

www.math.uni-bonn.de/people/bpetri

bpetri@math.uni-bonn.de

D. Witte-Morris: Introduction to Arithmetic Groups

oral exam

some exercises will be presented to us, highly recommended to try to solve them

Idea: groups obtained as integer points of algebraic groups

Ex. $SL_n(\mathbb{Z}) = \{A \in \text{Mat}_{n \times n}(\mathbb{Z}) \mid \det(A) = 1\}$

Def. $\mathbb{H}^2 := \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$

$SL_2(\mathbb{Z}) \curvearrowright \mathbb{H}^2$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$ easily seen to be well-defined

Need to check: this action preserves \mathbb{H}^2 :

$$\begin{aligned} \text{Im}\left(\frac{az+b}{cz+d}\right) &= \frac{1}{2i} \left(\frac{az+b}{cz+d} - \frac{a\bar{z}+b}{c\bar{z}+d} \right) \\ &= \frac{1}{2i} \cdot \frac{(az+b)(c\bar{z}+d) - (a\bar{z}+b)(cz+d)}{|cz+d|^2} \\ &= \frac{1}{2i} \cdot \frac{\overbrace{(ad-bc)}^1 z - \overbrace{(ad-bc)}^1 \bar{z}}{|cz+d|^2} = \frac{\text{Im}(z)}{|cz+d|^2} > 0 \end{aligned}$$

The interesting thing is that this action preserves the metric as well.

We can define a metric on \mathbb{H}^2 (and obtain the hyperbolic geometry) by:

$$g_{x+iy}: T_{x+iy} \mathbb{H}^2 \times T_{x+iy} \mathbb{H}^2 \longrightarrow \mathbb{R}$$

$$g_{x+iy}(u, v) = \frac{1}{y^2} \langle u, v \rangle$$

One notes that while distances differ from the Euclidean ones, angles do not.

Claim. $SL_2(\mathbb{Z})$ preserves g .

PF: EXERCISE. (Riemannian geometry)

Def. (\mathbb{H}^2, g) hyperbolic plane.

Question. What kind of space is $\mathbb{H}^2/SL_2(\mathbb{Z})$?

Def. Fundamental domain: if X is a top. space, G a group, $G \curvearrowright X$ by homeomorphisms, then a fund. domain for this action is a closed set

$$F \subseteq X \text{ s.t. (1) } \bigcup_{g \in G} gF = X$$

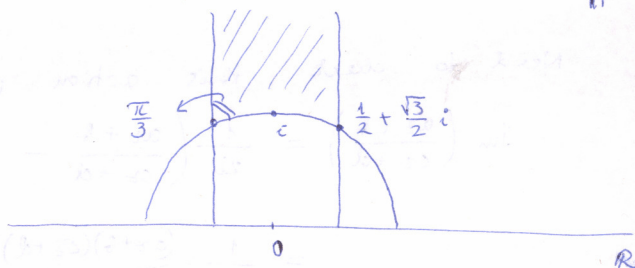
$$(2) gF \cap F = \emptyset \quad \forall g \neq e \in G$$

Ex. (0) $\mathbb{Z} \curvearrowright \mathbb{R}$ by $m \cdot x = x + m \rightarrow$ fund. domain: $[0, 1]$

$$\mathbb{R}/\mathbb{Z} = S^1 = [0, 1] / \sim$$

Claim. $F = \{z \in \mathbb{H}^2 \mid |z| \geq 1, -\frac{1}{2} \leq \operatorname{Re} z \leq +\frac{1}{2}\}$ is a fund. domain for $SL_2(\mathbb{Z}) \curvearrowright \mathbb{H}^2$.

Pf: EXERCISE 1.3.7. & 1.3.8. in [WM].



$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

elts of $SL_2(\mathbb{Z})$

$$S_z = \frac{-1}{z}$$

$$T_z = z + 1$$

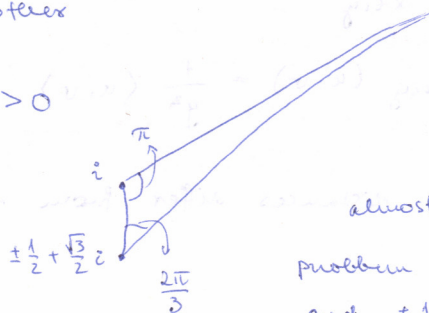
The action of S on the circle:

$$S(e^{i\theta}) = -e^{-i\theta} = e^{i(\pi-\theta)} \rightarrow S(i) = i \text{ and the arcs } \frown \text{ and } \smile$$

get mapped to each other

$$T(-\frac{1}{2} + ai) = \frac{1}{2} + ai \quad \forall a > 0$$

Claim. The quotient is



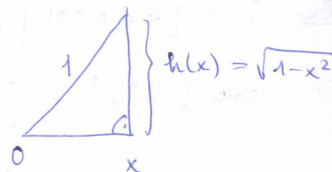
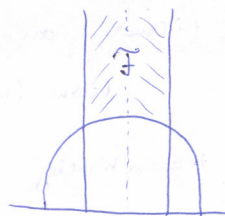
almost a manifold,
problem with the top. spaces at i
and $\pm \frac{1}{2} + \frac{\sqrt{3}}{2}i$.

(These come from the facts $S^2 = \text{Id}$ and $(ST)^3 = \text{Id}$.)

Fact. \exists finite cover of $(\mathbb{H}^2/SL_2(\mathbb{Z})) \setminus$ problematic points (that is, a branched cover of $\mathbb{H}^2/SL_2(\mathbb{Z})$) that is a manifold.

The quotient has finite area:

$$\begin{aligned} \text{area}(\mathbb{H}^2/SL_2(\mathbb{Z})) &= \int_{\mathbb{F}} \frac{dx dy}{y^2} = 2 \int_0^{1/2} \int_{h(x)}^{\infty} \frac{dx dy}{y^2} \\ &= 2 \int_0^{1/2} \left[-\frac{1}{y} \right]_{\sqrt{1-x^2}}^{\infty} dx \\ &= 2 \int_0^{1/2} \frac{dx}{\sqrt{1-x^2}} = 2 \left[\arcsin x \right]_0^{1/2} \\ &= 2 \cdot \frac{\pi}{6} = \frac{\pi}{3} < \infty \end{aligned}$$



Summary. Input: arithmetic subgroup of a Lie group (ie. $SL_2(\mathbb{R})$ in our case)

Output: finite volume "nice space" with a Riemannian metric

coming from a symmetric space the group acts on.
 ↑
 this means sth. nice
 locally symmetric

This course is about properly understanding and generalising the above.

- Locally symmetric spaces
- Lattices
- Arithmetic groups: def., examples, basic properties
- Advanced topics:
 - Margulis's super rigidity
 - Non-arithmetic lattices in $SO(n, 1)$
 - Arithmetic groups coming from hypergeometric functions (i.e. solutions to the hypergeometric DE)

1. Locally symmetric spaces

§ 1. Symmetric spaces

Def. A Riemannian mf. (M, g) is homogeneous if the gp of isometries

$$\text{Isom}(M) = \{ \varphi : M \rightarrow M \text{ diffeo.}, \varphi^* g = g \}$$

acts transitively on M , i.e. $\forall x, y \in M \exists \varphi \in \text{Isom}(M) : \varphi(x) = y$.

Ex. $S^n = \{ x \in \mathbb{R}^{n+1} \mid \|x\| = 1 \}$ w/ metric from \mathbb{R}^{n+1}

$$\text{Isom}^+(S^n) = \{ \varphi \in \text{Isom}(S^n) \mid \varphi \text{ preserves orientation} \}$$

$$= \text{SO}(n+1) = \{ A \in \text{Mat}_{(n+1) \times (n+1)}(\mathbb{R}), \langle Av, Aw \rangle = \langle v, w \rangle, \det A = 1 \}$$

↑
standard inner product on \mathbb{R}^{n+1}

We can rotate any point of S^n to any other point, rotations are in $\text{SO} \Rightarrow S^n$ is homogeneous.

Ex. \mathbb{R}^n is homogeneous with the std. Eu. metric

$$\text{Isom}^+(\mathbb{R}^n) = \text{SO}(n) \times \mathbb{R}^n$$

rotations translations

Recall the notion of the semidirect product: N, H groups, $\varphi : H \rightarrow \text{Aut}(N)$

a homomorphism. Then one defines $N \rtimes_{\varphi} H$ as follows:

the underlying set is the Cartesian product $N \times H$;

the multiplication is given by:

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2).$$

In the above case: $A_1, A_2 \in \text{SO}(n), v_1, v_2 \in \mathbb{R}^n$

$$(A_1, v_1) \cdot (A_2, v_2) w = (A_1, v_1)(A_2 w + v_2) = A_1 A_2 w + A_1 v_2 + v_1,$$

i.e. we have $\varphi : \text{SO}(n) \rightarrow \text{Aut}(\mathbb{R}^n)$ just the action of $\text{SO}(n)$ on \mathbb{R}^n .

Nb. translations alone would show the homogeneity of \mathbb{R}^n .

Ex. (\mathbb{H}^2, g) hyp. plane

$$\text{Isom}^+(\mathbb{H}^2) = \text{PSL}_2(\mathbb{R}) = \text{SL}_2(\mathbb{R}) / \{\pm \text{Id}\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d} \quad \text{if we replace } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ by } \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}, \text{ we get the same}$$

This is transitive: for this it suffices to show that $i \in \mathbb{H}^2$ can go anywhere (and anything can go to i)

$$\text{For } \lambda \in \mathbb{R}: \begin{cases} \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} z = \lambda^2 z \Rightarrow \text{can go anywhere on } i\mathbb{R} \\ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} z = z + x \Rightarrow \text{move horizontally} \end{cases} \left. \begin{array}{l} \text{(move vertically)} \\ \text{move horizontally} \end{array} \right\} \text{move anywhere}$$

Ex. $\mathbb{H}^n =$ hyperbolic n -space

Def. $\langle \cdot, \cdot \rangle_{i,n}: \mathbb{R}^{n+1} \times \mathbb{R}^{n+1} \rightarrow \mathbb{R}$

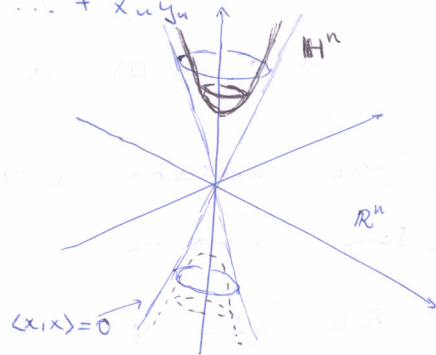
$$(x, y) \mapsto -x_0 y_0 + x_1 y_1 + \dots + x_n y_n$$

Def. $\mathbb{H}^n := \left\{ x \in \mathbb{R}^{n+1} \mid \langle x, x \rangle = -1, x_0 > 0 \right\}$

$$\langle x, x \rangle = 0 \Leftrightarrow x_0^2 = \|(x_1, \dots, x_n)\|^2$$

$\forall p \in \mathbb{H}^n: \langle \cdot, \cdot \rangle_{i,n} |_{T_p \mathbb{H}^n}$ defines an inner product

\rightarrow we have a R. metric g on \mathbb{H}^n



Def. (\mathbb{H}^n, g) is called the hyperbolic n -space.

$$\text{Isom}^+(\mathbb{H}^n) = \text{SO}(1, n)^0 = \left\{ A \in \text{GL}_{n+1}(\mathbb{R}) \mid \langle Av, Aw \rangle_{i,n} = \langle v, w \rangle_{i,n}, A\mathbb{H}^n = \mathbb{H}^n \right\}$$

$$-\text{Id} \notin \text{SO}(1, n)^0$$

This acts transitively (PO), \mathbb{H}^n is homogeneous.

Ex. Products of homog. spaces are homog. (Cartesian)

Def. X top space, $\varphi: X \rightarrow X$

- 1) φ is involution (or an involution) if $\varphi^2 = id$
- 2) $p \in X$ is a fixed point of φ if $\varphi(p) = p$
- 3) a fixed point p of φ is called isolated if $\exists U \subseteq X$ open st. $p \in U$ and $\forall u \in U: \varphi(u) = u \Rightarrow u = p$.

Def. A Riemannian mf. M is symmetric if

- M is homogeneous, connected, complete;
- $\forall p \in M \exists \varphi: M \rightarrow M$ involution isometry of which p is an isolated fixed pt.

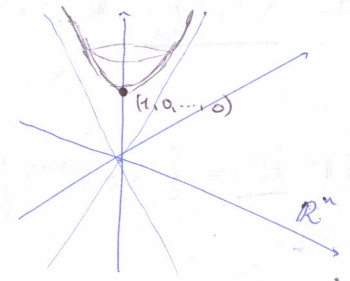
Rem. By homogeneity, it is equivalent to require M to have one isometry w/ an isolated fixed point.

