Ratner's Theorems and Homogeneous Dynamics

Lectures by Professor Ilya Khayutin
Scribe: Holden Lee

October 4, 2018

Contents

Introduction

We will use the book http://tbward0.wixsite.com/books/homogeneous.

We'll use theorems from representation theory, ergodic theory, and Lie groups. We'll state what we need, with specific examples.

Chapter 1

Homogeneous dynamics

1 Introduction: Homogeneous dynamics

Homogeneous dynamics is about a special kind of dynamical system. We start with G, a locally compact topological group. Think of 2 examples: $G = \mathbb{R}^n$ and $G = \mathrm{SL}_n(\mathbb{R}) = \{g \in \mathcal{M}_{n\times n}(\mathbb{R}) : \det g = 1\}$.

Consider $\Gamma < G$ discrete with finite covolume. Consider the quotient manifold $\Gamma\backslash G \circlearrowleft G$, which has a natural action by G,

$$h.\Gamma g = \Gamma g h^{-1}. \tag{1.1}$$

It has finite covolume if $\Gamma\backslash G$ carries a finite G-invariant Borel measure. It will always be explicit for us; we can write it down in coordinates. It always carries a left-invariant and right-invariant measure called the Haar measure, unique up to constant. The quotient group also carries a invariant measure but it doesn't have to be finite.

The Haar measure on $\mathbb{R}^n$ is the Lebesgue measure.

Exercise 1.1.1: Write a Haar measure on $\mathrm{GL}_n(\mathbb{R})$ in coordinates; write in terms of $g = (x_{ij})_{ij}$.

Remark 1.1.2: If $\Gamma\backslash G$ is compact, then Γ is a lattice in G ($\Gamma < G$).

Example 1.1.3: Let $\Gamma = \mathbb{Z}^n < \mathbb{R}^n = G$. Then $\Gamma\backslash G = \mathbb{Z}^n\backslash\mathbb{R}^n \cong \mathbb{T}^n$. Note $\mathbb{T}^1 \cong \mathbb{S}^1$. The quotient can be represented by a fundamental domain, $[0,1]$, where 0 and 1 are identified.

Example 1.1.4: Another example: $\Gamma = \mathrm{SL}_n(\mathbb{Z}) = \{g \in \mathcal{M}_{n\times n}(\mathbb{Z}) : \det g = 1\}$ is a lattice in $\mathrm{SL}_n(\mathbb{R})$. The quotient is not compact but has finite volume; it's a weird object. It has something that goes to infinity but gets thinner and thinner. It's a moduli problem of some sort.

Dynamics: Let $H < G$ be a closed subgroup. Then $H \circlearrowright \Gamma\backslash G$. We want to understand all orbits of this group, or as many as we can.

Consider a line in $\mathbb{R}^2$. If we quotient by $\mathbb{Z}^2$, the line folds into itself. This folding can be complicated. The closure of each orbit is either either periodic (a subtorus, if the slope is rational) or everything. This is a simple result we try to imitate in a more complicated setting.

Our aim is to understand orbit closures of $H \circlearrowright \Gamma\backslash G$ and H-invariant probability measures on $\Gamma\backslash G$.

The classic motivation was from geometry: flows on negatively curved manifolds. In the 80's, due to Margulis, the subject became related to number theory, and exploded exponentially.

Margulis solved the following problem, for which the field became famous.

Conjecture 1.1.5 (Oppenheim)**.** *Let $Q(x_1, \ldots, x_n) = x^\top Gx = \sum g_{ij}x_ix_j$ be an irrational indefinite non-degenerate quadratic form in $n \geq 3$ variables. Then $Q(\mathbb{Z}^n_{prim})$ is dense in $\mathbb{R}$. ($\mathbb{Z}^n_{prim}$ is the set of points with no common divisors.)*

Davenport proved this for $n \geq 9$. It was hard to push it down to 3.

The solution depends on this observation due to Raghunatan and Margulis. The conjecture is equivalent to the following statement: Consider $\mathrm{SO}(Q) = \{g \in \mathrm{SL}_n(\mathbb{Z}) : Q(g.x) = Q(x)\}$. Note $\mathrm{SO}(Q) \circlearrowright \mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{SL}_n(\mathbb{R})$. (To see this, note $Q(\mathbb{Z}^n)$ is invariant under $\mathrm{SL}_n(\mathbb{Z})$.)

Conjecture 1.1.6. *Every orbit of $\mathrm{SO}(Q)$ on $\mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{SL}_n(\mathbb{R})$ is either unbounded or it is compact and carries a finite $\mathrm{SO}(Q)$-invariant measure.*

You cannot have bounded orbits which are not compact. This dichotomy between 2 types of orbits is very close to the original conjecture.

This type of proof gives non-effective results at first. It's a soft statement. Since then it has been made effective to some extent.

The following example can be solved using homogeneous dynamics, or harmonic analysis and automorphic forms. The methods are related.

Example 1.1.7: Let V_d be the variety of matrices with $\det X = d$, $d \in \mathbb{N}$, so

$$V_d(\mathbb{R}) = \{X \in \mathcal{M}_{n\times n}(\mathbb{R}) : \det X = d\}. \tag{1.2}$$

Question: Fix a "nice" bounded open set $\Omega \subseteq V_1(\mathbb{R})$. How many integral points are there in Ω—how does this grow as $d \to \infty$?

$$\text{as } d \to \infty, \quad |d^{-1/n}V(\mathbb{Z}) \cap \Omega| \sim ? \tag{1.3}$$

The answer is that

$$\frac{|d^{-1/n}V(\mathbb{Z}) \cap \Omega_1|}{|d^{-1/n}V(\mathbb{Z}) \cap \Omega_2|} \to \frac{m(\Omega_1)}{m(\Omega_2)} \tag{1.4}$$

for the Haar measure m. It's easy to calculate the rate of convergence.

Observe that V_d is homogeneous, $G = \mathrm{SL}_n(\mathbb{R}) \times \mathrm{SL}_n(\mathbb{R}) \circlearrowright V_d(\mathbb{R})$ by

$$(g_1, g_2).X = g_1 X g_2^{-1}. \tag{1.5}$$

The action is transitive and $G(\mathbb{Z})$ stabilizes $V_d(\mathbb{Z})$. There's only finitely many $G(\mathbb{Z})$ orbits on $V_d(\mathbb{Z})$ (due to Borel, Harish-Chandra). To see this, note each matrix has a Smith normal form: for all $M \in \mathcal{M}_{n\times n}(\mathbb{Z})$ there exists $S, T \in \mathrm{GL}_n(\mathbb{Z})$ and $d_1 | \cdots | d_n$ such that $M = S \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} T$. There are finitely many orbits and you can classify them.

All points are conjugate, so to understand the stabilizer, fix your favorite point and calculate its stabilizer.

$$\mathrm{Stab}_G(d^{-1/n} I_d) = \mathrm{SL}_n(\mathbb{R})^\Delta \hookrightarrow \mathrm{SL}_n(\mathbb{R}) \times \mathrm{SL}_n(\mathbb{R}). \tag{1.6}$$

Understanding Q is the same as studying "periodic" orbits of $\mathrm{SL}_n(\mathbb{R})^\Delta \circlearrowright \mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{SL}_n(\mathbb{R}) \times \mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{SL}_n(\mathbb{R})$. If a group acts transitively, the space looks like the group quotiented by the stabilizer.

$$V_d(\mathbb{R}) \cong \mathrm{SL}_n(\mathbb{R}) \times \mathrm{SL}_n(\mathbb{R}) / \mathrm{SL}_n(\mathbb{R})^\Delta. \tag{1.7}$$

You can show this with automorphic forms, using a spectral gap, so don't be impressed by this example.

The following is more impressive, and brings the world of p-adics into the game.

Example 1.1.8: Let $V(\mathbb{R}) = \mathbb{S}^{n-1}(\mathbb{R}) \times \mathbb{S}^{n-1}(\mathbb{R}) = \{v, w \in \mathbb{R}^n : \langle v, v\rangle = 1, \langle w, w\rangle = 1\}$, $n \geq 3$. For $d \in \mathbb{N}, e \in \mathbb{Z}$.

$$V_{d,e}(\mathbb{Z}) = \left\{v, w \in \mathbb{Z}^n_{\mathrm{prim}} : \langle v, v\rangle = d, \langle w, w\rangle = d, \langle v, w\rangle = e\right\}. \tag{1.8}$$

A classical number theorist can check for which d, e there are solutions. For $\Omega \subseteq V(\mathbb{R})$ nice. Then the conjecture is that

$$\frac{\left|d^{-1/2} V_{d,e}(\mathbb{Z}) \cap \Omega\right|}{|V_{d,e}(\mathbb{Z})|} \to m \times m(\Omega) \tag{1.9}$$

where m is the rotation invariant measure on the sphere. if $d \to \infty$, $|e| \to \infty$.

This is known for $n \geq 4$ (certainly for $n \geq 6$). For $n = 3$ this is open, related to Fourier coefficients of modular forms, and the Andre-Orr conjecture.

For $n = 3$ you can count up to Ziegler's bound; the number of points on the sphere is a class number.

$SO_n(\mathbb{R}) \times \mathrm{SO}_n(\mathbb{R}) \circlearrowright V(\mathbb{R})$. The stabilizer is conjugate over $\mathbb{R}$ to $\mathrm{SO}_{n-1}(\mathbb{R})^\Delta \hookrightarrow \mathrm{SO}_n(\mathbb{R}) \times \mathrm{SO}_n(\mathbb{R})$ (You need to rotate the same). $\mathrm{SO}_{n-1}(\mathbb{R})^\Delta$ is compact, which is a big problem;

dynamics are simple and there's nothing you can use. Why can you solve it using dynamics? Enlarge your original problems. Because equations are integral, consider not just integral but p-adic places. Stabilizers of points may be non-compact in the p-adic place. Use dynamics of the p-adic places.

Except for Oppenheim's conjecture, in all applications you use p-adic places in some deep way.

You can also use dynamics to count points.

The next example is surprising. You generate a nontrivial integral point using dynamics. This is an example of a different nature.

Example 1.1.9 (Ellenberg-Venkatesh)**:** Let $(Z^n, Q), (Z^m, Q')$ be quadratic spaces (coordinate free version of quadratic form).

We try to represent one by another using more variables. In the simplest case, can we represent an integer by a given quadratic form; that's the $m = 1$ case.

We say that Q' is representable by Q if there is a homomorphism of abelian groups $\varphi : \mathbb{Z}^m \hookrightarrow \mathbb{Z}^n$ such that $Q' = Q \circ \varphi$. This is a fancy way to say the following: if you write in coordinates,

$$Q'(y) = Q(A.y), \quad A \in M_{n\times m}(\mathbb{Z}). \tag{1.10}$$

There are some obviously necessary conditions, the local conditions.

Definition 1.1.10: Q' is everywhere locally representable by Q if $Q' \otimes \mathbb{R}$ is representable by $Q \otimes \mathbb{R}$ and for all p, and for all p, $Q' \otimes \mathbb{Z}_p$ is representable by $Q \otimes \mathbb{Z}_p$, or equivalently, for all p^d, Q' mod p^d is representable over $\mathbb{Z}/p^d\mathbb{Z}$ by Q mod p^d.

Is this sufficient, i.e., does the local-to-global principle hold? Not necessarily.

