Lecture #4

In the last lecture, we developed a new proof that shows that hyperbolic toral automorphisms are mixing. The main idea came from Hopf, with new ideas by Coudène (and Babillot).

It turns out that any of these hyperbolic toral automorphisms have integer entries and determinant 1, meaning we can think of them as elements in $SL_n\mathbb{Z}$. In fact, most elements in $SL_n\mathbb{Z}$ are hyperbolic toral automorphisms.

There is a natural group action of $SL_n\mathbb{Z}$ on $(\mathbb{T}^n, m)$ given by the matrix acting linearly on $\mathbb{T}^n$. Note, any $A \in SL_n\mathbb{Z}$ is a linear map from $\mathbb{R}^n$ to $\mathbb{R}^n$ which preserves $\mathbb{Z}^n$ as a set, hence A descends to a map on $\mathbb{T}^n$. These linear maps form a group under composition which corresponds to the usual matrix multiplication in $SL_n\mathbb{Z}$. (We are conflating the matrix element A with the linear map.)

Naturally, one might ask if $SL_n\mathbb{Z} \curvearrowright (\mathbb{T}^n, m)$ is ergodic, or even mixing, given the above observation. But, this is a misleading question. We have no definition for mixing (or even ergodicity) of a group action. It will turn out that with the correct generalization of these definitions, despite the number of hyperbolic toral automorphisms in $SL_n\mathbb{Z}$, we give us that $SL_n\mathbb{Z} \curvearrowright \mathbb{T}^n$ is not mixing (rather, it is weakly mixing).

The first part of these notes will be devoted to introducing the definitions of ergodicity, weak mixing, and mixing for measurable group actions. Given time, we will also begin to specialize to specific groups, Lie groups, and discuss basic properties of Lie groups as well as their corresponding Lie algebras.

Before starting with definitions, we need to introduce a fact about locally compact groups.

FACT Every locally compact group G has a left Haar measure m_G which is a non-zero Radon measure satisfying, for any $g \in G$ and any $E^{\text{Borel}} \subseteq G$, $m_G(gE) = m_G(E)$. Moreover, m_G satisfies

① $\forall$ nonempty open set $U \subseteq G$, $m_G(U) > 0$.

② If m_G and $\tilde{m}_G$ are left Haar measures on G, then there exists $c \in (0, \infty)$ such that $\tilde{m}_G = c \cdot m_G$.

③ For every $f \in C_c^+(G)$ and every $g \in m_G$,

$$\int_G f(g^{-1} \cdot h)\, dm_G(h) = \int_G f(h)\, dm_G(h),$$

i.e. $(L_g)_* m_G = m_G$ where $L_g : G \to G$, $h \mapsto gh$.

Recall, a Radon measure is a Borel measure that is finite on all compact sets $K \subseteq G$ (locally finite), outer regular on Borel sets, and inner regular on open sets.

For a proof, see, for example, Folland's textbook "A Course in Abstract Harmonic Analysis," specifically section 2.2. For a simpler treatment in the case that G is metrizable, see Einsiedler-Ward, section 8.3.

Similarly, one can define a right Haar measure as a Radon measure $\tilde{m}_G$ satisfying, for any $g \in G$, $E^{\text{Borel}} \subseteq G$,

$$\tilde{m}_G(Eg) = \tilde{m}_G(E).$$

One can show that m_G is a left Haar measure if and only if $\tilde{m}_G := i_* \mu$ is a right Haar measure, where $i: G \longrightarrow G$ is the inversion map, $g \longmapsto g^{-1}$ (i.e. $\tilde{m}_G(E) = m_G(i^{-1}(E)) = m_G(E^{-1})$.) Because of this, the existence of a left Haar measure implies the existence of the right Haar measure. It turns out that there are instances where the left and right Haar measure are the same, and this ends up being equivalent to

the existence of a lattice $\Gamma \leq G$, i.e. a discrete subgroup such that G/Γ has finite volume, where the volume comes from the quotient of the Haar measure. We will return to this point at a later time in the course.

EXAMPLES (of Haar measures)

① Multiplicative group $\mathbb{R}\setminus\{0\}$: $\frac{dx}{|x|}$

② Multiplicative group $\mathbb{C}\setminus\{0\}$ with coordinates $z = x+iy$: $\frac{dx\,dy}{(x^2+y^2)}$

③ Real $n\times n$ matrices (a_{ij}) such that

$$\begin{cases} a_{ij} = 0 & \text{for } 1 \leq j < i \leq n \\ a_{ii} = 1 & \text{for } 1 \leq i \leq n. \end{cases}$$

Haar measure: $\prod_{i<j} da_{ij}$ (Lebesgue measure).

