5. More examples: toral endomorphisms

§5.1 Endomorphisms of a torus

Take $X = \mathbb{R}^k/\mathbb{Z}^k$ to be the k-torus.

Let $A = (a_{ij})$ be a $k \times k$ matrix with entries in $\mathbb{Z}$ and with $\det A \neq 0$. We can define a linear map $\mathbb{R}^k \to \mathbb{R}^k$ by

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \mapsto A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}.$$

For brevity, we shall often write this as $(x_1, \ldots, x_k) \mapsto A(x_1, \ldots, x_k)$.

Since A is an integer matrix, it maps $\mathbb{Z}^k$ to itself. We claim that A allows us to define a map

$$\begin{aligned} T = T_A \quad : \quad & \mathbb{R}^k/\mathbb{Z}^k \to \mathbb{R}^k/\mathbb{Z}^k \\ & (x_1, \ldots, x_k) \mapsto A(x_1, \ldots, x_k) \bmod 1. \end{aligned}$$

To see that this map is well defined, we need to check that if $x, y \in \mathbb{R}^k$ determine the same point in $\mathbb{R}^K/\mathbb{Z}^k$ then $Ax \bmod 1$ and $Ay \bmod 1$ are the same point in $\mathbb{R}^k/\mathbb{Z}^k$. But this is clear: if $x, y \in \mathbb{R}^k$ give the same point in the torus, then $x = y+n$ for some $n \in \mathbb{Z}^k$. Hence $Ax = A(y+n) = Ay+An$. As A maps $\mathbb{Z}^k$ to itself, we see that $An \in \mathbb{Z}^k$ so that Ax, Ay determine the same point in the torus.

Definition. Let $A = (a_{ij})$ denote a $k \times k$ matrix with integer entries such that $\det A \neq 0$. Then we call the map $T_A : \mathbb{R}^k/\mathbb{Z}^k \to \mathbb{R}^k/\mathbb{Z}^k$ a *linear toral endomorphism*.

The map T is not invertible in general. However, if $\det A = \pm 1$ then A^{-1} exists and is an integer matrix. Hence we have a map T^{-1} given by

$$T^{-1}(x_1, \ldots, x_k) = A^{-1}(x_1, \ldots, x_k) \bmod 1.$$

One can easily check that T^{-1} is the inverse of T.

Definition. Let $A = (a_{ij})$ denote a $k \times k$ matrix with integer entries such that $\det A = \pm 1$. Then we call the map $T_A : \mathbb{R}^k/\mathbb{Z}^k \to \mathbb{R}^k/\mathbb{Z}^k$ a *linear toral automorphism*.

Example. Take A to be the matrix

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

and define $T : \mathbb{R}^2/\mathbb{Z}^2 \to \mathbb{R}^2/\mathbb{Z}^2$ to be the induced map:

$$T(x_1, x_2) = (2x_1 + x_2 \bmod 1, x_1 + x_2 \bmod 1).$$

Then T is a linear toral automorphism and is called Arnold's cat[1] map.

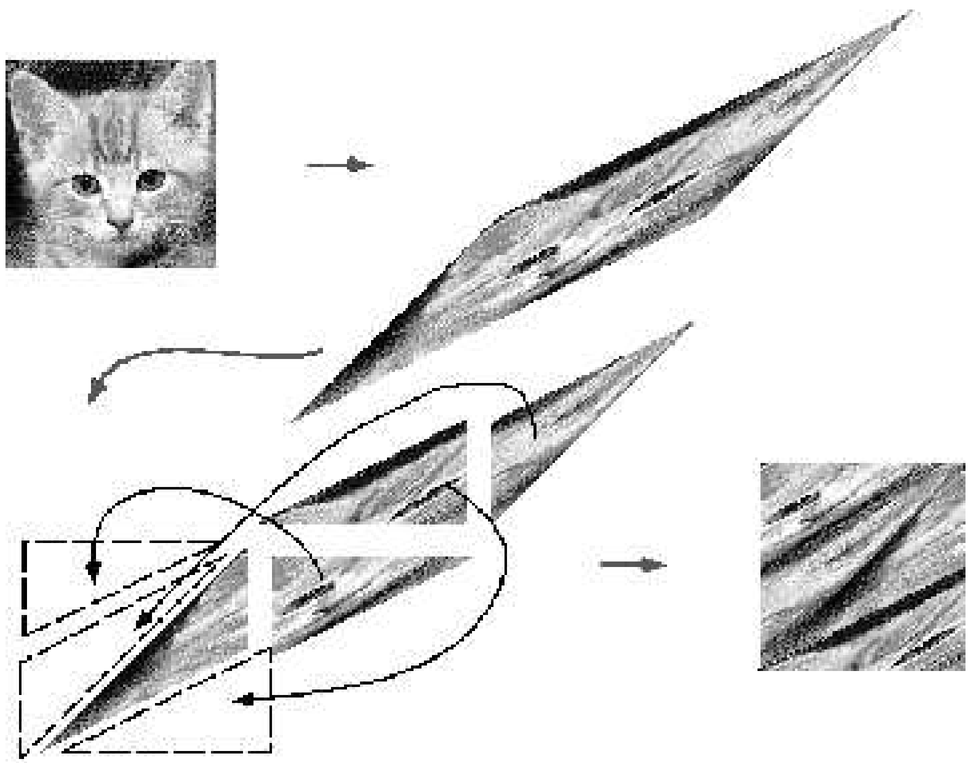

Figure 4.2: Arnold's cat map.