Theorem 1.1.11 (Ellenberg-Venkatesh)**.** *Let Q be a positive definite form over $\mathbb{Z}^n$. There exists $C(Q)$ such that if $m \le n - 7$ and $(\mathbb{Z}^m, Q')$ has square-free discriminant, Q represents Q' locally everywhere, and $\min_{\mathbb{S}^{m-1}(\mathbb{R})} Q' > C(Q)$, then Q represents $Q'/\mathbb{Z}$.*

The proof idea: it's known it has a rational point, you want to upgrade it to a integral point. Integrality can be checked locally, and so can be checked using dynamics.

Conjecture 1.1.12. *This holds if $n - m \ge 3$.*

What happens if $n - m = 2$ is interesting. It's unclear what to conjecture. The stabilizer becomes abelian; its nature changes.

There is another pair of examples, due to Venkatesh.

1. A modular form on nonarithmetic group cannot have multiplicative coefficients. This is a nice application of homogeneous dynamics. See Kowalski's blog.

2. Elliptic curves: higher-order Heegner points, traces are nontrivial.

Let G be a locally compact second countable group, $G = \mathrm{SL}_n(\mathbb{R})$. G carries a left invariant Borel measure m_L and a right invariant Borel measure m_R. I.e., for all A, for all $g \in G$,

$$m_L(gA) = m_L(A). \tag{1.11}$$

By Riesz representation, this is equivalent to: for all $f \in C_c(G)$,

$$\int f(gx)\, dm_L(x) = \int f(x)\, dm_L(x). \tag{1.12}$$

The measures are not always the same. G is **unimodular** if $m_L = m_R$.

Exercise 1.1.13: Show that $\mathrm{SL}_n(\mathbb{R})$ is unimodular.

Correction from last time: local-global: Q' represents Q, $\min_{\mathbb{Z}^n \setminus \{0\}} Q' \geq C(Q)$, not effective (?).

2 Haar measures

Let G be a locally compact group. There exists a right-invariance Borel measure $m \neq 0$ on G: for all B Borel, $g \in G$, $m_R(Bg) = m_R(B)$. This measure is unique up to scaling. We can define a left-invariant measure by $m_L(B) = m_R(B^{-1})$.

A group admits a finite Haar measure iff it is compact. A nice way is to prove this is with representation theory. A Haar measure satisfies:

1. $m_R(K) < \infty$ for all compact $K \subseteq G$.
2. $m_R(O) > 0$ for all open $O \subseteq G$.

Proposition 1.2.1: Let G be a compact abelian group, $g \in G$, $\overline{\langle g \rangle} = G$. Then any R_g-invariant probability measure is the Haar measure.

Proof. G acts on the right on $\mathcal{M}_1(G)$, the space of probability measures on G, by

$$(g.m)(B) = m(Bg). \tag{1.13}$$

$\mathcal{M}_n(G)$ is a compact metric space equipped with the weak-* topology. $\mathrm{Stab}_G(\mu) = \{g \in G : g.\mu = \mu\}$. It is a closed subgroup, by checking against continuous functions (by Riesz representation). $g \in \mathrm{Stab}_G(\mu)$ implies $\overline{\langle g \rangle} \subseteq \mathrm{Stab}_G(\mu)$, so $\mathrm{Stab}_G(\mu) = G$ and $\mu = m$. $\square$

This is a very soft argument.

Corollary 1.2.2. *Let $f \in C(G)$, $h \in G$. Then*

$$\frac{1}{N} \sum_{n=0}^{N-1} f(hg^{-n}) \xrightarrow{N \to \infty} \int f\, dm. \tag{1.14}$$

Proof. Let $\mu_n := \frac{1}{N}\sum_{n=0}^{N-1}\delta_{hg^{-n}}$. Let μ_∞ be any weak-$*$ limit point of μ_n. Then μ_∞ is R_g. ($g.\mu_N - \mu_N \to 0$ by telescoping.) Thus $\mu_\infty = m$. Hence $\mu_N \xrightarrow{\text{weak-*}} m$. $\square$

This is an extremely soft argument, but common in ergodic theory.

Exercise 1.2.3: Prove the same using Pontryagin duality: $\widehat{G} = \{\chi : G \to \mathbb{S}^n\}$ separates points.

Let G be a locally compact σ-compact group equipped with a left-invariant metric $d_G : G \times G \to \mathbb{R}_{\geq 0}$: For all $h, g_1, g_2 \in G$, $d(hg_1, hg_2) = d(g_1, g_2) = d(g_2^{-n}g_1, e)$. ($d_G$ exists always, if G has countable basis.)

Definition 1.2.4: Let $H \leq G$ be a closed subgroup. Define $d_{H\backslash G} : H\backslash G \times H\backslash G \to \mathbb{R}$ by $d(Hg_1, Hg_2) = \inf_{h_1,h_2\in H} d(h_1 g, h_2 g) = \inf_{h\in H} d(hg_1, g_2)$.

Check that $d_{G/H}$ is a metric, G/H is a locally compact σ-compact space, G and G/H metrically complete, $d_{H\backslash G}$ induces the quotient topology on G/H. Comment: If d_G is proper (closure of open ball is a closed ball) and $H = \Gamma < G$ is discrete then the inf is realized.

3 Radius of injectivity

Assume $\Gamma < G$ is discrete.

Proposition 1.3.1: For every $K \subseteq \Gamma\backslash G$ compact, there exists $r = r(K) > 0$, a **radius of injectivity** for K, such that for $\Gamma g \in K$,

$$B_r(g) = gB_r(0) \to \Gamma g B_r(e) \tag{1.15}$$

is injective (and hence is an isometry). In $\pi : G \to \Gamma\backslash G$, $\pi|_{B_r(g)}$ is injective. Moreoever, if $K = \{\Gamma h\}$ then

$$r = \frac{1}{4}\inf_{e\neq\gamma\in\Gamma} d(h^{-1}\gamma h, e) \tag{1.16}$$

works.

(This is > 0 because Γ is discrete.)

Proof. We show this for $K = \{\Gamma h\}$. Let $g_1, g_2 \in B_r(e)$.

$$d(\Gamma h g_1, \Gamma h g_2) = \inf_{\gamma\in\Gamma} d(h^{-1}\gamma h g_1, g_2). \tag{1.17}$$

We want to establish that the inf is realized at $\gamma = e$. By the triangle inequality,

$$\begin{aligned} 4r &\leq d(h^{-1}\gamma h, e) = d(e, h^{-1}\gamma h) \leq d(g_1, h^{-1}\gamma h) + d(e, g_1) && (1.18)\\ &\leq d(h\gamma h^{-1}g_1, e) + r \leq d(h\gamma h^{-1}g_1, g_2) + d(g_2, e) + r && (1.19)\\ &\leq d(hgh^{-1}g_1, g_2) + 2r. && (1.20)\end{aligned}$$

So

$$d(hgh^{-1}g_1, g_2) \geq 2r \geq d(g_1, g_2). \tag{1.21}$$

If $K \subseteq \Gamma\backslash G$ is compact, for any $y \in \Gamma g B_{r/2}(e)$, r the injective radius of Γg, $r/2$ is an injective radius. Use compactness. □

Definition 1.3.2: Define $r_{\text{inj}}(\Gamma g)$ as the supremum (maximum) over injectivity radii at $\Gamma g \in \Gamma\backslash G$.

$$\frac{1}{4}\inf_{e\neq\gamma\in\Gamma}(g^{-1}\gamma g, e) \leq r_{\text{inj}}(\Gamma g) \leq \inf_{e\neq\gamma\in\Gamma} d(g^{-1}\gamma g, e). \tag{1.22}$$

A word of caution.

Remark 1.3.3: $\pi : G \to \Gamma\backslash G$ is a covering map, Γ acts on G without fixed points. The same is not true for the following Let $K < G$ be a compact subgroup. G/K is a symmetric space. We want to understand $\pi : G/K \to \Gamma\backslash G/K$. But Γ can have stabilizers when acting on G/K, so G/K is not as nice. G/K may not be a manifold.

A famous example is the modular curve.

You really need to remember the stabilizers when not working in $\Gamma\backslash G$.

We want to understand the measure structure of $\Gamma\backslash G$.

4 Fundamental domains

Definition 1.4.1:

1. $\mathcal{F} \subseteq G$ is a **fundamental domain** for $\Gamma \leq G$ discrete if

$$G = \bigsqcup_{\gamma\in\Gamma} \gamma\mathcal{F}. \tag{1.23}$$

   This is true iff for all $g \in G$, $\Gamma g \cap \mathcal{F}$ is a singleton, iff $\pi|_{\mathcal{F}}$ is a bijection.

2. $B_{\text{inj}} \subseteq G$ is an **injective set** for Γ if $\pi : G \to G/\Gamma$ when restricted to B_{inj}.

3. $B_{\text{surj}} \subseteq G$ is a **surjective set** for Γ if $\pi|_{B_{\text{surj}}}$ is surjective.

For example, $[0, 1)^d$ is a fundamental domain for $\mathbb{Z}^d < \mathbb{R}^d$.

Proof. An injective and surjective set always exist (ϕ and G). We claim that if $B_{\text{inj}} \subset B_{\text{surj}}$ then there exists a fundamental domain $\mathcal{F}$, $B_{\text{inj}} \subseteq \mathcal{F} \subseteq B_{\text{surj}}$ where $\pi|_{\mathcal{F}}$ is bi-measurable.

Bi-measurable: π is continuous $\implies$ π is measurable.

G is σ-compact $\implies$ $G = \bigcup B_n$ where each B_n is an open injectiv eball.

For any B Borel, $\pi(B \cap B_n)$ is measurable, $\pi(B) = \bigcup_{n\in\mathbb{N}} \pi(B \cap B_n) \in$ Borel σ-algebra.

Construction of fundamental domain:

$$\begin{aligned}
\mathcal{F}_0 &= B_{\text{inj}} && (1.24)\\
\mathcal{F}_1 &= B_{\text{surj}} \cap B_1 \backslash \Gamma \mathcal{F}_0 && (1.25)\\
&\vdots && (1.26)\\
\mathcal{F}_n &= B_{\text{surj}} \cap B_n \backslash \bigcup_{k=0}^{n-1} \Gamma \mathcal{F}_k. && (1.27)
\end{aligned}$$

Define $B_{\text{inj}} \subseteq \mathcal{F} = \bigcup_{n=0}^{\infty} \mathcal{F}_n \subseteq B_{\text{surj}}$. For any Γg define $n = 0$ if $\Gamma g \cap B_{\text{inj}}$, otherwise n is the minimal k such that $\Gamma g \cap B_{\text{surj}} \cap B_k$. Check $\Gamma g \cap \mathcal{F}$ is a single element. □

Proposition 1.4.2:

Let m_L be a left Γ-invariant measure on G.

1. Any fundamental domain has the same measure: For any $\mathcal{F}$, $\mathcal{F}'$ fundamental domains, $m_L(\mathcal{F}) = m_L(\mathcal{F}')$.

2. Construct m_X on $X = \Gamma\backslash G$ by

$$m_X(B) = m_L(\pi^{-1}(B) \cap \mathcal{F}). \tag{1.28}$$

This is independent of $\mathcal{F}$. If G is unimodular and $m_L = m$ is the Haar measure then m_X is a right G-invariant measure on $\Gamma\backslash G$ and unique up to scaling.

Corollary 1.4.3. *If $B_{inj} \subseteq G$ is injective, then $m_X(\pi(B_{inj})) = m_L(B_{inj})$.*

Proof.

