defined as the smallest field extension of

$\mathbf{Q}$ which is both complete and algebraically closed with respect to $|.|_\nu$. For example, if $\nu|\infty$ then $\mathbf{\Omega}_\nu = \mathbf{C}$, the field of complex numbers. For each i we define the following local measures,

$$m_\nu(\alpha_i) = \lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} \log|\zeta^j - \alpha_i|_\nu, \tag{50}$$

where ζ is a primitive n-th root of unity inside $\mathbf{\Omega}_\nu$.

This definition of the local measure is a slight specialisation of the *Shnirelman integral*, introduced in 1938 [47] as a p–adic analogue of the line integral (in general, for the case $\nu|p$, the condition $p \not| n$ has to be imposed to guarantee convergence; because we are dealing with a special class of functions this is not needed here). See [22] for further applications.

If $\nu|\infty$ then it follows, after applying Baker's result (Lemma 4.1), that

$$m_\nu(\alpha_i) = \log^+|\alpha_i|_\nu. \tag{51}$$

By the estimate in (17), the same is clearly true if ν is non–archimedean. We reckon (51) to be the ν–adic analogue of Jensen's formula. This simple fact allows the $\log|a|$ term in (40) to be recognisable as a sum over non–archimedean contributions (see Lemma 7.1). So the third representation of $m(F)$ is

$$m(F) = \sum_i \sum_\nu d_\nu m_\nu(\alpha_i), \tag{52}$$

where $d_\nu = [K_\nu : \mathbf{Q}_p]$ are the local degrees making the product formula work. This local–to–global treatment of $m(F)$ is analogous to the local–to–global treatment of the topological entropy of a solenoidal endomorphism [28], the local entropies being precisely local Mahler measures. So the ν–adic decomposition of $h(\theta; \hat{R}_S)$ for the geometric dynamical system $(\hat{R}_S, \theta)$ (see Theorem 2.1) is highly suggestive of a local–to–global geometric Mahler measure theory.

We now extend from this arithmetic setting to $\mathbf{A}$–fields. Let k denote either $\mathbf{Q}$ or $\mathbf{F}_p(T)$ and let O_k denote the ring of algebraic integers in k. Choose $F(x) \in O_k[x]$ to be a non–zero irreducible element with $F(0) \neq 0$. Suppose F splits in some finite extension $k \subset K$ of degree d and has the factorisation

$$F(x) = a\prod_i (x - \alpha_i), \quad a \in O_k, \quad \alpha_i \in K. \tag{53}$$

Let ν denote any valuation of K extending the valuation ω of k. In the geometric case, it will be once again conventional to denote the distinguished place corresponding to the polynomial T^{-1} by ∞. Define, as in (50) and (52),

$$m_\nu(\alpha_i) = \lim_{n\to\infty}{}' \frac{1}{n}\sum_{j=1}^{n} \log|\zeta^j - \alpha_i|_\nu = \log^+ |\alpha_i|_\nu, \tag{54}$$

where ζ is a primitive n-th root of unity inside $\mathbf{\Omega}_\nu$, and

$$m_{\mathbf{A}}(F) = \sum_i \sum_\nu d_\nu m_\nu(\alpha_i), \tag{55}$$

where $d_\nu = [K_\nu : k_\omega]$. The notation $\lim'$ in (54) indicates no restriction on n in the arithmetic case, but in the geometric case we need to use an analogue of the classical Shnirelman integral by imposing the condition $M_\nu \not| n$ for some number $M_\nu \neq 1$ dependent on ν. The number M_ν can be computed from the proof of Theorem 4.4.

Lemma 7.1

$$m_{\mathbf{A}}(F) = \log|a|_\infty + \sum_i \sum_{\nu|\infty} d_\nu m_\nu(\alpha_i).$$

Proof. The method employed is as in Section 6 of [28]. Write $\prod_i(x - \alpha_i) = x^d + b_1x^{d-1} + \cdots + b_d$ where $b_1, \ldots, b_d \in k$ and the lowest common multiple of these coefficients is a. Then for any place of k with $\omega \neq \infty$,

$$|a|_\omega = \min\{|b_1|_\omega^{-1}, \ldots, |b_d|_\omega^{-1}, 1\}.$$

Suppose the roots $\alpha_1, \ldots, \alpha_d$ lie in a finite extension $k_\omega \subset K_\nu$ of degree d_ν, and order them so

$$|\alpha_1|_\nu \geq |\alpha_2|_\nu \geq \cdots \geq |\alpha_m|_\nu > 1 \geq |\alpha_{m+1}|_\nu \geq \cdots \geq |\alpha_d|_\nu.$$

We will prove that

$$\log|a|_\omega^{-1} = \sum_i d_\nu m_\nu(\alpha_i),$$

then it follows that $\log|a|_\infty$ is just the sum over the non–archimedean contributions in (55).