Ex. 1) $S^n: (x_1, \dots, x_{n+1}) \mapsto (-x_1, -x_2, \dots, -x_n, x_{n+1})$

the fixed points are $(0, \dots, 0, \pm 1) \rightarrow$ isolated

2) $\mathbb{R}^n: x \mapsto -x$, the only f.p. is 0

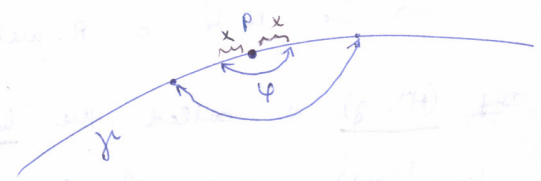
3) $H^n: (x_0, x_1, \dots, x_n) \mapsto (x_0, -x_1, \dots, -x_n)$
 $(1, 0, \dots, 0)$ is the fixed pt.



locally the involution will always be of the form $x \mapsto -x$:

Prop. X Riem. mf., $\varphi: X \rightarrow X$ involutive isometry with isolated fixed pt. p . Then

- 1) $d\varphi|_p = -id$
- 2) For every geodesic $\gamma: \mathbb{R} \rightarrow X$ with $\gamma(0) = p$ we have $\varphi(\gamma(t)) = \gamma(-t) \forall t \in \mathbb{R}$



Pf: 1) $d(\varphi^2)|_p = d\varphi_{\varphi(p)} \circ d\varphi_p$ (chain rule)
 $\underbrace{\quad}_{id} = d\varphi^2_p$ ($\varphi(p) = p$)

$\Rightarrow d\varphi_p$ satisfies $x^2 - 1 = (x+1)(x-1) = 0$, every root has multiplicity 1
 $\Rightarrow d\varphi_p$ is diagonalisable and the possible eigenvalues are ± 1

NTS all ev. are -1 . \uparrow Suppose not: $\exists v \in T_p X, d\varphi_p v = v$.

Let γ be the unique geodesic with $\gamma(0) = p, \gamma'(0) = v$

Consider the geodesic $\varphi \circ \gamma: \mathbb{R} \rightarrow X$ (φ is an isometry).

Since geodesics are uniquely determined by starting point and initial velocity, we get $\varphi \circ \gamma = \gamma$.

\Rightarrow every pt. on γ is fixed under $\varphi \Rightarrow p$ is not isolated ∇

$\Rightarrow d\varphi_p = -id$, as derived

2) Basically the same: $\gamma(0) = p \Rightarrow d\varphi_p \dot{\gamma}(0) = \dot{\gamma}(0) \Rightarrow \varphi \circ \gamma(t) = \gamma(-t)$. □

locally, such maps can always be found, but they need not extend to the whole mf.

Recall the exponential map. let M be a Riem. mf.

$$\exp_p: T_p M (\times \mathbb{R}) \longrightarrow M, \quad \exp_p(t v) = \gamma(t)$$

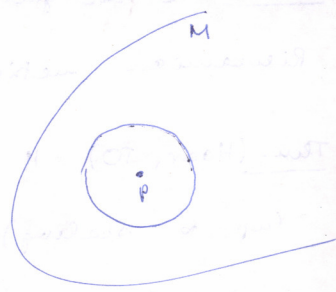
where γ is the unique geodesic with $\gamma(0) = p, \dot{\gamma}(0) = v$

Moreover $\forall p \in M \exists U \subseteq T_p M$ open set s.t.

$\exp_p: U \longrightarrow \exp_p(U)$ is a diffeomorphism.

By making U smaller, one can assume that

- U is symmetric, i.e. $U = -U$
- U is star-shaped, i.e. $\forall t \in [0, 1]: tU \subseteq U$



Def. The geodesic symmetry at p is the map

$$\tau: \exp_p(U) \longrightarrow \exp_p(U)$$

$$\exp_p(v) \longmapsto \exp_p(-v)$$

Note that 2) in the Prop. shows that if φ is an invol. isom. \Rightarrow
 $\Rightarrow \varphi$ agrees with τ near p .

Cor. A homogeneous space is symmetric iff it is connected, complete and $\forall p \in M$ the geodesic symmetry extends to a global isometry of M .

Note: usually our Riemannian mfs are nice, i.e. connected, complete, smooth, locally compact, ...

§2. Constructing symmetric spaces

Recall: topological group: group equipped with a topology s.t. all group operations are continuous.

Lemma: X connected homogeneous space,

$G := \text{Isom}(X)^\circ =$ connected component of the identity in $\text{Isom}(X)$

$K := \text{Stab}_G(x)$ where $x \in X$ and Stab denotes the stabiliser

$\Rightarrow X \cong G/K$ (homeo.) and $K \subset G$ is compact.

PF: EXERCISES 1.2.1., 1.2.2. □

Recall: a Lie group: group equipped with a smooth manifold structure, all group operations are smooth.

Lemma: G Lie group, $K \subset G$ compact subgroup. Then there is a G -invariant Riemannian metric on G/K , and G/K with this metric is a homogeneous space.

Thm. (Haar, PO) H a locally compact Hausdorff group. \Rightarrow there is a unique (up to scaling) σ -finite Borel measure μ on H s.t.

1) $\mu(C)$ is finite for $C \subseteq H$ compact

2) $\mu(hA) = \mu(A) \quad \forall A \text{ Borel } \forall h \in H.$

Def. This μ is called the Haar measure on H . □

Recall that σ -finiteness means that H is a countable union of sets with finite measure.

Note that $\mu(Ah) = \mu(A)$ need not be true.

Ex. 1) Finite groups: counting measure

2) $(\mathbb{R}^n, +)$: the Lebesgue measure is the unique translation invariant measure

PROOF OF LEMMA: Goal: left G -invariant Riemannian metric on G/K .

$\langle \cdot, \cdot \rangle: T_e G \times T_e G \rightarrow \mathbb{R}$ any inner product ($e \in G$ is the identity elt)

Given $g \in G$ define $L_g: G \rightarrow G$ by $L_g(h) := gh \quad \forall h \in G.$

Then we can define for $v, w \in T_g G$:

$$\langle v, w \rangle_g := \langle (dL_{g^{-1}})_g v, (dL_{g^{-1}})_g w \rangle$$

By construction this is left G -invariant. The problem is that it might not be right K -invariant.

$$\forall g \in G: R_g: G \rightarrow G, R_g(h) := hg$$

$$\langle v, w \rangle_g := \int_K \langle dR_k v, dR_k w \rangle_{gk} d\mu(k) \quad \text{smooth function integrated over a compact space} \Rightarrow \text{finite integral}$$

$$(dR_k v, dR_k w)_{gk} \stackrel{\text{def}}{=} \int_K \langle dR_l dR_k v, dR_l dR_k w \rangle_{gkl} d\mu(l)$$

$$= \int_K \langle dR_{kl} v, dR_{kl} w \rangle_{gkl} d\mu(l) \quad \text{chain rule}$$

$$= \int_K \langle dR_{kl} v, dR_{kl} w \rangle_{gkl} d\mu(kl) \quad \text{Haar measure}$$

$$= \int_K \langle dR_{k'} v, dR_{k'} w \rangle_{gk'} d\mu(k') = \langle v, w \rangle_g$$

\Rightarrow right K -invariance \Rightarrow descends to G/K .

Ex. 1) $S^n = SO(n+1) / SO(n)$



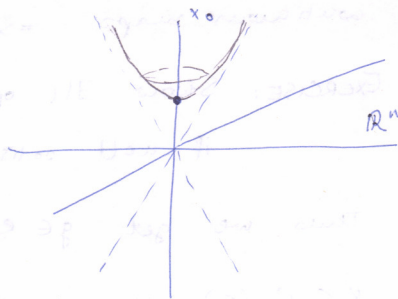
stabilising the North pole \Leftrightarrow rotating the hyperplane $\rightarrow SO(n)$

2) $R^n = SO(n) \times \mathbb{R}^n / SO(n)$

involution: $x \mapsto -x$ with fixed pt $(0, \dots, 0)$

3) $H^n = SO(1, n)^0 / SO(n)$

stabiliser of $(1, 0, \dots, 0)$



involution: $(x_0, x_1, \dots, x_n) \mapsto (x_0, -x_1, \dots, -x_n)$

Prop. Let G be a connected linear Lie group,

K a compact subgroup,

σ an involutive automorphism of G

such that K is an open subgroup of $\{g \in G \mid \sigma(g) = g\} = C_G(\sigma)$.

Then G/K can be given the structure of a symmetric space s.t.

$$\tau(gK) := \sigma(g)K$$

is an involutive isometry of which eK is an isolated fixed pt.

For involutions, stabilisers and centralisers are the same.

PF: We already know that G/K is homogeneous.

We only need to check that τ has the desired properties.

σ is an involution $\Rightarrow \tau$ is an involution

$G^+ := \langle \sigma \rangle \ltimes G \quad (\text{the action of } \sigma \text{ on } G \text{ comes from } \sigma \text{ being an aut. of } G)$
 $\simeq \mathbb{Z}/2\mathbb{Z}$

$$K^+ := \langle \sigma \rangle \times K$$

Thus we get $G/K = G^+/K^+$.

The same construction as last week gives that τ is an isometry.

$\tau(eK) = \sigma(e)K = eK$ is trivial.

The last thing to check is that eK is isolated.

Suppose that $\exists gK$ fixed pt of τ st. g is close to e .

$$gK = \tau(gK) = \sigma(g)K \Rightarrow \sigma(g) = g \cdot k \quad \text{for some } k \in K$$

$$g = \sigma^2(g) = \sigma(gk) = \sigma(g) \underbrace{\sigma(k)}_k = gk^2 \Rightarrow k^2 = e$$

$g^{-1}\sigma(g) = k$, g is close to the identity e , $(\)^{-1}$ and σ are continuous maps $\Rightarrow k$ is close to the identity e

EXERCISE: Show $\exists U$ open nbh. of $e \in G$ (lin. Lie group) s.t.

if $u \in U$ satisfies $u^2 = e$ then $u = e$.

Thus we get $k = e$, $\sigma(g) = g$, i.e. $g \in C_G(\sigma)$.

$K \subseteq C_G(\sigma)$ is open $\Rightarrow K$ contains an open nbh. of $e \Rightarrow$ contains e

$$\Rightarrow gK = eK$$

□

$$\text{Ex. 1) } \mathbb{S}^n = \text{SO}(n+1) / \text{SO}(n) \quad \sigma = \text{diag}(-1, \dots, -1, 1)$$

$$K = C_G(\sigma) = \{g \in G \mid \sigma L_g = L_g \sigma\}$$

$$2) \mathbb{R}^n = \text{SO}(n) \times \mathbb{R}^n / \text{SO}(n) \quad \sigma(k, v) = (k, -v)$$

$\uparrow \quad \uparrow$
 $\text{SO}(n) \quad \mathbb{R}^n$

$K = \text{SO}(n)$ (which is clearly an open subgroup of itself)

$$3) \mathbb{H}^n = \text{SO}(1, n) / \text{SO}(n) \quad \sigma = \text{diag}(1, -1, \dots, -1)$$

$$K = G_G(\sigma)$$

$$\text{Ex. } G = \text{SL}(n, \mathbb{R})$$

$$K = \text{SO}(n)$$

$$\sigma(g) = (g^{-1})^T \quad \text{involutive group automorphism}$$

By the Prop., we obtain a symmetric space $X = G/K$

Note that for $n=2$ we get $X = \mathbb{H}^2$ but this does not hold for $n > 2$.

Claim. $X = \{A \in \text{SL}(n, \mathbb{R}) \mid A^T = A \text{ (symmetric), all eigenvalues are } > 0 \text{ (pos. def.)}\}$
 \downarrow
 all eigenvalues are real

Define $\alpha: G \times X \rightarrow X$ by $\alpha(g, x) = g x g^T$.

EXERCISE: check that this is a transitive action.

Hint: a matrix x is positive (i.e. all eigenvalues are ≥ 0) if $x = yy^T$ for some y .

$$K = \text{Stab}_G(\text{Id}) = \text{SO}(n) = \left\{ A \in \text{SL}_n(\mathbb{R}) \mid \langle Av, Aw \rangle = \langle v, w \rangle \forall v, w \in \mathbb{R}^n \right\}$$

\updownarrow
 $A^T A = \text{Id}$

The following part involves some theory of Lie groups; one should not worry too much about not understanding it in full detail.

To get a metric, we first identify the tangent space:

$$T_e X = \left\{ A \in \text{Mat}_{n \times n}^{(\mathbb{R})} \mid A \text{ symmetric, } \text{tr } A = 0 \right\}$$

\downarrow
 comes from $1 = \det(\exp A) = \exp(\text{tr } A)$

Define $\langle A | B \rangle = \text{tr}(AB^T)$: will be an inner product.

For $A \in X$, let $\tau(A) := A^{-1}$. τ is an isometry.

Thus we obtain a symmetric space.

Def. 1) A symmetric space is irreducible if its universal cover is not isometric to a product of symmetric spaces.

(Ex.: S^n, H^n . Non-ex.: \mathbb{R}^n for $n > 1$.)

2) A Riemannian mf. is flat if its Riemann curvature tensor is zero at every point.

This is equivalent to every point having an open nbhd. that is isometric to an open subset of \mathbb{R}^n .

(Ex. $\mathbb{R}^n, \mathbb{T}^n = \mathbb{R}^n / \mathbb{Z}^n$)

3) A Lie group is simple if

- it is non-abelian
- it has no connected closed nontrivial normal subgroup.

(Ex. $SL_n(\mathbb{R})$ (PO))

4) G_1, G_2 Lie groups are isogenous if

- \exists finite index $G_i' < G_i$ for $i=1,2$
- \exists finite $N_i \triangleleft G_i$ for $i=1,2$

s.t. $G_1' / N_1 \cong G_2' / N_2$.

5) G is semisimple if it is isogenous to a product of simple groups.

Prop G connected non-compact simple Lie group with finite center

Then G has a maximal compact subgroup K s.t.

- K is unique up to conjugation
- G/K is a simply connected irreducible symmetric space (1)
- G/K has non-positive sectional curvature everywhere and it is not flat. (2)

Every symmetric space with properties (1) and (2) is of this form.

Most of these statements should not come as a surprise in light of our previous work and the above definitions.

Def. A complete Riemannian mf. is locally symmetric if its universal cover is a symmetric space.

Ex. Symmetric \Rightarrow locally symmetric.