1. $m_L(\mathcal{F}') = \sum_{\gamma\in\Gamma} m_L(\mathcal{F}' \cap \gamma\mathcal{F}) = \sum_{\gamma} m_L(\gamma^{-1}\mathcal{F}' \cap \mathcal{F}) = m_L(\mathcal{F})$.

2. $m_L = m$ is right and left invariant, so

$$\begin{aligned}
m_X(Bg) &= m(\pi^{-1}(B)g \cap \mathcal{F}) && (1.29)\\
&= m(\pi^{-1}(B) \cap \mathcal{F}g^{-1}) = m_X(B). && (1.30)
\end{aligned}$$

For uniqueness, let ν be a right G-invariant measure on $\Gamma\backslash G$. Given $f \in C_c(G)$, define $f_X : \Gamma\backslash G \to \mathbb{C}$, also in $C_c(\Gamma\backslash G)$, by

$$f_X(\Gamma g) = \sum_{\gamma\in\Gamma} f(\gamma g). \tag{1.31}$$

Define a measure on G by $\int_G f\, d\nu_G = \int_{\Gamma\backslash G} f_X\, d\nu$. It is easy to check that ν_G is right-invariant, so $\nu_G \propto m$.

□

5 Lattices

Definition 1.5.1: $\Gamma \leq G$ discrete is a **lattice** if $\Gamma\backslash G$ admits a right G-invariant finite (nonzero) Borel measure.

Remark 1.5.2: $\Gamma\backslash G$ is compact iff there exists a surjective? (sinj) compact set where a right G-invariant measure is always finite. We say Γ is co-compact or uniform. ???

Does a group admit a lattice; this is a very difficult question. It must be unimodular Given a unimodular group, does it admit a lattice? No. It's not easy to find a ocxunterexample.

Proposition 1.5.3: If G admits a lattice $\Gamma \subseteq G$ then G is unimodular.

Theorem 1.5.4 (Poincaré recurrence)**.** *Let $(X, \mathcal{B}, \mu)$ be a probability measure space and $T : X \to X$ be a measurable measure-preserving transformation (for all $B \in \mathcal{B}, \mu(T^{-1}B) = \mu(B)$). If $\mu(A) > 0$ then for μ a.e., $x \in A$, there exists $h_k \to \infty$ such that $T^{h_k}x \in A$.*

Proof: exercise.

Proof of Proposition. A measure m_X on $\Gamma\backslash G$ is right-invariant using folding we get μ on G which is G-right invariant and Γ-left invariant,

$$\mu(f) = m_X(\sum_{\gamma\in\Gamma} f(\gamma g)). \tag{1.32}$$

$(g.\mu)(B) = \mu(g^{-1}B)$ is a right Haar measure, $\mu(g^{-1}B) = \chi(g)\mu(B)$, where $\chi : G \to \mathbb{R}_{>0}$. It is straightforward to check that χ is a character, a continuous group homomorphism and $\Gamma < \ker\chi$. Fix $g \in G$, we want to show $\chi(g) = 1$. We will prove there exists $n_k \to \infty$ such that $|\chi(g)|^{n_k} \ll 1$ (i.e. $\leq C$ a constant).

Look at $(\Gamma\backslash G, \mathcal{B}, m_X)$, $T(h) = hg^{-1}$. By Poncaré rec, for all $0 < r < r_{\text{inj}}(\Gamma e)$, there exists $n_k \to \infty$, $\gamma_k \in \Gamma$, $h, h_k \in B_e(r)$ such that

$$\gamma_k h g^{-n_k} = h_k \tag{1.33}$$
$$\chi(g)^{-n_k} = \chi(h^{-1}h_k) \in \chi(B_{2r}(e)). \tag{1.34}$$

□

This is a recurrent pattern. Ergodic theory is often useful. In order to prove something you need a single point which satisfies conditions. Generate some point about which you know nothing and show everything trivializes. 9/20

Let G be a locally compact, σ-compact group, $d : G \times G \to \mathbb{R}$ be a left-invariant metric, and $\Gamma \leq G$ be discrete.

Definition 1.5.5: If m_R is a right-invariant measure on G then

$$m_R(gB) = \text{mod}_G(g)m_R(B) \tag{1.35}$$
$$\text{mod}_G : G \to \mathbb{R}_{>0}. \tag{1.36}$$

is the **modular character**.

Proposition 1.5.6: If G admits a lattice Γ, then $\operatorname{mod}_G \equiv 1$.

We proved this with Poincaré recurrence; here's another proof using dynamics.

Proof. If $\Gamma \subset \ker(\operatorname{mod})$, then we have maps

$$G \to \Gamma \backslash G \to \ker(\operatorname{mod})\backslash G \xrightarrow{\operatorname{mod}} \mathbb{R}_{>0} \tag{1.37}$$

Recall that if we have a measurable map $(X, \mathcal{X}, \mu) \xrightarrow{\pi} (Y, \mathcal{Y})$, the push-forward $\pi_*\mu$ on $(Y, \mathcal{Y})$ is defined by

$$\pi_*\mu(A) = \mu(\pi^{-1}(A)). \tag{1.38}$$

The push-forward of m_* from $\Gamma\backslash G$ to $H\backslash G$, for $H := \ker \operatorname{mod}$, is a G-invariant finite measure. Thus $H\backslash G$ has a finite Haar measure, and $H\backslash G$ is compact.

mod is a continuous homomorphism $H\backslash G \xrightarrow{\operatorname{mod}} \mathbb{R}_{>0}$. m is a finite Haar measure on $H\backslash G$. We have

$$0 < \int_{H\backslash G} \operatorname{mod}(Hg)\, dm(Hg) < \infty \tag{1.39}$$

For all $g \in G$,

$$\frac{1}{N}\sum_{n=0}^{N-1} \operatorname{mod}(g^n) \xrightarrow{N\to\infty} \int \operatorname{mod}\,(\text{some Haar measure}) < \infty \tag{1.40}$$

However, the LHS is a geometric series. If $\operatorname{mod}(g) \neq 1$, then

$$\frac{1}{N}\sum_{n=0}^{N-1} \operatorname{mod}(g^n) = \frac{1}{N}\sum_{n=0}^{N-1} \frac{\operatorname{mod}(g)^N - 1}{\operatorname{mod}(g) - 1}. \tag{1.41}$$

The limit can only be 1, if $\operatorname{mod}(g) = 1$, ∞, if $\operatorname{mod}(g) > 1$, or 0, if $\operatorname{mod}(g) < 1$. $\square$

Here, we didn't need to choose any generic element.

(Even easier: image is compact, so it has to be $\{1\}$.)

How can you check if a sequence of points in a noncompact space diverges? For homogeneous spaces there's a suprising and powerful way.

Let $\Gamma < G$ be discrete.

Definition 1.5.7: Let X be locally compact, σ-compact, then we say that a sequence $\{x_n\}$ diverges , $x_n \to \infty$ as $n \to \infty$, if for every $K \subseteq X$ compact, for all $n \gg_K 1$, $x_n \notin K$.

Proposition 1.5.8: If $\{g_n\} \subseteq \Gamma\backslash G$, Γ a lattice, then $\Gamma g_n \to \infty$ as $n \to \infty$ iff

$$r_{\text{inj}}(g_n) \xrightarrow{n\to\infty} 0, \tag{1.42}$$

iff there exists $\{\gamma_n\} \subseteq \Gamma$ such that $g_n^{-1}\gamma_n g_n \to e$ as $n \to \infty$.

Recall that $\frac{1}{4}\inf_{e\neq\gamma\in\Gamma} d(g^{-1}\gamma g, e) \leq r_{\text{inj}}(g) \leq \inf_{e\neq\gamma\in\Gamma} d(g^{-1}\gamma g, e)$.

Proof. 1. If $\Gamma g_{n_k} \not\to \infty$, then there exists K compact, n_k, $\{\Gamma g_n\} \subseteq K$, such that $r_{\text{inj}}(\Gamma g_{n_k}) \geq r_{\text{inj}}(K) > 0$.

2. If $\Gamma g_n \to \infty$, then by the Cauchy criterion, there exists $r_0 > 0$, for all $n, m > N$, $d(\Gamma g_n, \Gamma g_m) > r_0$. Fix $0 < r < \frac{1}{2}\min\{r_0, \liminf r_{\text{inj}}(\Gamma g_n)\}$. There exist infinitely many $n, m \gg 1$, $\Gamma g_n B_r(e) \cap \Gamma g_m B_r(e) = \phi$. But also $\Gamma g_n B_r(e)$ is injective for all $n \gg 1$. Thus

$$m(\Gamma\backslash G) \geq \sum_{n\gg 1} m(\Gamma g_n B_r(e)) = \sum_{n\gg 1} m_G(g_n B_r(e)) = \infty \cdot m_G(B_r(e)), \tag{1.43}$$

contradiction.

□

Here is an application: orbits of finite subgroups must be closed.

Let $H \circlearrowright X$, $x \in X$. Then there exists a bijection (of sets)

$$\text{Stab}_H(x)\backslash H \xrightarrow{\sim} H.x \tag{1.44}$$

$$\text{Stab}_H(x) \cdot h \mapsto h^{-1}.x. \tag{1.45}$$

Suppose the map $H \times X \to Y$ is continuous. (?) For example, let $\mathbb{R} \circlearrowright \mathbb{Z}^2\backslash\mathbb{R}^2$. Fix $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, and let

$$r_0(t, s) = (t + r, s + \alpha r). \tag{1.46}$$

The orbit of the identity is dense in $\mathbb{Z}^2\backslash\mathbb{R}^2$,

$$\{e\}\backslash\mathbb{R} \to \mathbb{R}.(0, 0). \tag{1.47}$$

Definition 1.5.9: Let $H \circlearrowright X$, $x \in X$. Fix a left Haar measure m_H on H. Define $\text{Vol}(H.x)$ as the volume of a fundamental domain for $\text{Stab}_H(x)$ in H (if it exists).

If $X = \Gamma\backslash G$ and $H < G$ (closed) acts on the right

$$\text{Stab}_H(\Gamma g) = g^{-1}\Gamma g \cap H < H \tag{1.48}$$

is discrete.

Definition 1.5.10: An orbit of $H < G$ (H closed) on $\Gamma\backslash G$ is a **periodic orbit** if it has finite volume.

This implies H is unimodular.

Remark 1.5.11: In order to compare volumes of different closed subgroups, fix a bounded identity neighborhood $e \in B \subseteq G$, and normalize m_H on H so that

$$m_H(H \cap B) = 1. \tag{1.49}$$

If the group is totally disconnected (e.g. p-adic), it has a maximal compact neighborhood. For archimedean groups, there isn't a canonical way to choose the neighborhood.

Proposition 1.5.12: Let $\Gamma \le G$ be a lattice and $H < G$ be closed. If $\Gamma g H$ is a finite volume orbit, then $\Gamma g H$ is closed in $\Gamma\backslash G$ and $g^{-1}\Gamma g \cap H \backslash H \to \Gamma g H$ is proper.

Proof. Notice that for all $h \in H$, $r_{\text{inj}}^H(h) \ge r_{\text{inj}}^G(gh)$, the LHS with respect to $\Gamma_H = g^{-1}\Gamma g \cap H$.

If there exist $b_1, b_2 \in B_r^H(e)$, $g^{-1}\gamma g \in H$, such that $g^{-1}\gamma g h b_1 = g^{-1}\gamma g h b_2$, then $bB_r^H(e)$ is not injective in H. Then $\gamma g h b_1 = \gamma g h b_2$, so it is not injective around gh in G.