Definition. Suppose that $\det A = \pm 1$. Then we call T a *hyperbolic* toral automorphism if A has no eigenvalues of modulus 1.

Exercise 5.1
Check that Arnold's cat map is hyperbolic. Decide whether the following matrices give hyperbolic toral automorphisms:

$$A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

[1]CAT stands for 'C'ontinuous 'A'utomorphism of the 'T'orus.

Let us consider the special case of a toral automorphism of the 2-dimensional torus $\mathbb{R}^2/\mathbb{Z}^2$.

Proposition 5.1
Let T be a hyperbolic toral automorphism of $\mathbb{R}^2/\mathbb{Z}^2$ with corresponding matrix A having eigenvalues λ_1, λ_2.

(i) The periodic points of T correspond precisely with the set of rational points of $\mathbb{R}^2/\mathbb{Z}^2$:

$$\left\{ \left(\frac{p_1}{q}, \frac{p_2}{q} \right) + \mathbb{Z}^2 \mid p_1, p_2, q \in \mathbb{N},\ 0 \leq p_1, p_2 < q \right\}.$$

(In particular, the periodic points are dense.)

(ii) Suppose that $\det A = 1$. Then the number of points of period n is given by:

$$\mathrm{card}\{x \in \mathbb{R}^2/\mathbb{Z}^2 \mid T^n(x) = x\} = |\lambda_1^n + \lambda_2^n - 2|.$$

Proof. (i) If $(x_1, x_2) = (p_1/q, p_2/q)$ has rational co-ordinates then we can write

$$T^n(x_1, x_2) = \left(\frac{p_1^{(n)}}{q}, \frac{p_2^{(n)}}{q} \right)$$

where $0 \leq p_1^{(n)}, p_2^{(n)} < q$ are integers. As there are at most q^2 distinct possibilities for $p_1^{(n)}, p_2^{(n)}$, this sequence (in n) must be eventually periodic. Hence there exists $n_1 > n_0$ such that $T^{n_1}(x_1, x_2) = T^{n_0}(x_1, x_2)$. As T is invertible, we see that $T^{n_1 - n_0}(x_1, x_2) = (x_1, x_2)$ so that (x_1, x_2) is periodic.

Conversely, If $(x_1, x_2) \in \mathbb{R}^2/\mathbb{Z}^2$ is periodic then $T^n(x_1, x_2) = (x_1, x_2)$ for some $n > 0$. Hence

$$A^n \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \tag{5.1}$$

for some $n_1, n_2 \in \mathbb{Z}$. As A is hyperbolic, A has no eigenvalues of modulus 1. Hence A^n has no eigenvalues of modulus 1, and in particular 1 is not an eigenvalue. Hence $A^n - I$ is invertible. Hence solutions to (5.1) have the form

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = (A^n - I)^{-1} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}.$$

As $A^n - I$ has entries in $\mathbb{Z}$, the matrix $(A^n - I)^{-1}$ has entries in $\mathbb{Q}$. Hence $x_1, x_2 \in \mathbb{Q}$.

(ii) A point (x_1, x_2) is periodic with period n for T if and only if

$$(A^n - I)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}. \tag{5.2}$$

We may take $x_1, x_2 \in [0,1)$. Let $u = (A^n - I)(0,1), v = (A^n - I)(1,0)$. The map $A^n - I$ maps $[0,1) \times [0,1)$ onto the parallelogram

$$R = \{\alpha u + \beta v \mid 0 \leq \alpha, \beta < 1\}.$$

For the point $(x_1, x_2) \in [0,1) \times [0,1)$ to be periodic, it follows from (5.2) that $(A^n - I)(x_1, x_2)$ must be an integer point of R. Thus the number of periodic points of period n correspond to the number of integer points in R. One can check that the number of such points is equal to the area of R. Hence that number of periodic points of period n is given by $|\det(A^n - I)|$.

Let us calculate the eigenvalues of $A^n - I$. Let μ be an eigenvalue of $A^n - I$ with eigenvector v. Then

$$(A^n - I)v = \mu v \Leftrightarrow A^n v = (\mu + 1)v$$

so that $\mu + 1$ is an eigenvalue of A^n. As the eigenvalues of A are given by λ_1, λ_2, the eigenvalues of A^n are given by λ_1^n, λ_2^n. Hence the eigenvalues of $A^n - I$ are $\lambda_1^n - 1, \lambda_2^n - 1$. As the determinant of a matrix is given by the product of the eigenvalues, we have that

$$\begin{aligned} |\det(A^n - I)| &= |(\lambda_1^n - 1)(\lambda_2^n - 1)| \\ &= |(\lambda_1 \lambda_2)^n + 1 - (\lambda_1^n + \lambda_2^n)| \\ &= \lambda_1^n + \lambda_2^n - 2, \end{aligned}$$

as $\lambda_1 \lambda_2 = \det A = 1$.

□