If $|\alpha_i|_\nu \leq 1$ for all i, then $|a|_\omega = 1$ and $\sum_i d_\nu m_\nu(\alpha_i) = 0$. Thus we may assume that $|\alpha_1|_\nu > 1$. Then we have

$$\begin{aligned} |b_m|_\omega &= \left| \sum_{i_1 < \cdots < i_m} \alpha_{i_1} \cdots \alpha_{i_m} \right|_\nu \\ &= |\alpha_1 \cdots \alpha_m + \text{smaller terms}|_\nu \\ &= |\alpha_1 \cdots \alpha_m|_\nu, \end{aligned}$$

and by a similar calculation $|b_i|_\omega \leq |b_m|_\omega$ for all $i = 1, \ldots, d$. So

$$|a|_\omega = \min\{|b_1|_\omega^{-1}, \ldots, |b_d|_\omega^{-1}\} = \prod_{|\alpha_i|_\nu > 1} |\alpha_i|_\nu^{-1}$$

and

$$\log |a|_\omega^{-1} = \sum_{|\alpha_i|_\nu > 1} \log |\alpha_i|_\nu = \sum_i d_\nu m_\nu(\alpha_i),$$

completes the proof.

□

We now feel justified in proclaiming $m_{\mathbf{A}}(F)$ to be the Mahler measure of F associated to an $\mathbf{A}$–field. Note the exact analogy between (51) and (54), also between (52) and (55). Using Lemma 7.1 we can rewrite the definition of $m_{\mathbf{A}}(F)$ as

$$m_{\mathbf{A}}(F) = \frac{1}{d} \sum_{\nu | \infty} \lim_{n \to \infty}{}' \frac{1}{n} \sum_{j=1}^{n} \log |F(\zeta^j)|_\nu. \tag{56}$$

So if $k = \mathbf{Q}$, $F(x)$ has integer coefficients and (56) collapses to the arithmetic Mahler measure (38).

Theorem 7.2 *The generalised Mahler measure $m_{\mathbf{A}}(F) = 0$ if and only if F is a division polynomial. That is, the arithmetic measure vanishes if and only if F is cyclotomic, and its geometric counterpart vanishes if and only if both the leading coefficient of F and its roots lie in $\mathbf{F}_p^*$.*

Proof. We have already seen that the arithmetic case follows from Kronecker's result Theorem 7.1, and, using exactly the same argument in the geometric case, we must have $\alpha_i \in \mathbf{F}_p^*$ for each i and $a \in \mathbf{F}_p^*$.

□

Notice how $\mathbf{F}_p^*$ plays the role of the roots of unity, as in Theorem 3.2. The term *division polynomial* was first used in [12], where it was proved that the elliptic Mahler measure vanishes if and only if the roots of $F(x)$ (an integral polynomial) are the x–coordinates of torsion points of the underlying elliptic curve. The results in this section allow us to make the following connection between topological entropy and Mahler measure.

Theorem 7.3 *Let $(\hat{R}_S, \theta)$ be an S–integer dynamical system and let $F(x)$ be the polynomial with coefficients in $\mathbf{Z}$ or $\mathbf{F}_p[T]$, obtained by multiplying the minimum polynomial of ξ by the lowest common multiple of the denominators of its coefficients. Then*

(i) $h(\theta; \hat{R}_S) = m_{\mathbf{A}}(F)$,

(ii) $h(\tilde{\theta}; k_\nu) = m_\nu(\xi)$ *for each place* ν *of* k,

(iii) $h(\theta; \hat{R}_S) = 0$ *if and only if* F *is a division polynomial.*

The problem of realising the elliptic Mahler measure as an entropy is being tackled by Everest and Ward.