1. If $\Gamma g h_n$ is convergent in $\Gamma\backslash G$, then

$$\limsup r_{\text{inj}}^H(h_n) \ge \limsup r_{\text{inj}}^G(gh_n) > 0. \tag{1.50}$$

   Then $\Gamma_H h_n$ is not divergent and has a convergent subsequence.

2. If $\Gamma_H h_n \to \infty$ then $r_{\text{inj}}^G(gh_n) \le r_{\text{inj}}^H(h_n) \to 0$.

□

Definition 1.5.13: A matrix $g \in \mathrm{GL}_n(\mathbb{R})$ is unipotent if there exists $k \in \mathbb{N}$, $(g-e)^K = 0$.

Exercise 1.5.14:

1. (a) Suppose $G < \mathrm{SL}_n(\mathbb{R})$ is a closed subgroup, and $\Gamma < G$ is a lattice, $\Gamma \subseteq \mathrm{SL}_n(\mathbb{Z})$. Then if $\Gamma\backslash G$ is not uniform (co-compact), then Γ contains a unipotent. (Use integral structure of $\mathrm{SL}_n(\mathbb{Z})$. This is true in much greater generality.)

   (b) Show the converse statement ($G = \mathrm{SL}_n(\mathbb{R})$).

2. Let (G, d) be such that d is proper and $\Gamma < G$ be a uniform lattice. Show Γ is finitely generated.

3.

   Definition 1.5.15: For a topological dynamical system (X, H), H a locally compact group with continuous action $H \times X \to H$, suppose X is a locally compact metric space. Say that (X, T) is **transitive** if there exists a dense orbit, **minimal** if every orbit is dense.

   Suppose $\Gamma \le G$ is discrete, and $H \subseteq G$ is closed.

   Show that $\Gamma \circlearrowright G/H$ is transitive (minimal) iff $\Gamma\backslash G \circlearrowleft H$ is transitive (minimal).

6 Modular spaces of Euclidean lattices

Now we talk about specific groups and their lattices.

Any lattice is the $\mathbb{Z}$-span of a basis.

Definition 1.6.1: 1. Let $\mathcal{L}_n$ be the space of all lattices in $\mathbb{R}^n$.

2. A lattice $\Gamma < \mathbb{R}^n$ is unimodular if the volume of $\Gamma\backslash\mathbb{R}^n$ with respect to the Lebesgue measure of $\mathbb{R}^n$ is $= 1$. The volume of $\Gamma\backslash\mathbb{R}^n$ is called the **covolume** of Γ: $\mathrm{Vol}(\Gamma\backslash\mathbb{R}^n) = \mathrm{covol}(\Gamma) > 0$.

3. $\mathcal{L}_n^1$ is the space of unimodular lattices.

Note $\mathrm{GL}_n(\mathbb{R}) \circlearrowleft \mathcal{L}_n$ acts transitively, and $\mathrm{SL}_n(\mathbb{R}) \circlearrowleft \mathcal{L}_n^1$ acts transitively.
$\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{R})}\,\mathbb{Z}^n = \mathrm{GL}_n(\mathbb{Z})$, and $\mathrm{Stab}_{\mathrm{SL}_n(\mathbb{R})}\,\mathbb{Z}^n = \mathrm{SL}_n(\mathbb{Z})$. Note here

$$\mathrm{SL}_n(R) = \{g \in \mathcal{M}_{n\times n}(R) : \det g = 1\} \tag{1.51}$$
$$\mathrm{GL}_n(R) = \left\{g \in \mathcal{M}_{n\times n}(R) : \det g \in R^X\right\}. \tag{1.52}$$

The second set does not look like a polynomial, we can embed it as

$$\{g \in \mathrm{SL}_{n+1}(R) : \forall 1 \le i < n, g_{in} = g_{ni} = 0\} \hookrightarrow \mathrm{SL}_{n+1}(R). \tag{1.53}$$

I.e. embed as $\begin{pmatrix} g & 0 \\ 0 & (\det g)^{-1}\end{pmatrix}$. (This can be cut out by polynomial equations. In contrast, $\mathrm{PSL}_n(R)$ cannot be cut out by poly equations, this has ramifications for math life.) Our objective is to understand $\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R})$ and similar spaces. $\mathrm{SL}_n(\mathbb{Z})$ is discrete; is it a lattice? Yes, but it's not compact. There is a tentacle (cusp) that goes to ∞.

What is the topology you get on $\mathcal{L}_n^1$, $\mathcal{L}_n$? A sequence of lattices $\Lambda_k \to \Lambda$ if for all k, we can write

$$\Lambda_k = \left\langle b_1^k, \dots, b_n^k\right\rangle_{\mathbb{Z}} \tag{1.54}$$
$$\Lambda = \langle b_1, \dots, b_n\rangle_{\mathbb{Z}} \tag{1.55}$$

such that $b_i^k \to b_i$ as $k \to \infty$.

Claim 1.6.2. *$\mathcal{L}_n^1$ is not compact.*

Proof. We construct a sequence that does not converge. Consider

$$\frac{1}{n}\mathbb{Z}e_1 + n\mathbb{Z}e_2 + \langle e_3, \dots, e_n\rangle_{\mathbb{Z}}. \tag{1.56}$$

Then $\Gamma_n \to \infty$.

Consider this in 2 dimensions. If it were to converge to a lattice, it would contain the whole x-axis, and no point with nonzero y. □

Our goal is to prove $\mathrm{SL}_n(\mathbb{Z})$ is a lattice. We need to know a priori that $\mathrm{SL}_n(\mathbb{R})$ is unimodular. One way is to write Haar measure; another is more conceptual.

Theorem 1.6.3. *Any perfect group is unimodular.*

Definition 1.6.4: A group is perfect if $G = [G, G]$.

A perfect group can have no nontrivial homorphisms to abelian groups. To show $\mathrm{SL}_n(\mathbb{R})$ is perfect, we use the following.

Lemma 1.6.5. *For all fields F, define for $1 \le i \ne j \le n$*

$$\mathrm{SL}_n(F) > U_{ij} = \{I + tE_{ij} : t \in F\} \tag{1.57}$$

$\mathrm{SL}_n(F)$ is generated by $\{U_{ij}\}_{1 \le i \ne j \le n}$. Well-known theorem: bounded generation. Can you put bound on length on product? This is false for $n = 2$ and true for $n > 2$. 9-25

$\mathrm{GL}_n(\mathbb{R}) \circlearrowleft \mathcal{L}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{R}) \circlearrowleft \mathcal{L}^1(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{Z}) \backslash \mathrm{SL}_n(\mathbb{R}) \xrightarrow{\sim} \mathcal{L}_n^1(\mathbb{R})$.

We showed that $\mathcal{L}_n^1$ is not compact.

For higher n, there's no known algorithm to compute the shortest vector of a given lattice.

Proposition 1.6.6: Let $\lambda_1 : \mathcal{L}_n^1 \to \mathbb{R}_{>0}$, $\lambda_1(\Lambda) = \min_{0 \ne v \in \Lambda} \|v\|_2$. This function is continuous.

Every primitive vector $v \in \Lambda$ can be completed to a $\mathbb{Z}$-basis of Λ. This is a statement of algebra; a lattice is $\cong \mathbb{Z}^n$, so this follows from theory of abelian groups.

Proposition 1.6.7: $U_{ij}(F)$ generates $\mathrm{SL}_n(F)$.

Corollary 1.6.8. $\mathrm{SL}_n(F) = [\mathrm{SL}_n(F), \mathrm{SL}_n(F)]$. *Hence,* $\mathrm{SL}_n(\mathbb{R})$ *is unimodular.*

Proof. It is enough to show that for all $i \ne j$, $U_{ij} \subseteq D(\mathrm{SL}_n(F))$. Take $a = \mathrm{diag}(a_1, \ldots, a_n)$; then

$$[a, u]_{i,j} = (a^{-1}u^{-1}au)_{i,j} = u_{ij}\left(1 - \frac{a_i}{a_j}\right) \tag{1.58}$$

by appropriate choice of a and u you find any $u \in U_{ij}(F)$ is in $D(\mathrm{SL}_n(F))$. (Diagonal matrices conjugate unipotents.) $\square$

We study the Siegel domain. It was constructed before he was born in the 19th century by 2 Russian mathematicians; he generalized the construction.

7 Iwasawa decomposition

We define some subgroups of $\mathrm{SL}_n(\mathbb{R})$ and see how to get $\mathrm{SL}_n(\mathbb{R})$ from these subgroups. First consider

$$K = \mathrm{SO}_n(\mathbb{R}) < \mathrm{SL}_n(\mathbb{R}), \tag{1.59}$$

the maximal compact subgroup. It acts transitively on the n-dimensional sphere, and is compact by induction (it is an extension of $\mathrm{SO}_{n-1}(\mathbb{R})$). Next, the diagonal matrices and the positive chamber,

$$A = \{\mathrm{diag}(a_1, \ldots, a_n) : \det = 1\} < \mathrm{SL}_n(\mathbb{R}) \tag{1.60}$$

$$A^+ = \left\{\mathrm{diag}(a_1, \ldots, a_n) : \prod_{i=1}^n a_i = 1, \forall i, a_i > 0\right\} \qquad \text{commutative} \tag{1.61}$$

$$N = \left\{\begin{pmatrix} 1 & \cdots & 0 \\ * & \ddots & \vdots \\ * & \cdots & 1 \end{pmatrix}\right\} \qquad \text{nilpotent} \tag{1.62}$$

$$B = NA = \left\{\begin{pmatrix} * & \cdots & 0 \\ * & \ddots & \vdots \\ * & \cdots & * \end{pmatrix}\right\} \tag{1.63}$$

$$B^\circ = NA^+ \tag{1.64}$$

The difference between $n = 2$ and $n > 2$ is a huge source of struggle in life. For $n = 2$, $\mathrm{SO}_n(\mathbb{R})$ is commutative. For $n > 2$ this has a free group inside it! Which is easier? It depends on the question. In many cases the commutative case is more difficult.

Proposition 1.7.1: $\mathrm{SL}_n(\mathbb{R}) = NA^+K$. For all $g \in \mathrm{SL}_n(\mathbb{R})$, there exists $n \in N$, $a \in A^+$, $k \in K$, such that $g = nak$.

Proof. This is the Gram-Schmidt process. Think of G as being n vectors. Given $v_1, \ldots, v_n$, let $v_1^* = v_1$, and $v_2^* = v_2 - \frac{\langle v_1, v_2\rangle}{\langle v_2, v_2\rangle} - v_1$. □

Note here that $a_1 = \|v_i^*\|_2$.

(If you compute something, you probably understand it, at least better than if you can't compute it.)

If a group is composed of 2 unimodular groups, like $B = NA$, then it is not unimodular.

We write down the Haar measure, so we can compute the volume of some specific sets.

Proposition 1.7.2: Suppose $G = ST$, $S \cap T = e$. Then

$$m_G^R \propto \mathrm{mod}_G m_S^L \times m_T^R \tag{1.65}$$

(If it's unimodular, you expect $m_S^L \times m_T^R$ to be the measure. If it's not unimodular, you get a modular character.) The easiest way to prove it is with conditional measures, which we'll introduce later.

Proof. What happens is a fancy version of Fubini.