④ The group of all affine transformations of $\mathbb{R}$, the "$ax+b$" group, is the group (under composition) of the maps of the form $x \longmapsto ax+b$ for $a>0$ and $b\in\mathbb{R}$.
Haar measure(s): $\frac{da\,db}{a^2}$ and $\frac{da\,db}{a}$.

EXAMPLES ① For each example above, determine if the Haar measure is a left Haar measure, right Haar measure, or both.

② Give a Haar measure on $GL_n\mathbb{R} \subseteq \mathbb{R}^{n^2}$ (open set).

Now, we turn our attention to our new definitions.

DEF Let G be a locally compact, second countable group with a left Haar measure m_G. Let (X, μ) be a measure space with σ-finite measure (X can be written as a countable union of sets, each of which has finite μ-measure).

A measurable (left) action of G on X ($G \curvearrowright X$) is a measurable mapping

$$\varphi : G \times X \longrightarrow X$$

$$(g, x) \longmapsto g \cdot x$$

with the following two properties:

$G \curvearrowright X$ is a group action

① $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ and $e \cdot x = x$, (identity in G)

for all $g_1, g_2 \in G$, $x \in X$, and

② G preserves the measure class of μ,

that is, for all measurable subsets $E \subset X$ and all $g \in G$, we have that $\mu(gE) = 0$ if and only if $\mu(E) = 0$. In this case, we say μ is a quasi-invariant measure.

(interaction between G and the measure μ. (μ is quasi-invariant))

⓪ REMARK on (lack of) existence of invariant measures...

NOTE ① We will say "action of G on (X, μ)" to implicitly mean "measurable action of G on (X, μ)".

② Most often, our measurable actions will have an invariant measure μ, not just a quasi-invariant measure. (ie. an invariant measure will satisfy for any $E^{meas} \subset X$, $g \in G$, $\mu(gE) = \mu(E)$.)

(3) For invariant measures, we have that for any $g \in G$,

$$g_* \mu = \mu.$$

In this case, we say that the action of G on (X, μ) is a measure-preserving action. Most actions that we will study will turn out to be measure-preserving actions.

(4) Flows on, say, a smooth manifold M are group actions on the manifold. There are both continuous and smooth flows, which are (continuous or smooth) maps

$$\Theta : \mathbb{R} \times M \longrightarrow M$$

satisfying the group laws: $\begin{cases} \Theta(t+s, p) = \Theta(t, \Theta_s(p)) \\ \Theta(0, p) = p \end{cases}$

sometimes more elegantly written in the form $\Theta_t : M \to M$ where $\Theta_t(p) := \Theta(t, p)$. In this form, the group laws are $\Theta_t \circ \Theta_s = \Theta_{t+s}$ and $\Theta_0 = Id_M$. Moreover, to be a flow, each Θ_t must be a homeomorphism or diffeomorphism (depending on whether Θ is continuous/smooth, resp.).

⑤ Along these lines, many authors define a measurable on a locally compact Hausdorff space S continuous (or smooth) left action to be a continuous map

$$\varphi : G \times S \longrightarrow S$$
$$(g, s) \longmapsto g \cdot s$$

such that

interaction w/ the topology { ① $s \longmapsto gs$ is a homeomorphism of S for each $g \in G$.

group action { ② $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$ and $e \cdot s = s$ for all $g_1, g_2 \in G$, $s \in S$.

EXERCISE Write a definition for a smooth left action of a group that an author might use.

DEF Let G act on (X, μ) (measurably). A function $f : X \to \mathbb{R}$ is essentially G-invariant if, for any $g \in G$, one has $f(gx) = f(x)$ for μ-almost all $x \in X$. The function is G-invariant if $f(gx) = f(x)$ for all $g \in G$ and all $x \in X$.

LEMMA Let G be a locally compact second group (lcsc group) acting on a σ-finite measure space (X, μ). Let $f : X \to \mathbb{R}$ be an essentially G-invariant function. Then, there exists a measurable G-invariant function $\tilde{f} : X \to \mathbb{R}$ s.t. $\tilde{f} = f$ a.e. on X.

For a proof of this fact, see Bekka-Mayer Lemma 1.2 in Chapter 1.