$\mathbb{T}^n = \mathbb{R}^n / \mathbb{Z}^n$ is loc. symmetric

Arithmetic Groups, lecture 4

Rmk. Loc. symmetric \Rightarrow the geodesic symmetry is a local isometry

Recall. $\mathbb{H}^2 = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$ with $ds^2 = \frac{dx^2 + dy^2}{y^2}$ being the metric. Geodesics: horizontal lines and half-circles.

$g: \mathbb{H}^2 \rightarrow \mathbb{H}^2$
 $z \mapsto z+1$

$\text{Isom}^+(\mathbb{H}^2, ds^2) = \text{PSL}_n(\mathbb{R}), \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{az+b}{cz+d}$

$\text{PSL}_2(\mathbb{Z}) = \Gamma = \langle g \rangle \cong \mathbb{Z}$

\mathbb{H}^2/Γ is loc. symmetric

The quotient is homeomorphic to a cylinder.

Why is this not a symmetric space?

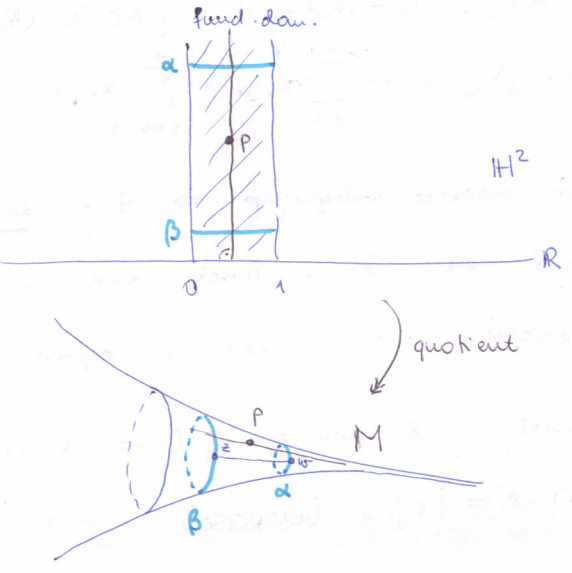
There is no nontrivially

nontrivial closed loop through z of length $< \epsilon$ (for ϵ small enough)

On the other hand, there is such a loop through w .

\rightarrow No isometry $M \rightarrow M$ can send z to w .

Also, a geodesic symmetry w to z flips the two ends.



Group version

Def. X loc. cpt top space, $G \curvearrowright X$ by homeomorphisms. The action is called properly discontinuous if $\forall K \subset X$ cpt: $\{g \in G \mid gK \cap K\}$ is finite.

Ex. $\mathbb{Z} \curvearrowright \mathbb{R}: m \cdot x = x+m \quad (m \in \mathbb{Z}, x \in \mathbb{R}) \rightarrow$ prop. discout.

$\mathbb{R} \curvearrowright \mathbb{R} \quad g \cdot x = x+y \quad y \in (0,1): (y + [0,1]) \cap [0,1] \neq \emptyset$, it is even uncountable
 \rightarrow this is not prop. discout.

Equivalent def. (locally symmetric) M complete mf. is loc. symmetric if there is a symmetric space X and $\Gamma < \text{Isom}(X)$ s.t.

- Γ acts prop. discontinuously and freely on X
- M is isometric to $\Gamma \backslash X$

So $M = \Gamma \backslash G/K$

In [W.M], we move on now to Ch. IV.

From now on: G semisimple ^{linear} Lie group with finitely many components.

$\Gamma < G$ lattice (def. comes later)

Ex. $G = \mathrm{SL}_n(\mathbb{R})$, $G = \mathrm{SO}(m, n) = \{ A \in \mathrm{SL}(m+n, \mathbb{R}) \mid \langle Ax, Ay \rangle_{m, n} = \langle x, y \rangle_{m, n} \ \forall x, y \}$

$$\text{where } \langle x, y \rangle_{m, n} = - \sum_{i=1}^m x_i y_i + \sum_{i=m+1}^n x_i y_i$$

Lemma. $\Lambda < G$ discrete subgroup $\Rightarrow \exists$ a strict fundamental domain for $\Lambda \backslash G$,
i.e. $\exists \mathcal{F} \subset G$ s.t. \mathcal{F} is Borel and $\mathcal{F} \rightarrow G/\Lambda$ is bijective.

(So the strictness means that we require injectivity.)

Pf: Λ discrete and non-empty (since it is a group) $\Rightarrow \exists U \subset G$ open s.t.

$$U^{-1}U \cap \Lambda = \{e\} \quad (\text{EXERCISE})$$

G is second-countable $\rightarrow \exists g_n \in G$ s.t. $\bigcup_{n=1}^{\infty} g_n U = G$

$\mathcal{F} := \bigcup_{n=1}^{\infty} \left(g_n U \setminus \left\{ \bigcup_{i < n} g_i U \cap \Lambda \right\} \right)$ This is clearly Borel and a strict fund. domain. □

Prop. $\Lambda < G$ discrete subgroup, μ Haar measure on G . $\Rightarrow \exists!$ (up to scalar) σ -finite, G -invariant Borel measure ν on G/Λ :

1) $A \subset G$ Borel with $A\Lambda = A \Rightarrow \nu(A/\Lambda) = \mu(A \cap \mathcal{F})$.

(Every Borel subset of G/Λ is of the form A/Λ for such an A .)

2) $A \subset G$ Borel $\Rightarrow \mu(A) = \int_{G/\Lambda} \#(A \cap x\Lambda) \, d\nu(x\Lambda)$

Pf: left-invariant measure is also right-invariant, this follows from semisimplicity

Ex. 4.1.7, 4.1.8. □

Convention. From now on μ and ν satisfy (1) and (2), i.e. the scaling between them is fixed.

Cor. $A \subset G$ Borel, $\varphi: G \rightarrow G/\Lambda$ quotient map $\Rightarrow \nu(\varphi(A)) = \mu(A)$. □

Rem. These μ and ν are really volumes since μ comes from a volume form on G .

Def. $\Gamma < G$ is a lattice if: Γ is discrete and G/Γ has finite volume.

Ex. $SL_2(\mathbb{Z}) < SL_2(\mathbb{R})$

Prop. $\Lambda < G$ discrete subgroup, μ Haar measure on G . TFAE:

- 1) Λ is a lattice
- 2) $\exists \mathcal{F}$ strict fund. domain for $\Lambda \backslash G$ with $\mu(\mathcal{F}) < \infty$
- 3) $\exists C \subseteq G$ Borel set s.t. $C\Lambda = G$ and $\mu(C) < \infty$

PF: 1) \Rightarrow 2) Use the previous Prop.:

$$\infty > \nu(G/\Lambda) = \mu(G \cap \mathcal{F}) = \mu(\mathcal{F})$$

2) \Rightarrow 3) $C = \mathcal{F}$ satisfies 3)

$$\text{3) } \Rightarrow \text{1) } \quad \nu(G/\Lambda) = \int_{G/\Lambda} 1 \, d\nu(x\Lambda) \leq \int_{G/\Lambda} \underbrace{\#(C \cap x\Lambda)}_{\geq 1} \, d\nu(x\Lambda) = \mu(C) \stackrel{3)}{<} \infty$$

Def. $\Lambda < G$ closed subgroup is called cocompact (or uniform) if G/Λ is compact.

Ex. $\mathbb{Z}^n < \mathbb{R}^n$, $\{e\} < SO(n)$ (since $SO(n)$ is compact)

Non-ex. $SL_2(\mathbb{Z}) < SL_2(\mathbb{R})$

Note that cocompactness $\not\Rightarrow$ finite volume.

Cor. Every cocompact discrete subgroup of G is a lattice.

Every finite index subgroup of a lattice is a lattice.

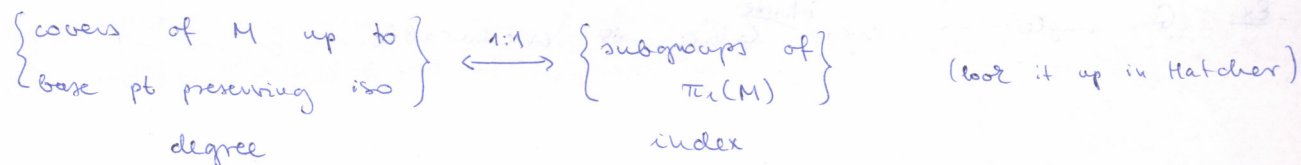
PF: Ex. 4.1.12., 4.1.13.

Commensurability

Def. Hgp., $\Lambda_1, \Lambda_2 < H$ are commensurable if $\Lambda_1 \cap \Lambda_2$ is finite index in both Λ_1 and Λ_2 .

Ex. $a\mathbb{Z}, b\mathbb{Z} < \mathbb{R}$ are comm. iff $\frac{a}{b} \in \mathbb{Q}$.

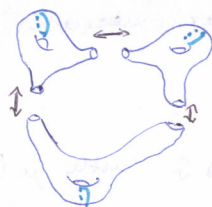
Recall. M mf., $M = \tilde{M}/\pi_1(M)$ where \tilde{M} is the univ. cover.



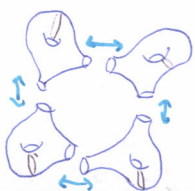
These given covers $M_1 \rightarrow M$ and $M_2 \rightarrow M$ correspond to $\Lambda_1, \Lambda_2 < \pi_1(M)$.

Then Λ_1 and Λ_2 are commensurable iff M_1, M_2 have a common finite cover.

Ex.



$$\Lambda_1 \triangleleft \pi_1(M) \xrightarrow[\text{index } 3]{\text{alg. intersect. with } a} \mathbb{Z} \xrightarrow{\text{mod } 3} \mathbb{Z}/3\mathbb{Z}$$



$$\Lambda_2 = \ker(\text{algebraic intersection with } b \text{ and } c)$$

$$\pi_1(M) \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

What is the common finite cover?

Def. $g \in G$ is said to commensurate $\Gamma < G$ if $g\Gamma g^{-1}$ is commens. to Γ .

24.04.2018

Commensurator of Γ : $\text{Comm}_G(\Gamma) := \{g \in G \mid g \text{ commensurates } \Gamma\}$

Note that $N_G(\Gamma) = \{g \in G \mid g\Gamma g^{-1} = \Gamma\} < \text{Comm}_G(\Gamma)$, but usually the normaliser is a lot smaller. (In this notation, $<$ probably allows $=$.)

Ex. $G = \text{SL}(n, \mathbb{R})$, $\Gamma = \text{SL}(n, \mathbb{Z})$ (we will prove that Γ is a lattice later)

Then $N_G(\Gamma)$ is commensurable to Γ and $\text{Comm}_G(\Gamma) > \text{SL}(n, \mathbb{Q})$ is dense in G .

Def. Λ_1, Λ_2 are abstractly commensurable if $\exists \Lambda'_i < \Lambda_i$ finite index subgroups s.t. $\Lambda'_1 \cong \Lambda'_2$.

Irreducible lattices

Def. Γ is called irreducible if (1) for every non-compact closed normal subgroup $N < G^0$ the set ΓN is dense and (2) Γ is infinite.

Ex. G simple \Rightarrow every infinite lattice is irreducible.

Counterex. $G = G_1 \times G_2$, $\Gamma = \Gamma_1 \times \Gamma_2$ where $\Gamma_i < G_i$ lattice.

Then $N = G_i^o$ does not satisfy (1).

Prop. Assume that \bullet G has trivial center and

\bullet Γ projects densely in the maximal component factor of G .

Then \exists a decomposition $G = G_1 \times \dots \times G_r$ and lattices $\Gamma_i < G_i$ s.t.

\bullet Γ is commensurable to $\Gamma_1 \times \dots \times \Gamma_r$ and

\bullet $\Gamma_i < G_i$ is irreducible.

Proof later, needs Borel density.

Def. A locally symmetric space $\Gamma \backslash X$ is called irreducible if there are no nontrivial locally symmetric spaces $\Gamma_1 \backslash X_1$ and $\Gamma_2 \backslash X_2$ s.t. $\Gamma_1 \backslash X_1 \times \Gamma_2 \backslash X_2$ is a finite cover of $\Gamma \backslash X$.

Prop. There are locally symmetric spaces $\Gamma_1 \backslash X_1, \dots, \Gamma_r \backslash X_r$ s.t.

\bullet $\Gamma_i \backslash X_i$ are irreducible

\bullet $\Gamma_1 \backslash X_1 \times \dots \times \Gamma_r \backslash X_r$ is a fin. cover of $\Gamma \backslash X$.

Pf. Induction. □

Prop. M irreducible loc. symm. space s.t. the univ. cover X of M has no compact factors and no flat factors and for any nontrivial product decomposition $X = X_1 \times X_2$ the img of X_i is dense in M . □

Pf. EXERCISE.

We wish to understand the structure of a loc. symm. space from its lattice.

Lemma. $\Gamma < G$ discrete subgp, $K < G$ cpt. subgp.

Then $\Gamma \backslash G$ is cpt. $\Leftrightarrow \Gamma \backslash G/K$ is cpt. and

$\Gamma \backslash G$ has finite volume $\Leftrightarrow \Gamma \backslash G/K$ has finite volume.

Pf. $\Gamma \backslash G$ cpt $\Rightarrow \Gamma \backslash G/K$ cpt. since the quotient operation preserves compactness in general.

Let $\frac{G}{\Gamma}$ be cpt., $(g_n)_n$ be a sequence in $\frac{G}{\Gamma}$. Want to find a convergent subseq.