We have projection $G = ST \xrightarrow{\pi_T} T$, $T \cong S\backslash ST$, $m_G^R \mapsto \pi_T^*.m_G^R$.

We can write

$$m_G^R = \int \mu^t \, d\pi_T^*.m_G^R(t). \tag{1.66}$$

The measure is the same on each fiber up to a constant that varies between fibers. We can move between any fibers by an element of G. □

Proposition 1.7.3: The unimodular character of B° is $\rho : B^\circ \to \mathbb{R}_{>0}$. $\rho(b) = \prod_{i<j} \frac{b_{ii}}{b_{jj}}$.

This is straightforward if we know about Lie groups.

Corollary 1.7.4.

$$m_{B^\circ}^L \propto \rho \cdot m_N \times m_{A^+} \tag{1.67}$$

$$m_{\mathrm{SL}_n(\mathbb{R})} \propto \rho \cdot m_N \times m_{A^+} \times m_K. \tag{1.68}$$

8 Siegel domain

Definition 1.8.1: Let $s, t > 0$. Then define N_s, A_t, and $\Sigma_{s,t}$ by

$$N \supseteq N_s = \left\{ \begin{pmatrix} 1 & \cdots & 0 \\ & \ddots & \vdots \\ (n_i j) & & a_n \end{pmatrix} : |n_{ij}| \leq s \right\}. \tag{1.69}$$

$$A^+ \supseteq A_t = \left\{ \mathrm{diag}(a_1, \dots, a_n) : a_1 > 0, \frac{a_{i+1}}{a_i} > t \forall i < n \right\} \tag{1.70}$$

$$\Sigma_{s,t} = N_s A_t K. \tag{1.71}$$

We have coordinates on A^+:

$$\log_A : A^+ \xrightarrow{\cong} (\mathbb{R}^{n-1}, +) \tag{1.72}$$

$$\mathrm{diag}(a_1, \dots, a_n) \mapsto (t_1, \dots, t_{n-1}) \tag{1.73}$$

$$\underbrace{\log_A(A_t)}_{\subseteq \mathbb{R}^{n-1}} = \left\{ (t_1, \dots, t_{n-1}) : t_i = \log\left(\frac{a_{i+1}}{a_i}\right), t_i > \log t \right\}. \tag{1.74}$$

Theorem 1.8.2. *$\Sigma_{s,t}$ is a surjective set for $\mathrm{SL}_n(\mathbb{Z})$ for all $s \geq \frac{1}{2}$, $t > \frac{\sqrt{3}}{2}$.*

Proof. Use the LLL algorithm.

Definition 1.8.3: 1. A basis for a lattice $g = nak$ is semi-reduced if its N-part n satisfies $n \in N_{\frac{1}{2}}$.

2. A basis $g = nak$ is t-reduced if $a \in A_t$, $g = (v_1, \dots, v_n)$, $\frac{\|v_{i+1}^*\|}{\|v_i^*\|} > t$.

($[-1/2, 1/2)$ is a fundamental domain of $\mathbb{R}$; that's why $1/2$ appears.) The algorithm is as follows.

1. Multiply $g = nak$ on the left by an element of $N(\mathbb{Z})$ such that g is semi-reduced.
2. If g is now t-reduced, finish.
3. If g is not t-reduced, find minimal i such that $\frac{a_{i+1}}{a_i} = \frac{\left\|v_{i+1}^*\right\|}{\left\|v_i^*\right\|} \le t$ and switch order of v_i and v_{i+1}.

We claim the process terminates. Define the capacity of an ordered basis by

$$D(v_1, \dots, v_n) = \prod_{i=1}^n \mathrm{covol}(\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_i) \tag{1.75}$$

$$= \prod_{i=1}^n \|v_i^*\|^{n-i+1}. \tag{1.76}$$

It's easy to see $D(v_1, \dots, v_n) \ge D\Lambda > 0$ where $\Lambda = \mathrm{span}_{\mathbb{Z}}(v_1, \dots, v_n)$, $D = \prod_{i=1}^n D_i$, $D_i = \mathrm{covol}(\mathbb{Z}v_1 + \cdots \mathbb{Z}v_i)$. To see that $D_i(v_1, \dots, v_i)$ has minimum > 0, notice that $\bigwedge^i \Gamma$ is discrete in $\bigwedge^i \Lambda$ is discrete in $\bigwedge^i \mathbb{R}^n$.

We will show that D decays geometrically each iteration. $D_i = \prod_{j=1}^i \left\|v_j^*\right\|$. Assume we have switched v_{i_0} and v_{i_0+1}. Note $D_i^{\mathrm{old}} = D_i^{\mathrm{new}}$ for all $i \ne i_0$. So

$$D^{\mathrm{new}} = D^{\mathrm{old}} \frac{D_{i_0}^{\mathrm{new}}}{D_{i_0}^{\mathrm{old}}} = D^{\mathrm{old}} \frac{\left\|v_{i_0}^{*,\mathrm{new}}\right\|}{v_{i_0}^{*,\mathrm{old}}}. \tag{1.77}$$

So

$$v_{i_0}^{\mathrm{new}} = v_{i_0+1}^{\mathrm{old}} - \frac{\left\langle v_{i_0+1}^{\mathrm{old}}, v_1^{\mathrm{old}}\right\rangle}{\|\cdots\|} v_1^{\mathrm{old}} - \cdots - \frac{\left\langle v_{i_0+1}^{\mathrm{old}}, v_{i_0-1}^{\mathrm{old}}\right\rangle}{\cdots} v_{i_0-1}^{\mathrm{old}} \tag{1.78}$$

$$v_{i_0+1}^{\mathrm{old},*} = v_{i_0}^{\mathrm{new},*} - \underbrace{\frac{\left\langle v_{i_0+1}^{\mathrm{old}}, v_{i_0}^{\mathrm{old}}\right\rangle}{\cdots}}_{|\cdot| \le \frac{1}{2}} v_{i_0}^{\mathrm{old}} \tag{1.79}$$

$$v_{i_0+1}^{\mathrm{new},*} = v_{i_0+1}^{\mathrm{old},*} + \mu v_{i_0}^{\mathrm{old},*}. \tag{1.80}$$

Thus

$$D_{i_0}^{\mathrm{new}} = D_{i_0}^{\mathrm{old}} \sqrt{\frac{\left\|v_{i_0+1}^{\mathrm{old},*} + \mu v_{i_0}^{\mathrm{old},*}\right\|^2}{\left\|v_{i_0+1}^{\mathrm{new},*}\right\|}} \tag{1.81}$$

$$\le D_{i_0}^{\mathrm{old}} \sqrt{t^2 + \frac{1}{2}} < D_{i_0}^{\mathrm{old}}. \tag{1.82}$$

□

How big is the Siegel set in the fundamental domain? On calculating the volume: This was the first important use of trace formula. The volume of the Siegel domain is $\exp(\mathrm{poly}(\mathrm{Vol}(\mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{SL}_n(\mathbb{R}))))$. You need Eisenstein series structure for this.

Exercise 1.8.4: Calculate that $\mathrm{Vol}(\Sigma_{s,t}) < \infty$. (Use $\log_A$ coordinate and modular character of B.

9-27

We need one general fact before we dive deeper.

$\mathcal{L}_1^n$ is not compact.

Lemma 1.8.5 (Mahler compactness criterion)**.** *For $\sigma > 0$ define $\mathcal{L}_n^1(\sigma) = \{\Lambda \in \mathcal{L}_n^1 : \lambda_1(\Lambda) \geq \delta\}$. Then for all $\delta > 0$, $\mathcal{L}_n^1(\delta)$ and for all $K \subseteq \mathcal{L}_n^1$ compact there exists $\delta_K > 0$ such that $K \subseteq \mathcal{L}_n^1(\delta)$.*

Proof. λ_1 is continuous, so restricted to a compact set K it attains minimum δ_K, so $K \subseteq \mathcal{L}_n^1(\delta_K)$.

If $\Lambda \in \mathcal{L}_n^1(\delta)$, let $0 \neq v_1 \in \Lambda$ be a vector of minimal length, and write $\Lambda = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$. This basis can be reduced using the LLL algorithm to a basis $v_1^*, \ldots, v_n^*$, $v_1 = v_1^*$.

We know that $a_1 = \|v_1^*\| \geq \delta$, $a_2 = \|v_2^*\| \geq t\|v_1^*\| = t\delta$, and so on, $a_n = \|v_n^*\| \geq t^{n-1}\delta$. We also know $\prod_{i=1}^n \|v_i^*\| = 1$ because the lattice is unimodular.

Then

$$\frac{1}{\prod_{i>1}\|v_i^*\|} \geq \|v_1^*\| \geq \delta \tag{1.83}$$

$$\frac{1}{\prod_{i\neq 2}\|v_i^*\|} \geq \|v_2^*\| \qquad \geq td \tag{1.84}$$

so each one of the diagonal entries is inside a closed interval, so it is a compact set. $\square$

From sticking other groups in $\mathrm{SL}_n(\mathbb{R})$ you can learn things about then. See e.g. the Borel-Harish-Chandra theorem. If you want to prove the class group is finite, use the geometry of numbers.

9 $\mathrm{SL}_2(\mathbb{R})$ and hyperbolic plane

We discuss the relation of $\mathrm{SL}_2(\mathbb{R})$ to hyperbolic geometry.

$\mathrm{SL}_2(\mathbb{R})$ is special. There are some infinite sequence of algebraic groups which are simple. Special linear group, orthogonal groups, symplectic groups, and not much beyond that. It is a special linear group, symplectic group, and group preserving a quadratic form. This collision of different properties makes it special.

Let $\mathbb{H} = \{z \in \mathbb{C} : \Re z > 0\}$.

There is a nice action of $\mathrm{GL}_2(\mathbb{C})$ on $\hat{\mathbb{C}}$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}. \tag{1.85}$$

It is 2-transitive. There is an action of $\mathrm{SL}_2(\mathbb{R}) \circlearrowright \mathbb{H}$. Consider the tangent space $T\mathbb{H} = \mathbb{H}\times\mathbb{C}$. Give $\mathbb{H}$ a Riemann metric by giving each point of the tangent space an inner product: for $z \in \mathbb{H}$, $u, v \in \mathbb{C} \cong \{z\} \times \mathbb{C}$, define

$$\langle u, v\rangle_z = \frac{\langle u, v\rangle}{(\Im z)^2} \tag{1.86}$$

The curvature is constant -1. This is the unique hyperbolic plane.

We have actions $\mathrm{SL}_2(\mathbb{R}) \circlearrowright \mathbb{H}$ by isometries and $\mathrm{SL}_2(\mathbb{R}) \circlearrowright T\mathbb{H}$ by differentiation (?):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.(z, u) = \left(\frac{az+b}{cz+d}, \frac{u}{(cz+d)^2}\right). \tag{1.87}$$

The action of $\mathrm{SL}_2(\mathbb{R}) \circlearrowright \mathbb{H}$ is not faithful, $-I$ doesn't doesn't do anything.

Definition 1.9.1: Let R be a commutative ring. Define $\mathrm{PSL}_2(R) = Z(\mathrm{SL}_2(R))\backslash \mathrm{SL}_2(R)$.

Note that $Z(\mathrm{SL}_2(\mathbb{R})) = \pm e = \mu_2$.

Exercise 1.9.2: No algebraic group represents PSL_2. (Check what happens over an algebraically closed field and compare with PGL_2.)