Bibliography

[1] L. M. Abromov, *The entropy of an automorphism of a solenoidal group*, Teor. Verojatnost. i Primenen. **4** (1959), 249-254 (Russian). Eng. tranl. *Theory of Prob. and Applic.* **IV** (1959), 231-236.

[2] R. L. Adler, A. G. Konheim and M. H. McAndrew, *Topological entropy*, Trans. Amer. Math. Soc. **114** (1965), 309-319.

[3] E. Artin, *The collected papers of Emil Artin*, Reading, Massachusetts, Addison–Wesley (1965).

[4] A. Baker (editor), *New Advances in Transcendence Theory*, Cambridge University Press (1988).

[5] R. Bowen, *Entropy for group endomorphisms and homogeneous spaces*, Trans. Amer. Math. Soc. **153** (1971), 401-414. Erratum, **181** (1973), 509-510.

[6] D. W. Boyd, *Speculations concerning the range of Mahler's measure*, Canad. Math. Bull. **24** (4) (1981).

[7] D. R. Heath–Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. **37** (2) (1986), 27-38.

[8] H. Cartan, *Sur la mesure de Haar*, C. R. Acad. Sci. **211** (1940), 759-762.

[9] M. Eisenberg, *Expansive automorphisms of finite–dimensional vector spaces*, Fund. Math. **LIX** (1966), 307-312.

[10] G. R. Everest, *Effective calculation of Mahler's Measure*, preprint, University of East Anglia.

[11] G. R. Everest, *On the elliptic analogue of Jensen's formula*, preprint, University of East Anglia.

[12] G. R. Everest, Bríd Ní Fhlathúin, *The elliptic Mahler measure*, Math. Proc. Camb. Phil. Soc. **120** (1996), 13-25.

[13] A. O. Gelfond, *Transcendental and Algebraic Numbers*, New York, Dover (1960).

[14] A. Haar, *Der massbegriff in der theorie der kontinuierlichen gruppen*, Ann. of Math. **34** (1933), 147-169.

[15] P. R. Halmos, *On automorphisms of compact groups*, Bull. Amer. Math. Soc. **49** (1943), 619-624.

[16] E. Hewitt, K. A. Ross, *Abstract Harmonic Analysis I*, Springer–Verlag (1963).

[17] C. Hooley, *On Artin's conjecture*, J. für Reine und Angew. Math. **225** (1967), 209-220.

[18] H. B. Keynes, J. B. Robertson, *Generators for topological entropy and expansiveness*, J. Math. Sys. Th. **3** (1969), 51-59.

[19] B. P. Kitchens, *Expansive dynamics on zero–dimensional groups*, Ergod. Th. & Dynam. Sys. **7** (1987), 249-261.

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

[21] N. Koblitz, *p–adic Numbers, p-adic Analysis, and Zeta Functions*, Springer: New York (1977).

[22] N. Koblitz, *p–adic Analysis: a Short Course on Recent Work*, London Math. Soc. Lecture Series No. 46.

[23] L. Kronecker, *Zwei sätze über gleichungen mit Ganzzahligen coefficienten*, J. für Reine und Angew. Math. **53** (1857), 173-175.

[24] W. Lawton, *The structure of compact connected groups which admit an expansive automorphism*, Recent advances in Topological Dynamics, Lecture Notes in Mathematics. Springer: Berlin–Heidelberg–New York (1973), 182-196.

[25] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. **34** (2) (1933), 461-479.

[26] D. A. Lind, *Dynamical properties of quasihyperbolic toral automorphisms*, Ergod. Th. & Dynam. Sys. **2** (1982), 49-68.

[27] D. A. Lind, *Ergodic group automorphisms and specification*, Lecture Notes in Math. **729** (1978), 93-103.

[28] D. A. Lind, T.Ward, *Automorphisms of solenoids and p-adic entropy*, Ergod. Th. & Dynam. Sys. **8** (1988), 411-419.

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

[30] K. Mahler, *An application of Jensen's formula to polynomials*, Mathematika **7** (1960), 98-100.

[31] K. Mahler, *On some inequalities for polynomials in several variables*, Journal London Math. Soc. **37** (1962), 341-344.

[32] R. Mañé, *Ergodic Theory and Differentiable Dynamics*, Springer–Verlag (1987).