$[g_n]_n$: the projection to $\frac{G}{\Gamma}$ \Rightarrow has a convergent subseq. $[g_{n_j}]_j$

Pick representatives \tilde{g}_{n_j} in each class, $g_{n_j} = \tilde{g}_{n_j} \cdot k_{n_j} \quad \forall j$

$k_{n_j} \in K \rightarrow \exists$ convergent subsequence $(k_{n_{j_\ell}})_\ell$

$\Rightarrow (g_{n_{j_\ell}}) = (\tilde{g}_{n_{j_\ell}} \cdot k_{n_{j_\ell}})_\ell$ is convergent in $\frac{G}{\Gamma}$. \checkmark

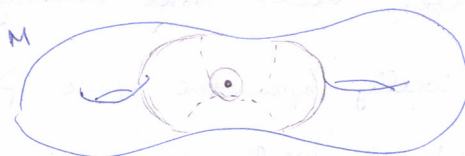
The finite volume equivalence is EXERCISE 1.3.6. □

Def. M Riemannian mf., $x \in M$

Injectivity radius at x :

$$inj_x(M) := \sup \{ r \geq 0 \mid \exp_x : \underbrace{(\exp_x^{-1}(B_r(x)))^o}_{\text{connected component containing } 0} \rightarrow B_r(x) \text{ is a diffeomorphism} \}$$

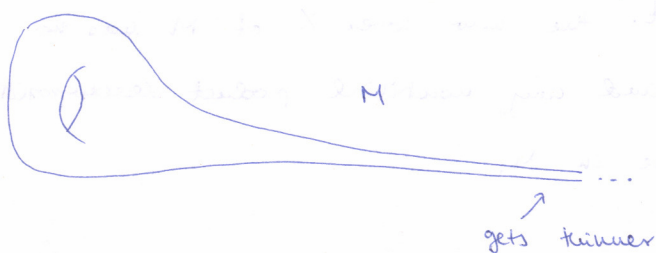
i.e. the inj radius is "the largest radius s.t. the ball does not overlap with itself". Here $B_r(x)$ denotes the open ball with radius r .
i.e. \exp_x is a local diffeo.



Def. Injectivity radius of M : $inj(M) := \inf \{ inj_x(M) \mid x \in M \}$

Observation: if M is compact then $inj(M) > 0$. This need not hold for non-compact manifolds M .

Ex.



$$\Rightarrow inj(M) = 0.$$

$\mathbb{H}^2 / SL_2(\mathbb{Z})$ is like this (although it is not a mf., but the def. can be extended to orbifolds)

Prop. $g \in G$ defines a map $\varphi_g: G \rightarrow G/\Gamma$
 $x \mapsto xg\Gamma$

Then G/Γ compact $\Leftrightarrow \exists U$ open nbhd. of e s.t. $\forall g \in G: \varphi_g: U \rightarrow G/\Gamma$ is injective.

Pf. " \Rightarrow " Let $\varphi: G \rightarrow G/\Gamma$, i.e. $\varphi = \varphi_e$.
 $x \mapsto x\Gamma$

This is a covering map (follows from the discreteness of Γ and structure of G)

i.e. $\forall p \in G/\Gamma \exists V_p$ connected open neighbourhood s.t. restricting φ to a connected component of $\varphi^{-1}(V_p)$ yields a diffeomorphism.

Claim. \exists connected nbhd. U of e in G s.t. $\forall p \in G/\Gamma \exists p' \in G/\Gamma$ s.t. $U \cdot p \subseteq V_{p'}$.

Note that Claim \Rightarrow Prop.

PF OF CLAIM: V_p open $\Rightarrow \exists U_p$ nbhd. of $e \in G$ s.t. $U_p \cdot p \subseteq V_p$.

Define new open nbhds of $e \in G$ W_p s.t. $v, w \in W_p \Rightarrow v \cdot w \in U_p$.

$\{W_p \cdot p \mid p \in G/\Gamma\}$ is an open covering of G/Γ $\xrightarrow{\text{compactness}}$ $\{W_{p_i} \cdot p_i\}_{i=1}^N$ finite subcover

$U := \bigcap_{i=1}^N W_{p_i}$ open nbhd of e in G

$q \in W_{p_i} \cdot p_i \Rightarrow uq \in U_{p_i} \cdot p_i \subseteq V_{p_i} \forall u \in U$ by construction. \checkmark

" \Leftarrow " We will prove that if $\emptyset \neq U \subset G$ open precompact and G/Γ not cpt.

$\Rightarrow \exists g \in G$ s.t. $\varphi_g: U \rightarrow G/\Gamma$ is not injective.

Let $C \subset G$ be compact.

$\underbrace{(G/\Gamma)}_{\text{cpt.}} \setminus \underbrace{U^{-1}G}_{\text{non-cpt.}} \neq \emptyset$ We can thus build a sequence $(g_n)_n$ in G such that $g_n U \subset G/\Gamma$ are all disjoint:

Take $g_0 = e, C_i := \overline{g_i U} \cup C_{i-1}, g_i \in (G/\Gamma) \setminus (U^{-1}C_i)$

Γ is a lattice $\Rightarrow \text{vol}(G/\Gamma) < \infty$

$\Rightarrow \text{vol}(g_n U) \rightarrow 0$ as $n \rightarrow \infty$

$\Rightarrow \exists n: \varphi_{g_n}: U \rightarrow G/\Gamma$ is not injective (otherwise the volume would be preserved). \square

This was still kind of geometric.

We want an algebraic version.

Notation. H group, $a, b \in H, A, B \subset H$.

$${}^b a := b a b^{-1}, \quad B_a := \{ {}^b a \mid b \in B \}$$

$${}^B A := \{ {}^b a \mid a \in A, b \in B \}$$

Corollary G/Γ is cpt. $\Leftrightarrow e \in G$ is not an accumulation point of G/Γ .

$\mathbb{P}: \varphi_g|_U$ injective $\Leftrightarrow \exists u_1, u_2 \in U$ s.t. $u_1 g \Gamma = u_2 g \Gamma$

$\Leftrightarrow g\Gamma \cap U U^{-1} = \{e\}$

□

26.04.2018

Simple Lie groups (introduction)

Classical Lie groups: all simple

1) $SL(n, \mathbb{R})$ $n \geq 2$ special linear group

2) $SO(m, n)^0 = \{g \in SL(m+n, \mathbb{R}) \mid g^T I_{m,n} g = I_{m,n}\}^0$ where $I_{m,n} = \begin{pmatrix} \overbrace{-1 \dots -1}^m & & & & \\ & & & & 0 \\ & & & & +1 \dots +1 \\ 0 & & & & \underbrace{}_n \end{pmatrix}$
 special orthogonal group \uparrow preserve bilinear form

3) $SU(m, n) = \{g \in SL(m+n, \mathbb{C}) \mid g^* I_{m,n} g = I_{m,n}\}$ where $g^* = \overline{g}^T$ is the adjoint
 special unitary group \uparrow preserve sesquilinear form

4) $F_{2m} := \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$ $Sp(2m, \mathbb{R}) = \{g \in SL(2m, \mathbb{R}) \mid g^T F_{2m} g = F_{2m}\}$
 $m \geq 1$ symplectic group \uparrow preserve antisymmetric form

Different fields:

1) $SL(n, \mathbb{C}), SL(n, \mathbb{H})$ where $\mathbb{H} = \text{quaternions} = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_n \in \mathbb{R}\}$
 with $j^2 = -j i^2 = k, i^2 = j^2 = k^2 = -1$

$\mathbb{H} \cong \mathbb{C}^2$ as a vector space. Thus taking det in $\text{Mat}_{n \times n}(\mathbb{H})$ can be done by taking it in $\text{Mat}_{2n \times 2n}(\mathbb{C})$. (This det is called the reduced norm.)

2) $SO(n, \mathbb{C}) = \{g \in SL(n, \mathbb{C}) \mid g^T g = I_n\}$

$SO(n, \mathbb{H}) = \{g \in SL(n, \mathbb{H}) \mid \text{tr}(g^T) g = I_n\}$ where $\text{tr}(a_0 + a_1 i + a_2 j + a_3 k) = a_0 + a_1 i - a_2 j + a_3 k$

3) $Sp(2m, \mathbb{C}) = \{g \in SL(2m, \mathbb{C}) \mid g^T F_{2m} g = F_{2m}\}$ complex symplectic group

4) $Sp(m, n) = \{g \in SL(m+n, \mathbb{H}) \mid g^* I_{m,n} g = I_{m,n}\}$

Thm. (E. Cartan) Every simple Lie group is isogenous either to a classical group or one of the finitely many exceptional groups.

From now on, think of a simple Lie group as one of these.

Def. A matrix $U \in SL(n, \mathbb{C})$ is called unipotent if $\exists m \in \mathbb{N} : (U - I_n)^m = 0$.

Equivalently, all eigenvalues are 1.

Note that any (semi)simple Lie group is in $SL(n, \mathbb{R})$ for large enough n .

Ex. $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL(2, \mathbb{C}) : (U - I_2)^2 = 0$. unipotent

Cor. If Γ has a nontrivial unipotent element, then G/Γ is not compact.

Pf: (1) $u := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$. Let $a := \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix} \in SL(2, \mathbb{R})$.

$$a^n u a^{-n} = \begin{pmatrix} 1 & 2^{-2n} \\ 0 & 1 \end{pmatrix} \xrightarrow{n \rightarrow \infty} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \text{ hence } e \text{ is an accumulation point of } G/\Gamma. \Rightarrow G/\Gamma \text{ non-cpt.}$$

We now show that (1) can be generalised.

Jacobson-Morosov Lemma: There is a continuous homomorphism

(Po) $\varphi : SL(2, \mathbb{R}) \rightarrow G$ with $\varphi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = U$ where G is non-compact, $U \in G$.

Set $g_n := \varphi\left(a^n \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} a^{-n}\right) \xrightarrow{n \rightarrow \infty} e \in G. \Rightarrow G/\Gamma \text{ non-cpt.}$

Note. Knapp: Structure theory of semisimple Lie groups \rightarrow quick overview

Fulbou-Harris: (start with "introduction" and "rep. theory")

Prop. Λ lattice in H , $C \subseteq H$. Then the img of C in H/Λ is precompact iff $e \in H$ is not an accumulation pt of C/Λ .

Pf: EXERCISE 4.4.2, just put the above proofs together.

Prop. (Mahler Compactness Criterion)

$C \subseteq SL(l, \mathbb{R})$. Then the img of C in $SL(l, \mathbb{R})/SL(l, \mathbb{Z})$ is precompact

iff 0 is not an accumulation point of $C\mathbb{Z}^l = \{cv \mid c \in C, v \in \mathbb{Z}^l\} \subseteq \mathbb{R}^l$.

Pf: " \Rightarrow " $\pi(C)$ precompact $\Rightarrow \exists C_0 \subseteq SL(l, \mathbb{R})$ compact s.t. $C \subseteq C_0 SL(l, \mathbb{Z})$ (Ex. 4.1.11.)

where $\pi : SL(l, \mathbb{R}) \rightarrow SL(l, \mathbb{R})/SL(l, \mathbb{Z})$ is the quotient map.

By enlarging C wma $C = C_0 SL(l, \mathbb{Z})$.

$$\Rightarrow C(\mathbb{Z}^l \setminus \{0\}) = C_0 SL(l, \mathbb{Z})(\mathbb{Z}^l \setminus \{0\}) = C_0(\mathbb{Z}^l \setminus \{0\})$$

C_0 cpt, hence closed. $\mathbb{Z}^l \setminus \{0\}$ closed $\Rightarrow C_0(\mathbb{Z}^l \setminus \{0\})$ closed,

hence contains all its accumulation pts.

§ If $0 \in C(\mathbb{Z}^l \setminus \{0\})$ then $\exists c \in C, v \in \mathbb{Z}^l \setminus \{0\}$ s.t. $cv = 0$. But elts of C are invertible. \nexists

" \Leftarrow " Suppose $(g_n)_n$ is a sequence of elts in $SL(n, \mathbb{R})$ s.t. 0 is not an acc. point of $\bigcup_{n \geq 0} g_n \mathbb{Z}^l$.

Our goal is to show that $\exists (g'_n)_n$ in $SL(n, \mathbb{Z})$ s.t. $(g'_n g_n)_n$ has a convergent subsequence.

For each n define

- $v_n^1 \in \mathbb{Z}^l \setminus \{0\}$ s.t. $\|g_n v_n^1\|$ has minimal norm
- $v_n^i \in \mathbb{Z}^l \setminus \text{Span}_{\mathbb{R}} \{g_n v_n^1, \dots, g_n v_n^{i-1}\}$ s.t. $\|\text{proj}_{\{g_n v_n^1, \dots, g_n v_n^{i-1}\}^\perp}(g_n v_n^i)\|$ is minimal

$$K_n = \text{conv} \{v_n^1, \dots, v_n^l\}$$

(Note that v_n^1, \dots, v_n^l are lin. independent.)

$$K_n \cap (\mathbb{Z}^l \setminus \{0\}) = \{v_n^1, \dots, v_n^l\} \text{ by non-minimality } (*)$$

Define $\gamma_n := [v_n^1 \dots v_n^l] \in \text{Mat}_{l \times l}(\mathbb{Z})$.

Claim. $\det(\gamma_n) = \pm 1$.

Pf: $\det(\gamma_n) = \pm \text{vol}(Q)$ where $Q = \text{conv} \left\{ \sum_{i=1}^l \epsilon_i v_n^i \mid \forall \epsilon_i \in [0, 1] \right\}$

We claim that Q is a full domain for $\mathbb{Z}^l \curvearrowright \mathbb{R}^l$.

This would imply $\text{vol}(Q) = \text{vol}(\mathbb{R}^l / \mathbb{Z}^l) = 1$, hence $\det(\gamma_n) = \pm 1$.