We will turn our attention to the notion of ergodicity:

DEF The action of a locally compact second countable group G on a σ-finite measure space (X,μ) is ergodic if there are no nontrivial invariant subsets of X: $\forall$ measurable $E \subseteq X$ that is G-invariant, then $\mu(E)=0$ or $\mu(X \setminus E)=0$.

G-invariant: $g \cdot E = E \ \forall g \in G$

allows for σ-measure space!

As before, we have (same setting as above)

THM G lcsc group, (X,μ) σ-finite measure space. G acts ergodically on (X,μ) if and only if for any $f: X \to \mathbb{R}$ that is measurable and G-invariant, f is constant a.e.

For a proof, see Bekka-Mayer, Chapter 1, or prove as an exercise! This is similar to the situation we encountered in the first lecture: you need a bootstrapping argument.

EXAMPLE $G = SL_n\mathbb{Z}$, $n \times n$ matrices with integer entries and determinant 1. $G \curvearrowright \mathbb{R}^n$ and preserves $\mathbb{Z}^n$, so $G \curvearrowright \mathbb{R}^n/\mathbb{Z}^n \cong \mathbb{T}^n$. We claim the

w/ Leb measure.

action is ergodic. Indeed, for any $A \in G$ without eigenvalues on the unit circle, $A : \mathbb{T}^n \to \mathbb{T}^n$ is ergodic (in fact, mixing!). This means any A-invariant measurable subset of $\mathbb{T}^n$ is either null or conull. Since $A \in G$, any G-invariant measurable subset must be A-invariant, thus $G \curvearrowright \mathbb{T}^n$ ergodically.

EXAMPLE Let $\mathbb{Z} \curvearrowright \mathbb{T}^1 = \mathbb{R}/\mathbb{Z}$ by $n \cdot x := x + \alpha n$ for $\alpha \notin \mathbb{Q}$.

Observe that our new definition agrees with the old (ergodicity).

We now change our perspective (and setting) slightly. Let G be a locally compact group and (X, μ) a probability space. Let G be a measure-preserving action on (X, μ). ($g_* \mu = \mu$ $\forall g \in G$).

DEF $\pi : G \to \mathcal{U}(L^2(X, \mu))$ given by $\pi(g) u(x) = u(g^{-1}x)$ is a unitary representation of G on $L^2(X, \mu)$ if

1. π is a homomorphism
2. [$\pi(g)$ is a unitary operator.] ← implied
3. the map $G \to L^2(X)$ given by $g \mapsto \pi(g) f$ is continuous for all $f \in L^2(X, \mu)$ (norm topology!)

More generally, $\pi: G \to \mathcal{U}(\mathcal{H})$, $\mathcal{H}$ Hilbert space, is a unitary representation of G on $\mathcal{H}$ when

① π is a homomorphism

[② $\pi(g)$ unitary] ← implied

③ $G \to \mathcal{H}$ given by $g \mapsto \pi(g)\xi$ is cont. for all $\xi \in \mathcal{H}$. ("π is continuous in the strong operator topology.)

THM A measure-preserving action of G on a prob. space (X,μ) is ergodic if and only if the space

$$\{f \in L^2(X) \mid \pi(g)f = f \ \forall g \in G\}$$

of the invariant vectors consists only of the constant functions, $\mathbb{C}\cdot\mathbb{1}$.

DEF $L^2_0(X,\mu) := (\mathbb{C}\cdot\mathbb{1})^\perp = \{f \in L^2(X) \mid \int_X f\,d\mu = 0\}$.

THM Let π_0 be the restriction of $\pi: G \to \mathcal{U}(L^2(X,\mu))$ to a representation of G on $L^2_0(X,\mu)$. Then $G \curvearrowright (X,\mu)$ is ergodic iff π_0 does not contain the trivial representation 1 of G, i.e. there is no non-zero subspace on which π_0 acts trivially ($\pi_0(g)f = f$ for f in the subspace).

NOTE The trivial representation is given by $\pi_0(g) = \underline{\mathrm{Id}} \quad \forall g \in G$.

EXERCISE Show that the restriction π_0 exists!

We now turn our attention to mixing. We need a definition first:

Y locally compact space

DEF $C_0(Y) := \{ f \text{ continuous} \mid f \text{ vanishes at infinity} \}$

where $f : Y \longrightarrow \mathbb{C}$ vanishes at infinity if $\forall \varepsilon > 0$,

$$\{ y \in Y \mid |f(y)| \geq \varepsilon \}$$

is compact.

DEF The action of G on (X, μ) is mixing if all of the matrix coefficients

$$g \longmapsto \langle \pi(g) u, v \rangle, \quad u, v \in L^2_0(X)$$

vanish at infinity.