We know $\mathrm{PSL}_2 \circlearrowright \mathbb{H}$ acts transitively. The stabilizer of i is $\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{R})}\, i = \mathrm{PSO}_2(\mathbb{R})$. Thus

$$\mathrm{SL}_2(\mathbb{R})/\,\mathrm{SO}_2(\mathbb{R}) \xrightarrow{\cong} \mathrm{PSL}_2(\mathbb{R})/\mathrm{PSO}_2(\mathbb{R}) \xrightarrow{\cong} \mathbb{H}. \tag{1.88}$$

The unit tangent bundle is $T^1\mathbb{H} = \{(z, u) : \langle u, u\rangle_z = 1\}$. Then $\mathrm{SL}_2(\mathbb{R}) \circlearrowright T^1\mathbb{H}$ simply transitively.

Topologically, $T^1\mathbb{H}$ is contractible to circle around a point, seen using Iwasawa decomposition.

The boundary of the upper half plane is line and point at infinity; that they seem disconnected is artificial.

The geodesics are vertical lines and semicircles perpendicular to $\mathbb{R}$. It's easy to show a vertical line is a geodesic. There is a unique geodesic between every two points; you can move the line to any other geodesic.

There is a geodesic flow $\mathbb{R} \circlearrowright T^n\mathbb{H}$. For all $(z, u) \in T^1\mathbb{H}$, there exists a unit speed geodesic $\gamma : \mathbb{R} \to \mathbb{H}$, such that $\gamma(0) = z$ and $d\gamma|_0 = u$.

Proposition 1.9.3: The geodesic flow coincides with the action of $A_+ < \mathrm{SL}_2(\mathbb{R})$, the group of diagonal matrices $A_T = \left\{\begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} : \lambda > 0\right\}$. Specifically, the time t flow is $\begin{pmatrix} e^{\frac{t}{2}} & \\ & e^{-\frac{t}{2}} \end{pmatrix}$.

Take a point on the real line; there are infinitely many geodesics coming out of it. Going towards the point, the distance decays exponentially with the flow. On the other side the distance grows exponentially. This is typical hyperbolic behavior, also responsible for interesting dynamics.

The $\mathrm{SL}_2(\mathbb{R})$ invariant measure on $\mathbb{H}$ is $\frac{dx\,dy}{y^2}$, for $z = x + iy$.

10 Horospherical groups

This is a completely general phenomenon.

Definition 1.10.1: Let G be locally compact and σ-compact. Define G_a^-, the **stable horospherical subgroup**,

$$G > G_a^- = \left\{ g \in G : \lim_{n\to\infty} a^n g a^{-n} = e \right\}. \tag{1.89}$$

The **unstable horospherical subgroup** is

$$G > G_a^+ = G_{a^{-1}}^- \tag{1.90}$$

Also define the parablic subgroups

$$P_a^- = \left\{ g \in G : \lim_{n\to\infty} a^n g a^{-n} \text{ exists} \right\} \tag{1.91}$$

$$P_a^+ = P_{a^{-1}}^-. \tag{1.92}$$

If G is abelian, this is just the whole group. If G is compact, also nothing exciting can happen. The group is too simple. The noncommutativity of isometries over hyperbolic space makes things interesting.

Why are these groups relevant? Let $\Gamma \subseteq G$ be closed. Let $u \in G_a^-$. Then for all $x = \Gamma g \in \Gamma \backslash G$, $d(a^n.x, a^n.ux) \to 0$ as $n \to \infty$. To see this, note

$$d(a^n.x, a^n.(u.x)) = d(\Gamma g a^{-n}, \Gamma g u^{-1} a^{-n}) \tag{1.93}$$

$$\leq d(a^{-n}, u^{-1}a^{-n}) \tag{1.94}$$

$$= d(a^n u a^{-n}, e) \xrightarrow{n\to\infty} 0 \tag{1.95}$$

What happens over $\mathrm{SL}_2(\mathbb{R})$? Take $a \in A^+$, $a = \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix}$. Then

$$\begin{pmatrix} \lambda^n & \\ & \lambda^{-n} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda^{-n} & \\ & \lambda^n \end{pmatrix} = \begin{pmatrix} a & \lambda^{2n} b \\ \lambda^{-2c} c & d \end{pmatrix}. \tag{1.96}$$

So for $\lambda > 1$,

$$G_a^- = \left\{ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\} \qquad P_a^- = \left\{ \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \right\} \tag{1.97}$$

$$G_a^+ = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} \qquad P_a^+ = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}. \tag{1.98}$$

Orbits of U are called horocycles. They are

1. horizontal lines
2. circles tangent to $\mathbb{R}$.

They are perpendicular to corresponding geodesics.

11 Fundamental domain for $\mathrm{SL}_2(\mathbb{Z}) \circlearrowright \mathbb{H}$

This is a set $\mathcal{F} \subset \mathbb{H}$ such that $\mathbb{H} = \bigsqcup_{\gamma \in \mathrm{PSL}_2(\mathbb{Z})} \gamma.\mathcal{F}$. One way to prove $\mathcal{F}$ is to look at the action under generators—one is inversion, one is translation. It's a classical calculation of 19th century mathematics. It has no way of working for $\mathrm{SL}_{57}(\mathbb{R})$.

The fundamental domain is

$$\mathcal{F}^\circ = \left\{ z \in \mathbb{H} : -\frac{1}{2} < \Re z < \frac{1}{2}, |z| > 1 \right\} \tag{1.99}$$

$$\mathcal{F} = \mathcal{F}^\circ \cup \text{part of boundary} \tag{1.100}$$

Consider the geodesic that is a vertical line at i; it goes to infinity. Most geodesics are dense. Many aren't; their closure can be weird. But a the closure of a horocyle can only be everything or periodic. If the closure is everything, in the limit it will be equidistributed.

How quickly do closed horocycles equidistribute? Finding the correct rate is equivalent to the Riemann hypothesis. We'll discuss the Margulis mixing argument, quantitative nondivergence. Just by understanding how the Haar measure behaves under G, we can understand equidistribution of horocycles; this doesn't work of other groups.

12 Measurable dynamical systems

The systems we are interested in will always be $(\Gamma \backslash G, \mu) \circlearrowleft H$, where $H \leq G$ is closed.

Definition 1.12.1:

1. An action $G \circlearrowright (X, \chi, \mu)$, where G is locally compact and χ is a probability space (σ-algebra), is measure-preserving if

$$\forall g \in G, \quad \forall A \in \chi : \quad \mu(g^{-1}.A) = \mu(A) \tag{1.101}$$

(A good example: G with Haar measure. The quality of being measure-preserving descends to subgroups.)

2. A measure-preserving $G \circ (X, \mu)$ is **ergodic** if any measurable set A satisfying $\mu(g^{-1}.A \triangle A) = 0$ for all $g \in G$, then $\mu(A) = 0$ or $\mu(X \backslash A) = 0$.

3. A measure-preserving action $G \circlearrowright (X, \mu)$ is **mixing** if for all A, B measurable and any $g_n \to \infty$ in G,

$$\mu((g_n^{-1}.A) \cap B) \xrightarrow{n \to \infty} \mu(A)\mu(B). \tag{1.102}$$

(If you move far away from the action, it becomes independent.)

Mixing implies ergodicity: Take A G-invariant; then because applying g many times you get $\mu(A)^2 = \mu(A)$.

Being weakly invariant under a subgroup is a weaker condition. Ergodicity does not descend to subgroups; mixing does. To show ergodic for a subgroup, you can prove mixing for a larger group.

13 Koopman representation

Let $G \circlearrowleft (X, \chi, \mu)$ be a measure-preserving map. There is a unitary representation of G,

$$U : G \to U(L^2(X, \mu)) \tag{1.103}$$
$$U_g(f) = f(g^{-1}.x) \tag{1.104}$$

continuous if $G \times X \to X$ is continuous. It preserves the inner product because it is measure-preserving.

Remark 1.13.1: 1. $G \circlearrowleft X$ is ergodic iff the only eigenfunctions of G in $L^2(X, \mu)$ with eigenvalue 1 is $\mathbb{C} \cdot 1$.

This is a fancy way of saying: for all $f \in L^2(X, \mu)$, $G \circ f = f$ implies $f \in \mathbb{C} \times 1$.

2. $G \circlearrowleft X$ is mixing if $\forall f, g \in L^2(X, \mu)$, for all $g_n \to \infty$,

$$\langle U_{g_n} f, g\rangle \xrightarrow{n\to\infty} \int f\, d\mu \int g\, d\mu. \tag{1.105}$$

Exercise 1.13.2: Let $\mathbb{T}^d = \mathbb{Z}^d \backslash \mathbb{R}^d$ with the Lebesgue measure. Let $\mu \in \mathrm{GL}_d(\mathbb{Z})$ be hyperbolic (no eigenvalues of modulus 1).

$\mathbb{Z}$ acts on $\mathbb{T}^d$ by M^n, $(v + \mathbb{Z}^d)$. Show that this action is mixing, in fact exponentially mixing,

$$|\langle M^n f, g\rangle - \int f \int g| \ll_{f,g} e^{-\alpha n} \tag{1.106}$$

(Use Fourier analysis.)

Fix $\alpha \in \mathbb{R}^d$, then $\mathbb{Z} \circlearrowleft \mathbb{T}^d$ by translations. Show this is not mixing.

10-2

14 Conditional expectation and the ergodic theorem

Mixing implies ergodicity, but the converse is false: irrational rotation on torus is ergodic but not mixing.

Today we prove this theorem.

Theorem 1.14.1. *Let $\Gamma \leq G$ be a lattice, $a \in G$ such that $G = \langle G_a^-, G_a^+\rangle$. Assume $a \circlearrowleft \Gamma\backslash G$ is mixing for the Haar measure and that $\Gamma\backslash G$ is compact. Then the Haar measure m is the unique G_a^--invariant measure on $\Gamma\backslash G$.*

For $\mathrm{SL}_2(\mathbb{R})$ take a to be the diagonal matrix, so G_a^- is the group of unipotent matrices. Every diagonal matrix acts mixingly on $\Gamma\backslash \mathrm{SL}_n(\mathbb{R})$.

The rate of mixing is exponential.

Recall that $a \circlearrowright \Gamma\backslash G$ is mixing for the Haar measure if for all $f, g \in L^2(\Gamma\backslash G, m)$,

$$\langle a^n f, g\rangle \to \int f \int g \tag{1.107}$$

for $n \to \infty$. Recall that $G > G_a^- = \{a \in G : \lim_{n\to\infty} a^n u a^{-n} = e\}$.

We will establish something much stronger, when $\Gamma\backslash G$ is noncompact. We will characterize all invariant measures. For each point, describe orbit closure of horospherical orbit.

Note a^{-1} also acts mixing. Thus the theorem is true for both G_a^- and G_a^+.

I'll talk about conditional expectation, a simple operator often forgotten by people who don't do probability.