$\mathbb{Z}^l Q = \mathbb{R}^l$ clearly holds.

NTS: $(v + \dot{Q}) \cap \dot{Q} = \emptyset \quad \forall v \in \mathbb{Z}^l$. This follows from (*).

(If they would intersect, we would obtain a nontriv lin. combination.) \square

Note: e_j standard basis vectors for \mathbb{R}^l . Then $\gamma_n e_j = v_n^j$

Since our proof is only up to $SL(l, \mathbb{Z})$, we may replace g_n by $g_n \gamma_n$.

\Rightarrow we have $v_n^j = e_j$.

$$\prod_{i=2}^l \left\| \text{proj}_{\{g_n v_n^1, \dots, g_n v_n^{i-1}\}} v_n^i \right\| = \text{vol}(\mathbb{Q}) = 1 \quad (**)$$

Goal: show that the sequence $g_n v_n^i$ is bounded.

Claim: $\left\| \text{proj}_{\{g_n v_n^1, \dots, g_n v_n^{i-1}\}} g_n v_n^i \right\| \geq \left\| \text{proj}_{\{g_n v_n^1, \dots, g_n v_n^{i-2}\}} g_n v_n^{i-1} \right\| \cdot \frac{1}{2}$

We can replace v_n^2 by $v_n^2 + k v_n^1$ ($k \in \mathbb{Z}$) in the above construction; all properties remain satisfied.

We do an almost Gram-Schmidt:

we want to replace v_n^2 by $v_n^2 - \frac{\langle v_n^1, v_n^2 \rangle}{\langle v_n^1, v_n^1 \rangle} \cdot v_n^1$, but this won't work since the fraction may not be in \mathbb{Z} .

Instead: we take the closest integer

$$\Rightarrow \left\| \text{proj}_{v_n^1} g_n v_n^2 \right\| \leq \frac{1}{2} \|g_n v_n^1\|$$

$$\Rightarrow \|g_n v_n^1\| \leq \|g_n v_n^2\| = \left\| \text{proj}_{v_n^1} g_n v_n^2 \right\| + \left\| \text{proj}_{v_n^1}^\perp g_n v_n^2 \right\|$$

$$\uparrow \text{by minimality} \leq \left\| \text{proj}_{v_n^1} g_n v_n^2 \right\| + \frac{1}{2} \|g_n v_n^1\| \quad \text{Same for higher indices.}$$

Combine this with (**): $\Rightarrow \|g_n v_n^i\|$ is bounded \Rightarrow the matrix entries

$g_n \gamma_n$ are bounded

Note that the above proof does not use the yet to be proven fact that $SL(l, \mathbb{Z})$ is a lattice.

We continue working towards the Borel Density Theorem.

The Borel Density Theorem

Thm. (Borel, but not the BDT)

Assume that G has no compact factors, G is connected;

V is a finite dimensional \mathbb{R} - or \mathbb{C} -vector space;

$\rho: G \rightarrow GL(V)$ is a cont. homomorphism.

1) Then every $\rho(\Gamma)$ -invariant vector in V is $\rho(G)$ -invariant.

2) Then every $\rho(\Gamma)$ -invariant sub-vector space $W \subseteq V$ is $\rho(G)$ -invariant.

(i.e. if the lattice does not do anything interesting, neither can the group.)

Pf: Application of ergodic theory: combination of probability measures and group theory. $\mathbb{K} = \mathbb{R}$ or \mathbb{C}

Note that 2) \Rightarrow 1):

Suppose Γ fixes $v \Rightarrow \Gamma$ fixes $\mathbb{K}v \stackrel{2)}{\Rightarrow} G$ fixes $\mathbb{K}v$

Then we get a homomorphism $G \rightarrow \mathbb{K}^\times$.

Claim: this is trivial.

$N := \text{Ker}(G \rightarrow \mathbb{K}^\times) \subseteq G$ closed normal subgroup

Semisimplicity $\Rightarrow N = G$ or $N = \{e\}$. The latter cannot happen since then $G \cong \mathbb{K}^\times$, but semisimple groups are non-abelian.

$\Rightarrow N = G$, i.e. $G \rightarrow \mathbb{K}^\times$ is trivial, G fixes v .

Lemma. (Poincaré Recurrence Theorem)

Let (X, d) be a separable metric space, $T: X \rightarrow X$ (translation), μ a T -invariant Borel measure, $\mu(X) < \infty$.

Then for μ -a.e. $x \in X$ $\exists n_k \rightarrow \infty$ sequence s.t. $T^{n_k} x \rightarrow x$.

Pf: $A_\epsilon := \{a \in X \mid \forall m > 0 \quad d(T^m a, a) > \epsilon\}$ "bad" points

STS: $\forall \epsilon > 0 \quad \mu(A_\epsilon) = 0$

\nexists Suppose not. Claim: $\exists B \subseteq A_\epsilon$ with $\mu(B) > 0$, $\text{diam}(B) < \epsilon$

PF OF CLAIM: Separability $\Rightarrow A_\varepsilon$ is the countable union of fin. many balls.

$$0 < \mu(A_\varepsilon) < \sum_{i=1}^{\infty} \mu(A_\varepsilon \cap B_\varepsilon(p_i)) \Rightarrow \exists p_i: \mu(A_\varepsilon \cap B_\varepsilon(p_i)) > 0$$

Set $B := A_\varepsilon \cap B_\varepsilon(p_i)$. This satisfies the conditions.

$$\mu(T^{-m}B) = \mu(B) \quad \forall m$$

$$\exists n > m: T^{-m}B \cap T^{-n}B \neq \emptyset \quad \text{since } \mu(X) < \infty$$

$$\stackrel{T^n}{\Rightarrow} T^{n-m}B \cap B \neq \emptyset$$

$$\Rightarrow \exists x \in B: d(T^m x, x) < \varepsilon.$$

PF OF 1): Let v be a fixed vector of $\rho(\Gamma)$. Goal: $\rho(G)$ fixes v .

Non-optimality $\Rightarrow \exists u \in G \setminus \{e\}$ unipotent elt

$$\underline{\text{Claim}}: N := \{u \in G, u \text{ unipotent}\} = G.$$

PF: Fact: unipotency is conjugacy invariant.

$\Rightarrow N$ normal and closed \Rightarrow we are done if G is simple.

If not: same for each factor.

New goal: show that every unipotent in G fixes v .

Since v is a $\rho(\Gamma)$ -fixed vector, we get a map

$$\bar{\rho}: G/\Gamma \rightarrow V$$

$$g\Gamma \mapsto \rho(g)v$$

Thus if ν is the finite volume G -invariant measure on G/Γ , then

$\bar{\nu} := \rho_* \nu$ is a finite volume measure on V .

Poincaré recurrence \Rightarrow if $u \in G$ unipotent then $(\rho(u^n g)v)_{n \in \mathbb{N}}$ has a convergent subsequence for a.e. $g \in G$.

Claim: The coordinates of $\rho(u^n g)v$ are polynomial functions of n .

Claim \Rightarrow 1): the only polynomial having a convergent subseq of values is a constant. $\Rightarrow \rho(u^n g)v$ constant for a.e. g

By continuity, $\rho(u^n)v$ is constant $\Rightarrow \rho(g)v = v \quad \forall g \in G$.

PF OF CLAIM: This is where we will use unipotency.

Claim': $\rho(u)$ is unipotent.

Claim' \Rightarrow Claim: $u \in GL(V)$ unip. $\Leftrightarrow \exists N \in \text{Mat}(V), k \in \mathbb{N}: u = \text{Id} + N, N^k = 0$.

$$u^n v = (\text{Id} + N)^n v = \sum_{l=0}^n \binom{n}{l} N^l v = \sum_{l=0}^k \binom{n}{l} N^l v, \text{ which is polynomial in } n.$$

PF OF CLAIM': Recall that $\exists a_u \in SL_2(\mathbb{R})$ st. $a_u \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix} a_u^{-1} \rightarrow \text{Id}$.

$$\rho \left(a_u \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix} a_u^{-1} \right) \rightarrow \text{Id}_V$$

Matrix \Rightarrow char poly is continuous $\Rightarrow \rho \left(\begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix} \right)$ has the same char poly as $\text{Id} \Rightarrow$ all eigenvalues are 1 \Rightarrow unipotency.

Jacobson-Morosov lemma \Rightarrow same for all unip. G .

This finishes the proof of 1). C
C
1

Now we prove 2). We start with a technical Prop. from meas. thy. 08.05.2018

Prop.: Assume G to be connected with no compact factors,

V to be a fin. dim. \mathbb{R} - or \mathbb{C} -vector space,

$\rho: G \rightarrow GL(V)$ to be a cont. homomorphism

μ to be a $\rho(G)$ -invariant vector space on $\mathbb{P}(V) = V \setminus 0 / \sim_{\mathbb{K}^\times}$

(note that ρ descends to an action on $\mathbb{P}(V)$, thus the above is valid)

such that $\mu(\mathbb{P}(V)) < \infty$.

Then μ is supported on $\text{Fix}(G) \stackrel{\text{def}}{=} \{[v] \in \mathbb{P}(V) \mid g[v] = [v] \quad \forall g \in G\}$.

PF OF PROP: Sts μ is supported on fixed points of

$$\{\rho(u) \mid u \in G, u \text{ unipotent}\},$$

just as in the pf. of 1). Recall that u unip. $\Rightarrow \rho(u)$ is unip.

$T = \rho(u) - \text{Id}$, $T^k \neq 0$ for some $k \in \mathbb{N}$, $T^{k+1} = 0$.

$$\rho(u) T^k v = (\text{Id} + T) T^k v = T^k v \Rightarrow [T^k v] \text{ is fixed by } \rho(u).$$

Moreover,

$$\rho(u^n)[v] = \rho(u)^n [v] = \left[\sum_{r=0}^k \binom{n}{r} T^r v \right] = \left[\binom{n}{k}^{-1} \sum_{r=0}^k \binom{n}{r} T^r v \right] \rightarrow [T^k v]$$

↑
projective space

as $n \rightarrow \infty$.

PRT: μ -a.e. $[v] \in P(V)$: $\exists (n_k)_{k \in \mathbb{N}}$ s.t. $\rho(u^{n_k})[v] \rightarrow [v]$.

$\Rightarrow \mu$ -a.e. $[v] \in P(V)$ is of the form $[T^k v]$, hence a fixed pt of $\rho(u)$.

Now we truly start proving 2).

Let W be a fixed subspace of $\rho(\Gamma)$, $d = \dim W$.

Consider the homomorphism $\hat{\rho}: G \rightarrow GL(\wedge^d V)$ induced by ρ .

If W has basis e_1, \dots, e_d then $\{e_{i_1} \wedge \dots \wedge e_{i_d} \mid \forall i_j \in \{1, \dots, d\}\}$ is a basis of $\wedge^d W$

when subject to the relation $e_{i_1} \wedge \dots \wedge e_{i_j} \wedge e_{i_{j+1}} \wedge \dots \wedge e_{i_d} = -e_{i_1} \wedge \dots \wedge e_{i_{j+1}} \wedge e_{i_j} \wedge \dots \wedge e_{i_d}$

Since W is $\rho(\Gamma)$ -invariant, $\wedge^d W$ is a 1-dim invariant subspace of $\hat{\rho}(\Gamma)$.

$\Rightarrow [\wedge^d W] \in P(\wedge^d V)$ is a fixed pt of $\hat{\rho}(\Gamma) \curvearrowright P(\wedge^d V)$

We get a map $\bar{\rho}: G/\Gamma \rightarrow P(\wedge^d V)$

$$g\Gamma \longmapsto g[\wedge^d W];$$

well-definedness follows from the above discussion.

We get a finite volume $\hat{\rho}(G)$ -invariant measure $\bar{\nu} := \bar{\rho}_* \nu$.

By the Prop.: $\bar{\rho}(G/\Gamma) = \text{supp } \bar{\nu} \subseteq \text{Fix}(G)$

\uparrow def. of $\bar{\nu}$ \uparrow Prop.

$\Rightarrow \bar{\rho}(e\Gamma) = [\wedge^d W]$ fixed by $\forall g \in G$

$\Rightarrow W$ is fixed by $\forall g \in G$

~~Since the action is continuous, W is fixed by $\forall g \in G$.~~

For the remainder of lecture 8, suppose that G is connected with no qpt. factors.

Cor. $H < G$ connected closed subgroup s.t. $\gamma H \gamma^{-1} = H \quad \forall \gamma \in \Gamma \Rightarrow H < G$.

Pf. \mathfrak{h} : the Lie algebra of H (i.e. the tangent space at $e \in H$)

\mathfrak{h} is a vector subspace of \mathfrak{g} , the Lie algebra of G .

Γ normalises $H \Rightarrow \mathfrak{h}$ is invariant under $\text{Ad}_G \Gamma = \{\text{int. autom. } G \rightarrow \text{GL}(\mathfrak{g})\}$

Thm. 2) $\Rightarrow \mathfrak{h}$ is invariant under $\text{Ad}_G G$

H closed, connected $\xrightarrow[\text{theory}]{\text{Lie}}$ $H < G$. □

Cor. $C_G(\Gamma) \stackrel{\text{def}}{=} \{g \in G \mid g\gamma = \gamma g \quad \forall \gamma \in \Gamma\} = Z(G) \stackrel{\text{def}}{=} \{g \in G \mid g h = h g \quad \forall h \in G\}$.