[33] S. A. Morris, *Pontryagin Duality and the Structure of Locally Compact Abelian Groups*, London Math. Soc. Lecture Note Series No. 29.

[34] G. Myerson, *A measure for polynomials in several variables*, Canad. Math. Bull. **27** (2) (1984), 185-191.

[35] G. Myerson, A. J. van der Poorten, *Some problems concerning recurrence sequences*, preprint, Macquarie University.

[36] K. R. Parthasarathy, *Introduction to Probability and Measure*, Macmillan, London (1977).

[37] A. J. van der Poorten, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sc. Paris **306**, Série 1 (1988), 97-102.

[38] A. J. van der Poorten, *Some facts that should be better known, especially about rational functions*, R. A. Mollin (ed.), Number Theory and Applications (1989), 497-528.

[39] P. Ribenboim, *'1093'*, Math. Intelligencer **5** (1983), 28-33.

[40] P. Ribenboim, *The Book of Prime Number Records*, Springer–Verlag, New York (1988).

[41] R. S. Rumely, *Notes on van der Poorten's proof of the Hadamard Quotient Theorem*, Sé. Théorie des Nombres de Paris 1986-87, Birkhäuser (1988).

[42] R. Salem, *A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan*, Duke Math. Jour. **11** (1944), 103-108.

[43] R. Salem, *Algebraic Numbers and Fourier Analysis*, D. C. Heath and Company, Boston (1963).

[44] K. Schmidt, *Automorphisms of compact abelian groups and algebraic varieties*, Proc. London Math. Soc. **61** (1990), 480-496.

[45] K. Schmidt, *Dynamical Systems of Algebraic Origin*, Birkhäuser–Verlag (1995).

[46] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Mathematics **785**, Springer–Verlag (1980).

[47] L. G. Shnirel'man, *O funkcijah v normirovannyh algebraičeski zamknutyh telah (On functions in normed algebraically closed division rings)*, Izvestija AN SSSR **2** (1938), 487-498.

[48] C. L. Siegel, *Algebraic integers whose conjugates lie in the unit circle*, Duke Math. Jour. **11** (1944), 597-602.

[49] S. Smale, *Differentiable dynamical systems*, Bull. Amer. Math. Soc. **73** (1967), 747-817.

[50] C. J. Smyth, *A Kronecker-type theorem for complex polynomials in several variables*, Canad. Math. Bull. **24** (4) (1981).

[51] C. J. Smyth, *On measures for polynomials in several variables*, Bull. Austral. Math. Soc. **23** (1981), 49-63.

[52] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London. Math. Soc. **3** (1971), 169-175.

[53] J. T. Tate, *Fourier Analysis on Number Fields and Hecke's Zeta–Function*, Princeton, May 1950.

[54] S. Waddington, *The prime orbit theorem for quasihyperbolic toral automorphisms*, Mh. Math. 112 (1991), 235-248.

[55] S. S. Wagstaff Jr., *Divisors of Mersenne numbers*, Math. Comp. **40** (1983), 385-397.

[56] P. Walters, *An Introduction to Ergodic Theory*, Springer: New York (1982).

[57] T. B. Ward, *Periodic points for expansive actions of* $\mathbf{Z}^d$ *on compact abelian groups* Bull. London Math. Soc. **24** (1992), 317-324.

[58] T. B. Ward, *The Entropy of Automorphisms of Solenoidal Groups*, MSc. Thesis (1986).

[59] A. Weil, *Basic Number Theory*, 3rd ed., Springer: New York (1974).

[60] A. Weil, *Sur les Espaces a Structure Uniforme et sur la Topologie Génerale* Hermann, Paris (1938).

[61] A. Wieferich, *Zum letzten Fermatschen Theorem*, J. für die reine und angewandte Math. **136** (1909), 293-302.

[62] R. F. Williams, *Classification of subshifts of finite type*, Annals of Math. **98** (1973), 120-153. Errata: **99** (1974), 380-381.

[63] S. A. Yuzvinskii, *Computing the entropy of a group endomorphism*, Sibirsk. Math. Ž. **8** (1967), 230-239 (Russian). Eng. transl. Siberian Math. J. **8** (1968), 172-178.

[64] R. J. Zimmer, *Ergodic Theory and Semisimple Groups*, Birkhaüser–Boston (1984).