Definition 1.14.2: Let $(X, \mathcal{A}, \mu)$ be a probability space and $\mathcal{B} \subseteq \mathcal{A}$ be a sub-σ-algebra. (To be measurable with a smaller class is a more restrictive condition. If we have $(X, ,\mu) \xrightarrow{\pi} (Y, \mathcal{Y})$ we can push-forward and pull-back. Pull-back gives a sub-σ-algebra. When is a function measurable with respect to it? f is measurable with respect to $\pi^{-1}(\mathcal{Y})$ iff there exists measurable $f' : Y \to \mathbb{C}$ such that $f = \pi \circ f'$. All probability theory is encoded in σ-algebra; points are meaningless.)

$$\begin{tikzcd} & (X, \mathcal{A}, \mu) \arrow[dl] \arrow[d, "\pi"] \\ \mathbb{C} & (Y, \mathcal{Y}). \arrow[l] \end{tikzcd} \tag{1.108}$$

Then there is a unique linear operator of norm one

$$\mathbb{E}(\bullet|\mathcal{B}) : = L^1(X, \mathcal{A}, \mu) \to L^1(X, \mathcal{B}, \mu) \tag{1.109}$$

such that the following property is satisfied:

$$\forall B \in \mathcal{B} : \qquad \int_B f \, d\mu = \int_B \mathbb{E}[f|\mathcal{B}] \, d\mu. \tag{1.110}$$

Example 1.14.3:

1. If $\mathcal{B} = \{\phi, X\}$, then $\mathbb{E}[f|\mathcal{B}]$ is the constant function equal to the integral:

$$\mathbb{E}[f|\mathcal{B}] = \int f \, d\mu. \tag{1.111}$$

2. If $\mathcal{B} = \mathcal{A}$, then $f \mapsto \mathbb{E}[f|\mathcal{B}]$ is the identity operator:

$$\mathbb{E}[f|\mathcal{B}] = f. \tag{1.112}$$

3. Consider the unit square. Let $X = [0,1]^2$ and m be the Lebesgue measure. Let $\mathcal{B}$ be the Borel σ-algebra. Let $Y = [0,1]$. Then $\pi(x,y) = x$ and

$$\begin{aligned} \mathcal{B} &= \pi^{-1}\left(\text{Borel } \sigma \text{ algebra on } [0,1]\right) && (1.113)\\ &= \mathcal{B}_{[0,1]} \times \{\phi, [0,1]\}. && (1.114) \end{aligned}$$

$\mathbb{E}[f|\mathcal{B}]$ must be constant on y-fibers, so

$$\mathbb{E}[f|\mathcal{B}](x,y) = \int_0^1 f(x,z)\,dz \tag{1.115}$$

There is something interesting going on because it's an integral over a set of measure 0 in the original measure.

(You can think of the integral as the limit over a set shrinking to a set of measure 0.)

The construction is as follows.

1. $\mathbb{E}[\bullet|\mathcal{B}] : L^2(X,\mathcal{A},\mu) \to L^2(X,\mathcal{B},\mu)$ can be defined as the orthogonal projection on $L^2(X,\mathcal{B},\mu) < L^2(X,\mathcal{A},\mu)$ (a closed subspace).
2. To construct on L^1, we can either use some completion argument, or use the Radon-Nikodym derivative,

$$\mathbb{E}[f|\mathcal{B}] = \frac{(f\,d\mu)_{\mathcal{B}}}{(d\mu)_{\mathcal{B}}}. \tag{1.116}$$

Proposition 1.14.4: 1. $\mathbb{E}[\bullet|\mathcal{B}]$ is a linear operator of norm 1.

2. $\forall g \in L^\infty(X,\mathcal{B},\mu)$, $\mathbb{E}[fg|\mathcal{B}] = g\mathbb{E}[f|\mathcal{B}]$.
3. If $\mathcal{B}' \subseteq \mathcal{B}$ is a sub-σ-algebra, then

$$\mathbb{E}[\mathbb{E}[\bullet|\mathcal{B}]|\mathcal{B}'] = \mathbb{E}[\bullet|\mathcal{B}']. \tag{1.117}$$

4. $\mathbb{E}[\bullet|\mathcal{B}]$ is positive: if $f \geq 0$ then $\mathbb{E}[\bullet|\mathcal{B}] \geq 0$.
5. If $f \in L^1(X,\mathcal{B},\mu)$ then $\mathbb{E}[f|\mathcal{B}] = f$.
6. (Triangle inequality) $|\mathbb{E}[f|\mathcal{B}]| \leq \mathbb{E}[|f||\mathcal{B}]$.

Let's say $G \circlearrowright (X,\mathcal{A},\mu)$. Then we can define $\mathcal{E} \subseteq \mathcal{A}$ as the sub-σ-algebra of G-invariant sets.

We say that $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{A}$ are equivalent up to μ, $\mathcal{B}_1 \overset{\mu}{\equiv}$ if for all $B \in \mathcal{B}_i$, there exists $B' \in \mathcal{B}_j$ $(i \neq j)$ such that $\mu(B \triangle B') = 0$. Then $G \circlearrowright (X,\mu)$ is ergodic iff

$$\mathcal{E} \overset{\mu}{\equiv} \{\phi, X\}. \tag{1.118}$$

Theorem 1.14.5 (Ergodic theorem)**.** *Let $G = \mathbb{R}^d$, $\mathbb{Z}^d \circlearrowright (X, \mu)$. Fix $f \in L^1(X, \mu)$. Then*

1. *For $G = \mathbb{R}^d$, $d\,Vol(g)$ the Haar measure on $\mathbb{R}^d$,*

$$\frac{1}{Vol(B_0(r))} \int_{B_0(r)} f(g, x)\, d\,Vol(g) \xrightarrow{r \to \infty} \mathbb{E}[f|\mathcal{E}](x). \tag{1.119}$$

2. *For $G = \mathbb{Z}$,*

$$\frac{1}{N} \sum_{n=0}^{N-1} f(g^n.x) \xrightarrow{N \to \infty} \mathbb{E}[f|\mathcal{E}](x) \tag{1.120}$$

where the convergence is in L^1 and μ-a.e.

In many cases it's nontrivial that there even exists 1 point where we have converges. If the function is ergodic, then we just get the integral over the whole space.

It is easy to see that if G converges, then $\mathbb{E}[f|\mathcal{E}]$ is the only possible limit, by Fubini's Theorem.

Remark 1.14.6: 1. For $B_0(r)$ one can take balls with respect to any norm on $\mathbb{R}^d$.

2. The set of points where the ergodic theorem holds depends on f. This is important!

f doesn't have to be continuous, just measurable. We often apply to continuous functions.

G must at least be amenable. Ergodic theory is geometric property of the group and not the action. Roughly, $\mathbb{R}^d$ being amenable means the following. In $\mathbb{R}^d$, if you take 2 consecutive balls of close enough radius, the difference in the volume between them is small compared to each one of them. You can choose a sequence of balls such that the difference between consecutive sets has small volume. You can cover the group with sets with small boundary. (This is not true for free groups. Another example is $\mathrm{SL}_2(\mathbb{R})$. Act on the projective space in measure-preserving way. There is no ergodic theorem. There's a big tree/free group standing in $\mathrm{SL}_2(\mathbb{R})$. Hyperbolic spaces are similar to trees. Amenability is specific to some groups.)

I want to connect the threads.

In order for Theorem 1.14.1 to be non-vacuous, we need group elements in $\Gamma\backslash G$ to be mixing in the Haar measure. This is closely related to representation theory. Spectral properties of unitary representation.

15 Mautner phenomenon

Lemma 1.15.1. *Let $G \to \mathcal{U}(H)$ be a unitary representation on a Hilbert space H_0. Fix $L \leq G$ a subgroup and assume $v_0 \in H$ is L-invariant.*

Then if $G \ni g_n \to e$ as $n \to \infty$, $\{\ell_n\}, \{\ell'_n\} \subseteq L$ such that $\ell_n g_n \ell'_n \xrightarrow{n \to \infty} h \in G$, then $h.v_0 = v_0$.

Usualy we apply this to conjugation by a power.

Proof.

$$\|h.v_0 - v_0\| = \lim_{n\to\infty} \|\ell_n g_n \ell'_n.v_0 - v_0\| = \lim_{n\to\infty} \|\ell_n g_n.v_0 - v_0\| \tag{1.121}$$

$$= \lim_{n\to\infty} g_n.v_0 - \ell_n^{-1}.v_0 = \lim_{n\to\infty} \|g_n.v_0 - v_0\| = 0 \tag{1.122}$$

because $g_n \to e$. □

If g generates a bounded subgroup, the action of g cannot be mixing.

Lemma 1.15.2 (Mautner phenomenon for $\mathrm{SL}_2(\mathbb{R})$)**.** *For every $g \in \mathrm{SL}_2(\mathbb{R})$, either g or $-g$ is conjugate to a matrix from A^+, N or K, dependin on whether $|\operatorname{Tr} g| > 2$, $|\operatorname{Tr} g| = 2$, or $|\operatorname{Tr} g| < 2$.*

(A matrix with 2 real eigenvalues is conjugate to a diagonal matrix.)

Theorem 1.15.3. *Let $G = \mathrm{SL}_2(\mathbb{R}) \to \mathcal{U}(H)$. Fix $g \in G$, with powers unbounded. If $v_0 \in H$ satisfies $g.v_0 = v_0$, then $G.v_0 = v_0$.*

Corollary 1.15.4. *For any lattice $\Gamma < G = \mathrm{SL}_2(\mathbb{R})$, the action of $g \circlearrowright (\Gamma\backslash G, m)$ is ergodic.*

Proof. We can conjugate g to be diagonal (in A^+) or unipotent (in N).

1. Let $g = \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} \in A^+$, WLOG $\lambda > 0$. We apply the lemma for all $t \in \mathbb{R}$

$$a^n \begin{pmatrix} 1 & \frac{t}{\lambda^{2n}} \\ 0 & 1 \end{pmatrix} a^{-n} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \tag{1.123}$$

$$\ell_n = a_n,\ \ell'_n = a^{-n},\ L = \langle a \rangle \tag{1.124}$$

$$e_n \leftarrow g_n = \begin{pmatrix} 1 & \frac{t}{\lambda^{2n}} \\ 0 & 1 \end{pmatrix}. \tag{1.125}$$

The lemma implies that k is $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$-invariant for every $t \in \mathbb{R}$. Similar calculations show that it is $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$-invariant.

2. Let $g = u = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$. Let $\lambda_n \to 1$.

$$u^n \underbrace{\begin{pmatrix} \lambda_n & \\ & \lambda_n^{-1} \end{pmatrix}}_{g_n} u^{-n} = g_n.(g_n^{-1} u^n g_n).u^{-n} \tag{1.126}$$

$$= g_n \begin{pmatrix} 1 & nt\lambda_n^{-2} - nt \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda_n & \lambda_n(nt\lambda_n^{-2} - nt) \\ & \lambda_n^{-1} \end{pmatrix} \tag{1.127}$$

we want $\lambda_n \to 1$ and $nt\left(\frac{1}{\lambda_n^2} - 1\right) \xrightarrow{n\to\infty} s$, $0 \neq s \in \mathbb{R}$. A good choice for λ_n is

$$\lambda_n^{-2} = 1 + \frac{s}{nt} \tag{1.128}$$

$$\Leftarrow \lambda_n = \frac{1}{\sqrt{1+\frac{s}{nt}}} \xrightarrow{n\to\infty} 1. \tag{1.129}$$

This is a good choice for the lemma. We know that v_0 is $U^+ = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Set $H > H_0 = \{v \in H : U^+.v = v\}$, a closed subspace. We know $v_0 \in H_0$. For all $u, v \in H_0$, define $f : G \to \mathbb{C}$ continuous by $f(g) = \langle g.v_1, v_2 \rangle$.

f is a continuous function on $U^+\backslash G/U^+$, iff f is U^+-invariant function on G/U^+. Let $G = \mathrm{SL}_2(\mathbb{R})$ act transitively on $\mathbb{R}^2\backslash 0$. The stabilizer of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is U^+. So $G/U^+ \cong \mathbb{R}^2\backslash 0$, f is a U^+-invariant function on $\mathbb{R}^2\backslash 0$.