Pf. G linear $\Rightarrow G \subseteq \text{SL}_\ell(\mathbb{R})$ for some $\ell \Rightarrow G \subseteq \text{Mat}_{\ell \times \ell}(\mathbb{R})$

Define $\rho: G \longrightarrow \text{GL}(V)$

$(\rho(g))^{-1} A \rho(g) \longmapsto g A g^{-1}$

If $c \in C_G(\Gamma) \Rightarrow \rho(\gamma)c = c \quad \forall \gamma \in \Gamma$

Thm. 1) $\Rightarrow \rho(g)c = c \quad \forall g \in G \Rightarrow c \in Z(G) \Rightarrow C_G(\Gamma) \subseteq Z(G)$. □

The inclusion $C_G(\Gamma) \supseteq Z(G)$ always holds.

Cor. $N < \Gamma$ finite $\Rightarrow N < Z(G)$. (Note that $N < Z(G) \Rightarrow N < G$ always holds.)

Pf. $\Gamma \curvearrowright N$ by $\gamma \cdot n = \gamma n \gamma^{-1} \quad \forall \gamma \in \Gamma, n \in N$.

$\gamma \in \Gamma$ acts trivially on N iff $\gamma \in C_\Gamma(N)$

We get a map $\Gamma / C_\Gamma(N) \hookrightarrow \text{Aut}(N)$.

By the finiteness assumption, $|\text{Aut}(N)| \leq |N|! < \infty$

$\Rightarrow \Gamma / C_\Gamma(N)$ is finite $\Rightarrow |\Gamma : C_\Gamma(N)| < \infty$. Hence $C_\Gamma(N)$ is a lattice in Γ .

(Check all the properties as an EXERCISE.)

$N < C_G(C_\Gamma(N)) = Z(G)$ by the prev. Cor. □

Cor. $|N_G(\Gamma) : \Gamma| < \infty$.

Pf. Claim. $N_G(\Gamma)^\circ$ centralises Γ .

Γ discrete. Hence if $g\gamma g^{-1} \in \Gamma$ & g is close to e then $g\gamma g^{-1} = \gamma$.

(This could be made rigorous.) This proves the Claim.

$N_G(\Gamma)^\circ \subseteq C_G(\Gamma) = Z(G)$ is finite

$\Rightarrow N_G(\Gamma)^\circ$ is trivial. $\Rightarrow N_G(\Gamma)$ is discrete.

$\Rightarrow N_G(\Gamma)$ has a strict fundamental domain in G

Set $F := \{f_i\}_{i \in I}$ as a set of coset representatives for $N_G(\Gamma)/\Gamma$.

Let \mathcal{F} be a strict fund. domain for $N_G(\Gamma)/\Gamma$

$\Rightarrow \bigcup_{i \in I} f_i \mathcal{F}$ is a strict fund. domain for Γ .

$\Rightarrow F \cdot \mathcal{F}$ is of finite volume $\Rightarrow F$ is finite. $\Rightarrow |N_G(\Gamma) : \Gamma| < \infty$

Zariski topology (intermezzo)

Def. $\mathbb{R}[x_{11}, \dots, x_{ee}] \ni q, A \in \text{Mat}_{e \times e}(\mathbb{R}), q(A)$ is defined entry-wise, substituting $x_{ij} := a_{ij}$.

Def. $S \subseteq \text{Mat}_{e \times e}(\mathbb{R})$ is Zariski-closed if $\exists Q \subseteq \mathbb{R}[x_{11}, \dots, x_{ee}]$ s.t.

$$S = \left\{ A \in \text{Mat}_{e \times e}(\mathbb{R}) \mid q(A) = 0 \quad \forall q \in Q \right\}.$$

Ex. These form the closed sets of a topology on $\text{Mat}_{e \times e}(\mathbb{R})$.

Def. The Zariski closure of $X \subseteq \text{Mat}_{e \times e}(\mathbb{R})$ is its closure in the Zariski topology, denoted as \overline{X}^Z .

Ex. $SL_2(\mathbb{R})$ is Zariski-closed.

$H = \left\{ \begin{pmatrix} e^t & e^{-t} \\ 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbb{R} \right\}$ is not Zariski-closed, a polynomial does not recognize an exponential (non-precise)

$\overline{H}^Z = \left\{ \begin{pmatrix} 1/a & a \\ 1 & t \\ 0 & 1 \end{pmatrix} \mid a, t \in \mathbb{R}, a \neq 0 \right\}$ This is not the same as the closure in the usual topology.

Recall. $\mathbb{R}[x_1, \dots, x_n]$ is noetherian \Rightarrow any Zariski-closed set can be described with finitely many polynomials

Thm. (Borel Density Theorem) Γ is Zariski-dense in G , i.e. $\overline{\Gamma}^Z = G$.

Pr. $(\overline{\Gamma}^Z)^\circ < G$ Ex. check this. (Every operation is algebraic, polynomials are algebraic, taking the conn. component is continuous.)

$(\overline{\Gamma}^Z)^\circ$ is closed in G (Ex.)

Γ normalises $(\overline{\Gamma}^Z)^\circ \Rightarrow G$ normalises $(\overline{\Gamma}^Z)^\circ \Rightarrow (\overline{\Gamma}^Z)^\circ = G$.
 G semis.
 Γ lattice

Further properties of lattices (no proofs)

15.05.2018 □

Recall. For a set S , $S^{-1} = \{s^{-1} \mid s \in S\}$ where s^{-1} is just a formal symbol.

$F(S) = \{\text{all words on } S \cup S^{-1} \text{ containing no substring of the form } ss^{-1} \text{ or } s^{-1}s, s \in S\}$

Multiplication = concatenation followed by reduction of substrings $ss^{-1}, s^{-1}s$

$|S| = |S'| \Rightarrow F(S) \cong F(S')$, so we write $F_{|S|}$ for $F(S)$

Def. H group is finitely generated if $F_r \twoheadrightarrow H$ for some r .

H is finitely presented if in addition $\exists R \subset F_r$ s.t. $\ker(F_r \twoheadrightarrow H)$ is the smallest normal subgroup containing R .

Notation. H fin. pres. gp., S fin. set., $R \subset F(S)$ as above, i.e. $\langle\langle R \rangle\rangle = \ker(F(S) \twoheadrightarrow H)$ normally generated subgroup

then we write $G = \langle S \mid R \rangle$.

Thm. Γ is finitely presented. □

Def. A group H is torsion free if $\nexists n \in \mathbb{N}, h \in H: h^n = e$ for $h \neq e$.

$SL_2(\mathbb{Z})$ is not torsion free: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Thm. (Selberg's Lemma, PO) Γ has a torsion free finite index subgroup. □

5. Arithmetic groups

We want to generalise $SL_n(\mathbb{Z}) < SL_n(\mathbb{R})$: given $G < SL_n(\mathbb{R})$ take $G \cap SL_n(\mathbb{Z})$.

Problem. $\exists B \in SL_n(\mathbb{Z})$ s.t. $BGB^{-1} \cap SL_n(\mathbb{Z}) = \{e\}$ Ex. 5.1.1.

Hence in order to get an interesting theory of groups we need to do something more: in particular, we need \mathbb{Q} to get involved.

Prop. $W \subset \mathbb{R}^l$ subspace. Then TFAE:

- 1) $W \cap \mathbb{Z}^l$ is a cocompact lattice in W
- 2) W is spanned by $W \cap \mathbb{Z}^l$
- 3) $W \cap \mathbb{Q}^l$ is dense in W
- 4) W can be defined by linear equations over \mathbb{Q} .

Pf: 1) \rightarrow 2): $V = \text{Span}_{\mathbb{R}}(W \cap \mathbb{Z}^l) < W \Rightarrow W/V = \mathbb{R}^d$ for some $d \in \mathbb{N}$

$W \cap \mathbb{Z}^l \subset V \rightarrow$ we have a cont. ^{surj.} map $\underbrace{W/W \cap \mathbb{Z}^l}_{\text{cocomp.}} \rightarrow W/V = \mathbb{R}^d$

$\Rightarrow d = 0$. by compactness.

2) \rightarrow 1): $\{e_1, \dots, e_k\}$ basis of \mathbb{R}^k . $\exists T: \mathbb{R}^k \rightarrow W$ lin. isom.

s.t. $\{T(e_j)\}_j \subseteq W \cap \mathbb{Z}^l \Rightarrow T(\mathbb{Z}^k) \subseteq W \cap \mathbb{Z}^l$

$\mathbb{R}^k / \mathbb{Z}^k$ is cpt., T is continuous, $\Rightarrow W \cap \mathbb{Z}^l \subset W$ is a lattice

2) \rightarrow 3): $\mathbb{Q} \subset \mathbb{R}$ dense $\Rightarrow T(\mathbb{Q}^l)$ is dense

4) \rightarrow 2): W solution space to lin. eqs. over \mathbb{Q}

\rightarrow we can find a basis of vectors with \mathbb{Q} -coefficients

Multiply with denominators $\rightarrow \mathbb{Z}$ -basis.

3) \rightarrow 4): $\mathbb{Q}^l \cap W \subset W$ dense

$W^\perp = \{x \in \mathbb{R}^l \mid wx = 0 \ \forall w \in W \cap \mathbb{Q}^l\}$, this is def'd by lin. equations $/\mathbb{Q}$

\rightarrow has a \mathbb{Q} -basis $\Rightarrow W = (W^\perp)^\perp$ is def'd by lin. equations $/\mathbb{Q}$.

Def. Let $H < SL(l, \mathbb{R})$ be a closed subgroup. We say that H is defined over \mathbb{Q} if

$$\exists Q \subseteq \mathbb{Q}[x_{11}, \dots, x_{ll}] \text{ s.t. } \bullet \text{Var}(Q) = \{g \in SL(l, \mathbb{R}) \mid q(g) = 0 \ \forall q \in Q\} \subseteq SL(l, \mathbb{R}) \text{ subgroup,}$$

$$\bullet H^{\circ} = \text{Var}(Q)^{\circ},$$

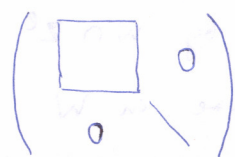
$\bullet H$ has only fin. many connected components.

In other words, H is countable to a group def'd by polynomials with \mathbb{Q} -coefficients.

Ex. 1) $SL(l, \mathbb{R})$, $Q = \emptyset$

2) $n < l$, $SL(n, \mathbb{R})$ in the top left corner of $SL(l, \mathbb{R})$,

$$Q = \{x_{ij} - \delta_{ij} \mid \max(i, j) > n\}$$



3) $A \in SL(l, \mathbb{Q})$

$$SO_l(A, \mathbb{Q}) = \{g \in SL(l, \mathbb{R}) \mid gAg^T = A\}$$

Rule. By countability, Q can always be chosen to be finite.

Prop. G is isogenous to a group defined over \mathbb{Q} .

PF. Go over the list.

Notation. $\mathcal{O} \subset \mathbb{R}$ ring, $1 \in \mathcal{O}$. Then define $G_{\mathcal{O}} := G \cap SL(l, \mathcal{O})$

Ex. $\varphi: SL(n, \mathbb{C}) \hookrightarrow SL(2n, \mathbb{R})$ embedding

$$\text{Then } \varphi(SL(n, \mathbb{C}))_{\mathbb{Q}} = \varphi(SL(n, \mathbb{Q}[i])),$$

$$\varphi(SL(n, \mathbb{C}))_{\mathbb{Z}} = \varphi(SL(n, \mathbb{Z}[i]))$$

Prop. $H < SL(l, \mathbb{R})$ connected, almost Zariski closed subgroup.

Then H is def'd over \mathbb{Q} iff $H_{\mathbb{Q}} < H$ is dense.

Def. H is almost Zariski closed if

$\bullet H$ has finitely many connected components

$\bullet \exists H_1 < SL(l, \mathbb{R})$ Zariski-closed s.t. $H^{\circ} = H_1^{\circ}$.

Thm. G def'd over $\mathbb{Q} \Rightarrow G_{\mathbb{Z}}$ lattice.

A lattice of the form $G_{\mathbb{Z}}$ is called arithmetic (not in the most general form yet).

For slightly more flexibility: we want the following

- G_1, G_2 \mathbb{Q} -groups, $\varphi: G_1 \rightarrow G_2$ iso.

If $\Gamma < G_1$ arithmetic then we want that $\varphi(\Gamma) < G_2$ is arithmetic.

- we want to ignore cpt factors
- Γ_1 comm. to Γ_2 and Γ_1 arith. $\Rightarrow \Gamma_2$ arith.

Def. $\Gamma < G$ arithmetic if

- $\exists G' < SL(n, \mathbb{R})$ closed conn. semisimple subgroup of $SL(n, \mathbb{R})$ for some n ; G' def'd over \mathbb{Q}
- $\exists K < G, K' < G'$ compact normal subgrps.
- $\exists \varphi: G^0/K \rightarrow G'/K'$ iso s.t. $\varphi(\overline{\Gamma})$ is commensurable to $\overline{G'_{\mathbb{Z}}}$, where

$$\overline{\Gamma} = G^0 \cap \Gamma / \Gamma \cap K \quad \text{and} \quad \overline{G'_{\mathbb{Z}}} = G'_{\mathbb{Z}} / G'_{\mathbb{Z}} \cap K'$$
 ($\overline{\cdot}$ does not mean Zariski closure)

Examples. • $SL(2, \mathbb{Z})$

• $SO(A, \mathbb{R})_{\mathbb{Z}}, \quad A \in S\mathbb{Q}(2, \mathbb{Q})$

• $\varphi: SL(n, \mathbb{C}) \xrightarrow{\sim} SL(2n, \mathbb{R})$.