NOTE $$\langle \pi(g) u, v \rangle = \int_X \pi(g) u \cdot v \, d\mu = \int_X u(g^{-1}x) \, v(x) \, d\mu.$$

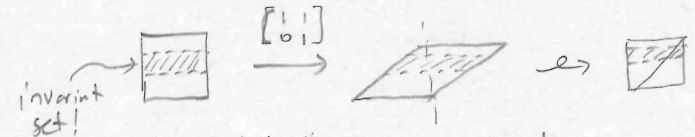
This "agrees" with one equivalent notion of mixing for mp. transformations.

EXAMPLE $G = SL_n\mathbb{Z} \curvearrowright \mathbb{T}^n$ is <u>not</u> mixing for $n \geq 2$.

To see this, let

$$H = \left\{ \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \mid m \in \mathbb{Z} \right\} \subseteq SL_2\mathbb{Z}.$$

The action of H on $\mathbb{T}^2$ is not even ergodic...

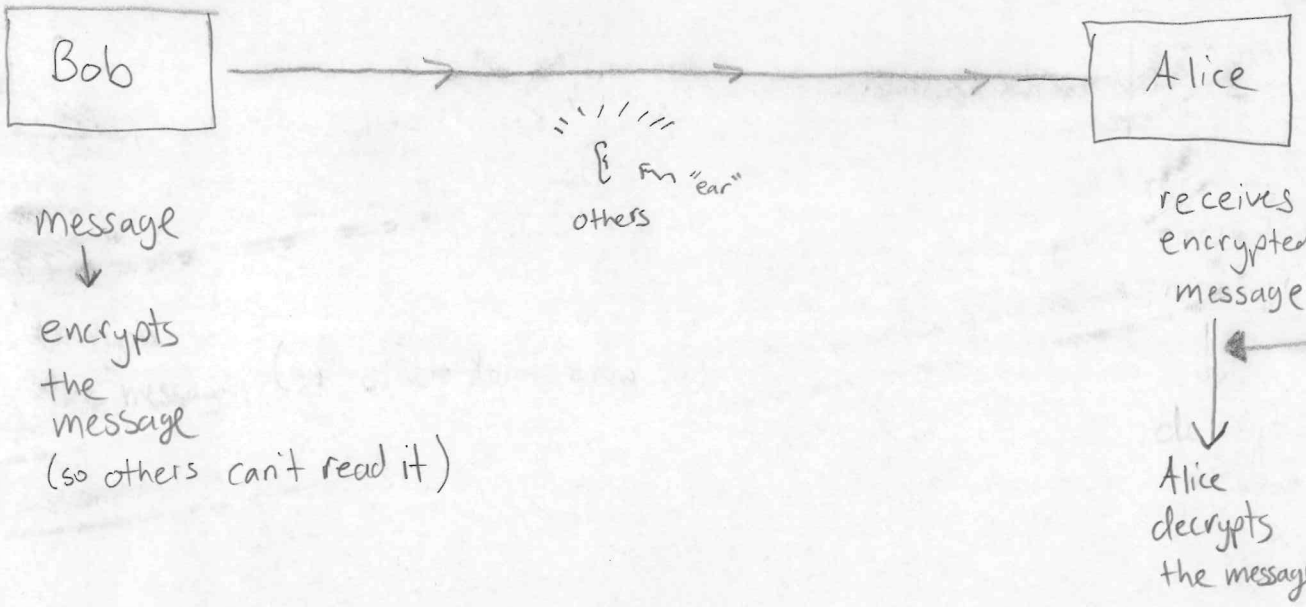


in fact, all horizontal lines are invariant!

EXERCISE For any $h \in H$, construct a matrix coefficient by picking $u, v \in L^2_0(X, \mu)$ such that $\langle \pi(h^n)u, v \rangle > 0$ for all $n \in \mathbb{N}$. Show that this matrix coefficient is <u>not</u> in $C_0(G)$. (Alternatively, show $h^n \to \infty$ in G.)

Cryptography

Classically



3 Examples

"cypher" British English

① Shift Cipher : $(\mathbb{Z}/26\mathbb{Z})$

② Anonymous voting technique : Division algorithm

③ Book cypher :] Explain this.

] Do variations on these.

(Division Algorithm : If a and b are integers and $b>0$, then there are unique integers q (the quotient) and r (the remainder) s.t. $a=bq+r$ where $0 \leq r < b$.

Note : Problem with $\mathbb{Z}$: can't divide...