(The x-axis moves nowhere. Any other axis moves with some speed. The function is constant on horizontal lines. This means it must be continuous on the x-axis too by continuity.)

A continuous U^+-function on $\mathbb{R}^2\backslash 0$ must be constant on the x-axis. So f is constant on A, which implies that for all $v_1, v_2 \in H_0$, $\langle a.v_1, v_2 \rangle = \langle v_1, v_2 \rangle$, or equivalently for all $a \in A$, $\langle a.v_1 - v_1, v_2 \rangle = 0$. So $a.v_1 = v_1$.

□

Exercise 1.15.5: Prove the analogous statement for $\mathrm{SL}_2(\mathbb{Q}_p)$:

- If g is conjugate to a diagonal matrix then the same result holds.
- The unipotent case is different because no unipotent element can generate an unbounded group ($\begin{pmatrix} 1 & t \in \mathbb{Z} \\ 0 & 1 \end{pmatrix}$ is bounded in $\mathbb{Q}_p$). Here the analogous statement is: every $v_0 \in H$ invariant under a 1-parameter unipotent subgroup $\left\{\begin{pmatrix} 1 & t \in \mathbb{Q}_p \\ 0 & 1 \end{pmatrix}\right\}$ is G-invariant.

10-4

Recap: There exists $u \in U$, $u.v_0 = v_0$. Then $U.v_0 = v_0$. Let $H_0 < H$ be the subspace of U-invariant vectors. For $v_1, v_2 \in H_0$, consider $f(g) = \langle g.v_1, v_2 \rangle$, $f : U\backslash G/U \to \mathbb{C}$ continuous. Then $G/U \cong \mathbb{R}^2\backslash 0$, and f is a function on the punctured plane, $f : \mathbb{R}^2\backslash 0 \to \mathbb{C}$. The function must be constant on the diagonal subgroup: for all $a \in A^+$, $\langle a.v_1, v_2 \rangle = \langle v_1, v_2 \rangle$. So $a.v_1 = v_1$.

Definition 1.15.6: Let R be a commutative ring. Then a linear algebraic group $\mathbb{G}$ defined over R is a functor $\mathrm{Alg}_R \to \mathrm{Grp}$ (i.e., if A/R algebra, $\mathbb{G}(A)$ is a group) such that there is an ideal $I \subseteq R[t_{ij}]_{1\le i,j\le n}$ such that there is an ideal $I \subseteq R[t_{ij}]_{1\le i,j\le n}$ so $\mathbb{G}(A) = \{g \in \mathrm{SL}_n(A) : p(g) = 0\,\forall p \in I\}$.

Example 1.15.7: Examples include SL_d, GL_d, $\mathrm{PGL}_d(A) = Z_{\mathrm{GL}_d}(A)\backslash \mathrm{GL}_d(A)$. To see GL_d is an algebraic group, consider $\mathrm{GL}_d \hookrightarrow \mathrm{SL}_{d+1}$ by adding a diagonal entry $\det(A)^{-1}$. To see PGL_d is an algebraic group, take $\mathrm{PGL}_d \hookrightarrow \mathrm{GL}(\mathcal{M}_{d\times d})$ acting by conjugation.

For Q a quadratic form over R, $O(Q)$ and $\mathrm{SO}(Q)$ are algebraic groups (linear transformations preserving Q, and those with determinant 1).

Also, $\mathbb{G}_a(A) = (A, +)$ and $\mathbb{G}_m(A) = \left\{\begin{pmatrix} a & \\ & a^{-1}\end{pmatrix} : a \in A^+\right\}$ are linear algebraic groups.

Also, $\mathrm{SL}_2 \ltimes \mathbb{G}_a^2$ given by $\begin{pmatrix} g & & v \\ & & \vdots \\ 0 & 0 & 1\end{pmatrix}$.

Definition 1.15.8: Let $\mathbb{G}/\mathbb{R}$ is a linear algebraic group, and A/R an algebra.

1. $g \in \mathbb{G}(A)$ is **diagonal** over A if $g \in \mathbb{G}(A) \hookrightarrow \mathrm{SL}_n(A)$ is conjugate in $\mathrm{SL}_n(A)$ to a diagonal matrix. Let $g \in \mathbb{G}(A)$ is **semisimple** if it is diagonalizable in $\mathbb{G}(B)$ for B/A. (If A is a field, it is enough to check the algebraic closure$B = A^{\mathrm{alg}}$.)[1]

2. $g \in \mathbb{G}(A)$ is **unipotent** if $g - e$ is nilpotent in $\mathcal{M}_{n\times n}(A)$, $G \hookrightarrow \mathrm{SL}_n \hookrightarrow \mathcal{M}_{n\times n}$.

Definition 1.15.9: Let $G = \mathbb{G}(\mathbb{R})$, and $\mathbb{G}$ be a linear algebraic group over $\mathbb{R}$. Then G is a **simple Lie group** if it is non-abelian and has no non-trivial connected closed normal subgroups.

Remark 1.15.10: G has a finite center because it is linear. The fundamental group of $\mathrm{SL}_2(\mathbb{R})$ is $\mathbb{Z}$.

Definition 1.15.11: $G = \mathbb{G}(\mathbb{R})$, is a **semi-simple** linear group if there exists $G_1, \ldots, G_r \lhd G$ connected normal subgroups, pairwise commuting $[G_i, G_j] = e$, $G = G_1 \cdot \cdots \cdot G_r$, and the homomorphism

$$\varphi : G_1 \times \cdots \times G_r \to G \tag{1.130}$$

has kernel $\ker\varphi$ that is a finite central group, and each G_i is simple.

15.1 Mautner phenomenon for simple Lie groups

Theorem 1.15.12. *Let $G = \mathbb{G}(\mathbb{R})$ be a simple linear Lie group and $g \in G$ such $g^n \to \infty$. Let $G \to \mathcal{U}(H)$ and $v_0 \in H$ be g-invariant. Then $G.v_0 = v_0$.*

Proof sketch. 1. Using the Jordan normal form, reduce to the case that either g is semisimple or unipotent.

[1] This has nothing to do with elements being semisimple.

2. If $g = a$ is semi-simple, then v_0 is invariant under G_a^- and G_a^+, and $\langle G_a^-, G_a^+, a\rangle = G$. For $u \in G_0$, $a^n u a^{-n} \to e$,

$$\|u.v_0 - v_0\| = \left\|a^n u a^{-n}.v_0 - v_0\right\| \xrightarrow{n\to\infty} 0. \tag{1.131}$$

3. The Jacobson-Morozov Theorem says that if $g = n \in G$ is unipotent, then there is a homomorphism $\varphi : \mathrm{SL}_2(\mathbb{R}) \to G$, such that $\varphi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = n$. The $\mathrm{SL}_2(\mathbb{R})$ case implies that v_0 is invariant under a diagonal element.

□

Corollary 1.15.13. *If $\Gamma < G$ is a lattice, and G is as above, $g \in G$ with $g^n \to \infty$, then $g \circlearrowright (\Gamma\backslash G, m)$ is ergodic.*

Theorem 1.15.14 (Howe-Moore)**.** *Let $G = \mathbb{G}(\mathbb{R})$ be semisimple, $G \to \mathcal{U}(H)$. Fix $\{g_n\} \subset G$. If either*

1. *$G = G_1 \cdots G_r$, where G_i are the simple factors, and for any non-compact G_i there is no non-nontrivial fixed vector in H and $g_n \to \infty$.*

2. *$g_n = g_n^{(1)} \cdots g_n^{(r)}$; for all i, $g_n^{(i)} \in G_i$ and assume $g_n^{(i)} \to \infty$ for every G_i non-compact. Let $G_d = \prod_{G_i \text{ non-compact}} \lhd G$. Assume there is no non-trivial G_d-fixed vector.*

Then for all $v_1, v_2 \in H$, $\langle g_n.v_1, v_2\rangle \to \infty$ as $n \to \infty$.

In each option there are 2 conditions: one about the sequence going to ∞, and one about the lack of fixed vectors.

The proof requires the use of the Cartan decomposition.

Proof. Any simple Lie group M over $\mathbb{R}$ has a Cartan decomposition: $M = KAK$, where $K < M$ is a compact group, and $A < M$ is a commutative group of diagonal matrices over $\mathbb{R}$. (The Cartan decomposition is useful because it takes the compact parts out, isolating the noncompact part out in A.)

M also has an Iwasawa decomposition, $M = NAK$, where N is A-normalized and conjugate to a subgroup of upper triangular matrices with 1's on the diagonal.

Our goal is to show $\langle g_n.v_1, v_2\rangle \to 0$. It is enough to show that there exists $n_k \to \infty$ such that $\langle g_{n_k}.v_1, v_2\rangle \to 0$. (If not, find a subsequence that converges to something that is not 0, $\langle g_{n_k}.v_1, v_2\rangle \to c$. It still satisfies the assumption. The argument says that there is a subsequence of that sequence that goes to 0, contradiction.)

Write the Cartan decomposition $g_n = k_n a_n k_n'$. By going to a subsequence assume $k_n \to k$, $k_n' \to k'$.

By Cauchy-Schwarz and unitarity,

$$|\langle k_n a_n k_n'.v_1, v_2\rangle - \langle k a_n k'.v_n, v_2\rangle| \le \left|\left\langle a_n k_n'.v_1, k_n^{-1}.v_2\right\rangle - \left\langle a_n k'.v_1, k^{-1}.v_2\right\rangle\right| \xrightarrow{n\to\infty} 0. \tag{1.132}$$

For all n, $\|a_n.v_1\| = \|v_1\|$.

This sits in the unit ball in an infinite-dimensional Hilbert space, which is not compact, but is compact in weak-$*$ topology.

The Banach-Alaoglu Theorem says: if $w_n \in H$ is a sequence of vectors with $\|w_n\| < 1$, then there exists $n_k \to \infty$, $w^* \in H$ such that for any $v \in H$, $\langle w_{n_k}, v\rangle \to \langle w^*, v\rangle$.

Passing to a subsequence, $a_{n_k}.v_1 \xrightarrow{w-*} v^*$. For all v_2, $\langle a_n.v_1, v_2\rangle \to \langle v^*, v_2\rangle$.

We need to show that $v^* = 0$. We will show that v^* is invariant under either all G-noncompact or G_d.

The Mautner phenomenon implies that it is enough to find, for all i such that G_i is non-compact, some non-trivial unipotent $u_i \in G_i$ such that $U_i.v^* = v^*$. Decompase a_n by semi-simple factors, $a_n = a_n^{(1)} \cdots a_n^{(r)}$. The $a_n^i \to \infty$ then use Iwasawa decompostion to find $u_i \in G_i$ such that $a_n^{(i-1)} u_i q_n^{(i)} \xrightarrow{n\to\infty} e$ for a subsequence and then

$$\|u_i.v^* - v^*\|_2 = \lim_{n\to\infty} \left\|a_n^{(i-1)} u_i a_n^{(i)}.v_1 - v_1\right\| = \lim_{n\to\infty} \left\|u_i a_n^{(i)}.v_1 - a_n^i.v_1\right\| = 0. \tag{1.133}$$

$\square$