$\varphi(SL(n, \mathbb{Z}[i])) = \varphi(SL(n, \mathbb{C}))_{\mathbb{Z}}$

• $SL(2, \mathbb{Z}) < SL(2, \mathbb{R})$

$N \in \mathbb{N}: \Gamma(N) = \left\{ g \in SL(2, \mathbb{Z}) \mid g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{matrix} a \equiv d \equiv 1 \pmod{N} \\ b \equiv c \equiv 0 \pmod{N} \end{matrix} \right\} < SL(2, \mathbb{Z})$

$\Gamma(N)$ is of finite index. To see this, consider the reduction

$r_N: SL(2, \mathbb{Z}) \rightarrow SL(2, \mathbb{Z}/N\mathbb{Z})$; and recognize that $\Gamma(N) = \ker(r_N)$.

Prop. • G has no cpt factors $\Rightarrow K$ is finite.

- Since there are only countably many finite subsets of $\mathbb{Q}[x_1, \dots, x_{2n}]$, there are only countably many arithmetic lattices.

Two big theorems by Margulis

Thm. (Margulis)

- If G is not isogenous to $SO(1, n) \times K$ or $SU(1, n) \times K$ for any cpt Lie group K ;
 - $\Gamma < G$ is an irreducible lattice,
- then Γ is arithmetic.

Note: $SL(2, \mathbb{R})$ is isog. to $SO(1, 2)$

$SL(2, \mathbb{C})$ is isog. to $SO(1, 3)$ \Rightarrow the Margulis thm. does not apply

Recall: $\text{Comm}_G(\Gamma) = \{g \in G / \Gamma g \Gamma g^{-1} < \Gamma \text{ is of finite index}\}$

Exc. If G is def'd over \mathbb{Q} then $\text{Comm}_G(G_{\mathbb{Z}}) > G_{\mathbb{Q}}$ (EXERCISE 4.8.11)

So if Γ is arithmetic, G is connected and has no split factors then $\text{Comm}_G(\Gamma) < G$ is dense.

Thm. (Margulis, Commensurability criterion for arithmeticity)

$\Gamma < G$ is arithmetic iff $\text{Comm}_G(\Gamma) < G$ is dense.

Prop. (Godement compactness criterion)

G def'd over \mathbb{Q} . Then $G/G_{\mathbb{Z}}$ is cpt iff $G_{\mathbb{Z}}$ does not contain any nontrivial nilpotent elts.

Pf: $G/G_{\mathbb{Z}}$ cpt. $\Rightarrow G_{\mathbb{Z}}$ contains no nontrivial nilp. elts, this was already seen for lattices.

$G/G_{\mathbb{Z}}$ noncpt, WTS $\exists \gamma \in G_{\mathbb{Z}}$ nontrivial nilpotent

$G_{\mathbb{Z}}$ noncpt lattice $\Rightarrow \text{Id}$ is an accumulation point of $G_{\mathbb{Z}}$.

$\Rightarrow \exists g \in G, \gamma \in G_{\mathbb{Z}}$ s.t. $g\gamma \approx \text{Id}$.

$\Rightarrow \text{char}_{\gamma}(x) = \text{char}_{g\gamma}(x) \approx (x-1)^l$

$\Rightarrow \text{char}_{\gamma}(x) = (x-1)^l \Rightarrow \gamma$ nilpotent. □

Thm. G has no cpt factors, $\Gamma < G$ arithmetic.

Then G/Γ cpt. $\Leftrightarrow \Gamma$ has no nontrivial unipotent elt.

Pf: Consequence of the previous Prop. (i.e. the GCC).

Prop. If $B: \mathbb{Q}^l \times \mathbb{Q}^l \rightarrow \mathbb{Q}$ is a symmetric bilinear form,

$B(x, x) \neq 0 \quad \forall x \in \mathbb{Q}^l \setminus \{0\}$.

Then $SO(B)_{\mathbb{Z}} < SO(B)_{\mathbb{R}}$ is cocompact, where $SO(B) = \left\{ g \in SL(l, \mathbb{R}) \mid B(gv, gw) = B(v, w) \right\}^*$
 $\forall v, w \in \mathbb{R}^l$

Pf: We will use the Mautner compactness criterion.

Let $G = SO(B)_{\mathbb{R}}$, $\Gamma = G_{\mathbb{Z}}$, assume $B(\mathbb{Z}^l, \mathbb{Z}^l) \subseteq \mathbb{Z}$.

* Technically B takes rational vectors as arguments, but we may $\otimes \mathbb{R}$.

We can do this because $\tilde{B} = \frac{1}{d} \cdot B$ is such a form
 d denominator in the coeffs of B
 and $SO(B) = SO(\tilde{B})$.

1) Use MCC to show that $\pi(G)$ is precompact where

$\pi: SL(l, \mathbb{R}) \rightarrow SL(l, \mathbb{R}) / SL(l, \mathbb{Z})$ is the projection map.

2) Show that $\pi(G)$ is closed, hence cpt.

3) Show that $G/\Gamma \rightarrow SL(l, \mathbb{R}) / SL(l, \mathbb{Z})$ is a homeo onto $\pi(G)$.

Since $\pi(G)$ is cpt, this finishes the proof.

1) $\{g_n \in G, v_n \in \mathbb{Z}^l \setminus \{0\} \text{ s.t. } g_n v_n \rightarrow 0\}$

$B(\mathbb{Z}^l, \mathbb{Z}^l) \subseteq \mathbb{Z} \Rightarrow 1 \leq |B(v_n, v_n)| = |B(g_n v_n, g_n v_n)| \rightarrow 0 \quad \zeta$

2) Suppose $g_n \gamma_n \rightarrow h \in SL(l, \mathbb{R})$ for $g_n \in G, \gamma_n \in SL(l, \mathbb{Z})$.

WTS $h \in G \cdot SL(l, \mathbb{Z})$.

Let $\{e_1, \dots, e_l\}$ be the std. basis of \mathbb{R}^l .

$B(\gamma_n e_j, \gamma_n e_k) \in \mathbb{Z}$

$B(g_n \gamma_n e_j, g_n \gamma_n e_k) = B(\gamma_n e_j, \gamma_n e_k)$

$\downarrow n \rightarrow \infty$

$B(h e_j, h e_k)$

$\exists n_0 \in \mathbb{N}$ s.t. $B(\gamma_n e_j, \gamma_n e_k) = B(e_j, e_k)$ $\forall n > n_0$ by discreteness

$(\gamma_n e_j)_j$ is a basis in \mathbb{R}^l and $B((h\gamma_n^{-1})\gamma_n e_j, (h\gamma_n^{-1})\gamma_n e_k) = B(\gamma_n e_j, \gamma_n e_k)$,

implying the claimed equality above.

Thus $h\gamma_n^{-1} \in SO(B)$, as desired.

3) $\varphi: G/\Gamma \longrightarrow SL(l, \mathbb{R})/SL(l, \mathbb{Z})$ G/Γ is a T2-space.
 $g\Gamma \longmapsto gSL(l, \mathbb{Z})$

Automatically bijective with compact image. $\pi(G)$.

STS: $\varphi^{-1}: \pi(G) \longrightarrow G/\Gamma$ is continuous. (Point set topology fact: if $f: X \rightarrow Y$ is bijective, continuous, X cpt, Y T2 $\Rightarrow f$ homeo.)

Suppose $\varphi(g_n \Gamma)$ converges. WTS $g_n \Gamma$ converges.

$\exists (\gamma_n)_n$ sequence in $SL(l, \mathbb{Z})$, $\exists h \in G$ s.t. $g_n \gamma_n \rightarrow h$.

Use the proof of 2) (i.e. discreteness argument) $\Rightarrow h \in G \gamma_n$ for $n \gg 1$.

$\Rightarrow \gamma_n \in G h = G$. $\Rightarrow \gamma_n \in \underbrace{G \cap SL(l, \mathbb{Z})}_{\Gamma}$ for $n \gg 1$

$\Rightarrow g_n \Gamma \rightarrow h \Gamma$, as desired. □

Thm. (Legendre) $a, b, c \in \mathbb{Z} \setminus \{0\}$ square-free, pairwise rel. prime, do not all

29.05.2018

have the same sign. Then $\exists (x, y, z) \in \mathbb{Z}^3 \setminus \{0\}$ s.t. $ax^2 + by^2 + cz^2 = 0$

iff $\exists u, v, w \in \mathbb{Z}$ s.t.

$$-ab \equiv u^2 \pmod{c}$$

$$-bc \equiv v^2 \pmod{a}$$

$$-ac \equiv w^2 \pmod{b}$$

PO, not hard, see "A classical intro to modern number theory" by K. Ireland, M. Rosen, Ch. 17 § 3. □

Ex. $q_1(x, y, z) := x^2 + y^2 - z^2 \rightsquigarrow q_1(1, 0, 1) = 0$, \exists nontrivial isotropic vector

$q_2(x, y, z) := 11x^2 + 7y^2 - 5z^2$ has no nontrivial isotropic vectors:

$$-7 \cdot 11 = -77 \equiv 3 \pmod{5}$$

Note that over \mathbb{R} these two forms are cogredient, so q_2 does have nontrivial isotropic vectors, just not in \mathbb{Z}^3 .

Fact. (to be proven later) $SO(B_1)_{\mathbb{Z}} < SO(B_1)_{\mathbb{R}} = SO(2,1)$ non-cocpt

$SO(B_2)_{\mathbb{Z}} < SO(B_2)_{\mathbb{R}} \cong SO(2,1)$ cocpt.

Basis-free definition of arithmetic groups

So far we have always implicitly chosen a basis.

Def. V a linear vector space

1) A \mathbb{Q} -subspace $V_{\mathbb{Q}}$ of V is called a \mathbb{Q} -form of V if the \mathbb{R} -lin. map

$V_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R} \rightarrow V$ is an isomorphism.

$$v \otimes t \mapsto tv$$

2) A polynomial $f: V \rightarrow \mathbb{R}$ is defined over \mathbb{Q} wrt. a \mathbb{Q} -form $V_{\mathbb{Q}}$

if $f(V_{\mathbb{Q}}) \leq \mathbb{Q}$.

3) A subgroup \mathfrak{L} of the additive group $V_{\mathbb{Q}}$ is called a \mathbb{Z} -lattice

if \bullet \mathfrak{L} is finitely generated

\bullet the \mathbb{Q} -linear map $\mathfrak{L} \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow V_{\mathbb{Q}}$ is an iso.

4) For a \mathbb{Q} -form $V_{\mathbb{Q}} \subset V$ let

$$\text{End}(V)_{\mathbb{Q}} := \{A \in \text{End}(V) \mid A(V_{\mathbb{Q}}) = V_{\mathbb{Q}}\}.$$

5) For a real vector space W a map $Q: W \rightarrow \mathbb{R}$ is a polynomial

if $\exists \varphi: \mathbb{R}^l \xrightarrow{\sim} W$ \mathbb{R} -linear isomorphism s.t. $Q \circ \varphi: \mathbb{R}^l \rightarrow \mathbb{R}$ is a polynomial in the usual sense.

6) A subgroup $H < SL(V)$ is defined over \mathbb{Q} wrt a \mathbb{Q} -form $V_{\mathbb{Q}} \subset V$ if

$\exists \mathcal{Q}$ set of polynomials on $\text{End}(V)$ s.t.

$\bullet \forall q \in \mathcal{Q}$ is defined over \mathbb{Q} wrt. $V_{\mathbb{Q}}$

$\bullet \text{Var}(\mathcal{Q}) = \{g \in SL(V) \mid q(g) = 0 \forall q \in \mathcal{Q}\}$ is a subgroup of $SL(V)$

$\bullet \text{Var}(\mathcal{Q})^{\circ} < H$ is of finite index.

Remark. $V_{\mathbb{Q}} = \mathbb{Q}^n \leq \mathbb{R}^n$ yields our previous definition.

Lemma. \uparrow V real vector space with a \mathbb{Q} -form $V_{\mathbb{Q}}$.

Then $\exists \varphi: V \xrightarrow{\sim} \mathbb{R}^l$ \mathbb{R} -lin. iso s.t. $\varphi(V_{\mathbb{Q}}) = \mathbb{Q}^l$.

Furthermore if $\mathfrak{L} \subset V_{\mathbb{Q}}$ is any \mathbb{Z} -lattice then we may choose φ s.t.

$$\varphi(\mathfrak{L}) = \mathbb{Z}^l.$$

2) A polynomial $f: \mathbb{R}^d \rightarrow \mathbb{R}$ is defined over \mathbb{Q} wrt. \mathbb{Q}^d iff the coefficients of f are in \mathbb{Q} .

Prop. $G < GL(V)$ defined over \mathbb{Q} wrt. $V_{\mathbb{Q}}$. Then

1) For any \mathbb{Z} -lattice L in $V_{\mathbb{Q}}$:

$$G_L = \{g \in G \mid gL = L\}$$

is an arithmetic subgroup.

2) If L_1, L_2 are \mathbb{Z} -lattices then G_{L_1} and G_{L_2} are commensurable.

Lemma. 3) If $L_1, L_2 < V_{\mathbb{Q}}$ \mathbb{Z} -lattices then $\exists p \in \mathbb{Z} \setminus \{0\}$ s.t.

$$pL_1 \leq L_2, \quad pL_2 \leq L_1$$

PF OF LEMMA: linear algebra, EXC.

PF OF PROP: use the Lemma.

Restriction of scalars

Need some alg. n.t., PO.

Recall: algebraic number field, ring of integers \mathcal{O}_F

$\{\sigma_1, \dots, \sigma_r\}$ embeddings into \mathbb{C}

$$\Delta: \mathcal{O}_F \longrightarrow \mathbb{C}^r$$

$$x \longmapsto (\sigma_1(x), \dots, \sigma_r(x))$$

$$\text{Exc. } SL(\ell, \mathbb{C}^r) \cong SL(\ell, \mathbb{C})^r$$

$$\Rightarrow SL(\ell, \mathcal{O}_F) \xrightarrow{\Delta} SL(\ell, \mathbb{C})^r \text{ homomorphism}$$

Note that as $\mathcal{O} < \mathbb{C}$ is discrete, $\Delta(\Gamma)$ is discrete $\forall \Gamma < SL(\ell, \mathcal{O}_F)$

Goal: if $\Gamma = G_{\mathcal{O}_F}$ and G is defined over F then

$\Delta(\Gamma) < SL(\ell, \mathbb{C})^r$ is an arithmetic subgroup.

Ex. $\Gamma = SL(2, \mathbb{Z}[\sqrt{2}])$, $G = SL(2, \mathbb{R}) \times SL(2, \mathbb{R})$, $\sigma: \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}$ the nontrivial embedding

$$\Delta: \Gamma \longrightarrow G$$

$$r \longmapsto (r, \sigma(r))$$

Claim. $\Delta(\Gamma)$ is an irreducible arithmetic subgroup of G .

Pf: $F = \mathbb{Q}(\sqrt{2}), \mathcal{O} = \mathbb{Z}[\sqrt{2}]$

$\{(1,1), (\sqrt{2}, -\sqrt{2})\}$ is a \mathbb{Q} -basis for $\Delta(F)$ and an \mathbb{R} -basis for \mathbb{R}^2

$\Rightarrow \Delta(F)$ is a \mathbb{Q} -form for \mathbb{R}^2 .

$\Rightarrow \Delta(F^2) = \{(u, \sigma(u)) \in F^2 \mid u \in F^2\}$ is a \mathbb{Q} -form for \mathbb{R}^4

and $\Delta(\mathcal{O})$ is a \mathbb{Z} -lattice in $\Delta(F^2)$

Moreover G is defined over \mathbb{Q} (Exc. 5.5.1, 5.5.2)

$\Rightarrow G_{\Delta(\mathcal{O}^2)}$ is an arithmetic subgroup of G by the prev. Prop.

and $G_{\Delta(\mathcal{O}^2)} = \Delta(\Gamma)$.

Irreducibility: $\{e\} = \Delta(\Gamma) \cap (SL(2, \mathbb{R}) \times \{e\}) \Rightarrow \Delta(\Gamma)$ is irreducible.

Addendum to this proof: the proof of discreteness is missing.

Discreteness follows from the fact that $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}: \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}$.

Def. F an algebraic number field.

1) Two distinct embeddings $\sigma_1, \sigma_2: F \hookrightarrow \mathbb{C}$ are called equivalent if $\sigma_1(x) = \overline{\sigma_2(x)} \quad \forall x \in F$.

2) A place of F is an equivalence class of embeddings $\sigma: F \hookrightarrow \mathbb{C}$.

• A place σ is called real if it contains a single embedding, i.e. $\sigma(F) \subseteq \mathbb{R}$.

• A place σ is called complex if it contains two embeddings, i.e. $\sigma(F) \not\subseteq \mathbb{R}$.

3) S^∞ := {places of F }

4) For $\sigma \in S^\infty$: F_σ := $\begin{cases} \mathbb{R} & \sigma \text{ real} \\ \mathbb{C} & \sigma \text{ complex} \end{cases}$

F_σ is called the completion of F at σ . (Note that $F \subset F_\sigma$ is dense.)

5) For $Q \subseteq F_\sigma[x_{11}, \dots, x_{ll}]$: $\text{Var}_{F_\sigma}(Q)$:= $\{g \in SL(l, F_\sigma) \mid q(g) = 0 \quad \forall q \in Q\}$

6) Suppose $G \in SL(2, \mathbb{R})$ is defined over F , i.e. $\exists Q \in F[x_1, \dots, x_{2\ell}]$ s.t. $G^\circ = \text{Var}(Q)^\circ$.
 Then $\forall \sigma \in S^\infty$ let $G^\sigma := \text{Var}_{F^\sigma}(\sigma(Q))^\circ$, called the Galois conjugate of G at σ .
 (Note that G^σ is defined over $\sigma(F)$.)

Prop. If G is defined over an algebraic number field $F \subseteq \mathbb{R}$ and \mathcal{O}_F is the ring of integers of F then $\exists \dot{G}_{\mathcal{O}_F} < G_{\mathcal{O}_F}$ finite index subgroup such that $\dot{G}_{\mathcal{O}_F}$ embeds as an arithmetic subgroup of $\prod_{\sigma \in S^\infty} G^\sigma$ via the natural embedding $\Delta: g \mapsto (\sigma(g))_{\sigma \in S^\infty}$.

Furthermore if G is simple then $\Delta(\dot{G}_{\mathcal{O}_F})$ is irreducible.

We give a proof through examples.

Ex. 1) $G = \text{SO}(x^2 + y^2 - \sqrt{2}z^2, \mathbb{R}) \cong \text{SO}(1, 2)$

Then $G_{\mathbb{Z}[\sqrt{2}]}$ is a cocompact arithmetic subgroup of G .

Pf of Ex: $\sigma: \mathbb{Q}[\sqrt{2}] \hookrightarrow \mathbb{C}$ the nontrivial embedding

$$\Gamma = G_{\mathbb{Z}[\sqrt{2}]}$$

$K' := \text{SO}(x^2 + y^2 + \sqrt{2}z^2) = \text{SO}(3)$ compact. Recall that arithmetic groups are defined only up to quotients by compacts.

So $\sigma(\Gamma) \subseteq K' \neq G$.

$$\begin{aligned} \text{Define } \Delta: \Gamma &\longrightarrow G \times K' \\ \uparrow &\longmapsto (g, \sigma(g)) \end{aligned}$$

By the same argument as before: $\Delta(\Gamma) \subseteq G \times K'$ is an arithmetic subgroup.

K' cpt \Rightarrow by modding out K' we obtain an arith. subgroup $G_{\mathbb{Z}[\sqrt{2}]}$

It remains to show cocompactness.

We want to use Godement's compactness criterion, i.e. show that Γ has no nontrivial unipotent elements. Let $\gamma \in \Gamma \setminus \{e\}$.

$\Rightarrow \sigma(\gamma) \in K' \setminus \{e\}$. K' is compact $\Rightarrow \sigma(\gamma)$ is not unipotent

$\Rightarrow \exists \lambda \neq 1$ an eigenvalue of $\sigma(\gamma) \Rightarrow \gamma$ has eigenvalue $\sigma^{-1}(\lambda) \neq 1$

$\Rightarrow G_{\mathbb{Z}[\sqrt{2}]}$ is cpt by GCC. □

Cor. If G^σ is compact for some $\sigma \in S^\infty$ then $\Delta(G_{\mathcal{O}_F})$ is cocompact.

Ex. 2) $F = \mathbb{Q}(\sqrt[4]{2})$, $\mathcal{O}_F = \mathbb{Z}[\sqrt[4]{2}]$, $\Gamma = SL(2, \mathcal{O}_F)$, $G = SL(2, \mathbb{R}) \times SL(2, \mathbb{R}) \times SL(2, \mathbb{C})$

Claim: Γ embeds into G as an arithmetic subgroup.

Pf: Set $\alpha = \sqrt[4]{2}$. Its minimal polynomial is $x^4 - 2$ which has 4 distinct roots, determined by $\sigma_0(\alpha) = \alpha$, $\sigma_1(\alpha) = -\alpha$, $\sigma_2(\alpha) = i\alpha$, $\sigma_3(\alpha) = -i\alpha$

We get the embedding $\Delta: F \longrightarrow \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{C}$ restricting to $\Gamma \longrightarrow G$.

$$\sigma \longmapsto (\sigma, \sigma_1(\sigma), \sigma_2(\sigma))$$

$$N(x) = \prod \sigma_i(x) = \sigma_0(x) \sigma_1(x) \cdot |\sigma_2(x)|^2$$

Remark. So far we did everything over \mathbb{R} , but they all work over \mathbb{C} as well if the analogous conditions hold:

- $G \subseteq SL(l, \mathbb{C})$
- F is an alg. number field, $F \neq \mathbb{R}$
- G is defined over F , i.e. $\exists Q \in F[x_1, \dots, x_{ll}]$ s.t. $G^\circ = \text{Var}_{\mathbb{Q}}^\circ(Q)$.

Ex. By doing the same as before we can show that $SO(n, \mathbb{Z}[i, \sqrt{2}])$ is an arithmetic lattice in $SO(n, \mathbb{C}) \times SO(n, \mathbb{C})$.

Prop. If $\Gamma = G_{\mathbb{Z}}$ is an irreducible lattice in G then there are

- 1) an alg. number field F with completion F_∞
- 2) a connected simple subgroup $H < SL(l, F_\infty)$ for some l such that H is defined over F .
- 3) an isogeny $\varphi: \prod_{\sigma \in S^\circ} H^\sigma \longrightarrow G$ s.t. $\varphi(\Delta(H_{\mathcal{O}_F}))$ is commensurable to Γ .

This basically means that all irreducible arithmetic lattices come from a restriction of scalars.

Pf: To make life easier: $G \subseteq SL(n, \mathbb{C})$, $\Gamma = G_{\mathbb{Z}[i]}$, G defd over $\mathbb{Q}(i)$.

Write $G = G_1 \times \dots \times G_r$, all G_i are simple, $H = G_1$.

If $r=1$: set $F = \mathbb{Q}(i)$

$\Sigma := \text{Gal}(\mathbb{C}/\mathbb{Q}(i))$. Since G is defined over $\mathbb{Q}(i)$, $\forall \sigma \in \Sigma$ fix G_i

σ permutes the factors G_i .

Claim: $\Sigma \curvearrowright \{G_i\}_{i=1}^r$ transitively.

Pf: \curvearrowright Suppose $\{G_{i_1}, \dots, G_{i_m}\}$ invariant under Σ , $i_1 < \dots < i_m$

$$\Rightarrow A = G_{i_1} \times \dots \times G_{i_m} \text{ def'd over } \mathbb{Q}(i)$$

$$\Rightarrow A' = \prod_{j \notin \{i_1, \dots, i_m\}} G_j \text{ def'd over } \mathbb{Q}(i) \quad (\text{Exc. 5.5.4})$$

$$\Rightarrow \Gamma = A_{\mathbb{Z}[i]} \times A'_{\mathbb{Z}[i]} \text{ where } A_{\mathbb{Z}[i]} \subset A, A'_{\mathbb{Z}[i]} \subset A' \text{ arithmetic}$$

$\Rightarrow \Gamma$ is not irreducible. \curvearrowright

Set $\Sigma_1 = \{\sigma \in \Sigma \mid \sigma(H) = H\}$. Since the above action is transitive, $[\Sigma : \Sigma_1] = r$.

$\Rightarrow F := \{z \in \mathbb{C} \mid \sigma(z) = z \ \forall \sigma \in \Sigma_1\}$ is a degree r field extension of $\mathbb{Q}(i)$

and H is defined over F as $\sigma(H) = H \ \forall \sigma \in \Sigma_1$.

Choose coset representatives $\sigma_1, \dots, \sigma_r$ of $\Sigma_1 < \Sigma$.

Then $\sigma_1|_F, \dots, \sigma_r|_F$ are the r places of F . After renumbering: $\sigma_j(H) = G_j$

$$\Rightarrow \prod_{\sigma \in \Sigma} H^\sigma = H^{\sigma_1|_F} \times \dots \times H^{\sigma_r|_F} = G_1 \times \dots \times G_r$$

For $u \in H_F$ let $\Delta^1(u) := \prod_{j=1}^r \sigma_j(u)$.

$$\sigma(\Delta^1(u)) = \Delta^1(u) \ \forall \sigma \in \Sigma \quad \rightarrow \Delta^1(u) \in G_{\mathbb{Q}(i)}$$

In fact, $\Delta^1(H) = G_{\mathbb{Q}(i)}$. This follows from the transitivity of the action.

$\Delta(H_{\mathbb{O}_F})$ is commensurable to $\Gamma = G_{\mathbb{Z}[i]}$. \square

Cor.

Arithmetic subgroups of $SL(2, \mathbb{R})$ (Ch. 6.)

Def. $SO(A, F) := \{g \in SL(2, F) \mid g^T A g = A\}$ for $A \in \text{Mat}_{2 \times 2}(F)$ symmetric invertible

Def. $SO(B, F) := \{g \in SL(2, F) \mid B(gv, gw) = B(v, w) \forall v, w \in F^2\}$

where B is a non-degenerate bilinear form ($\forall v \in F^2 \setminus \{0\} \exists w \in F^2: B(v, w) \neq 0$)

Examples. 1) $SL(2, \mathbb{Z}) < SL(2, \mathbb{R})$ non-coapt arith subgroup ($\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is unipotent)

Rule. We will prove that up to conjugation and commensurability

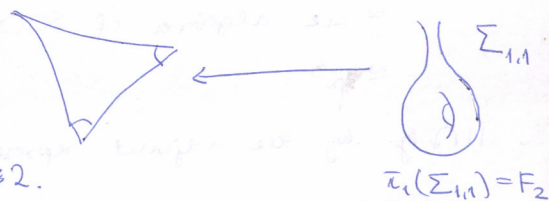
this is the only non-coapt arith subgroup of $SL(2, \mathbb{R})$.

However, there are a lot of interesting finite index subgroups,

e.g. $\exists \Gamma' < SL(2, \mathbb{R})$ fin. index s.t. $\Gamma' \cong F_2$

$F_r < F_2$ is of fin index $\forall r \geq 2$

$\Rightarrow F_r$ is a fin index subgp in $SL(2, \mathbb{R}) \forall r \geq 2$.



Every graph has a free fundamental group because by contracting the spanning tree we get a top equivalence to a wedge of circles.

We can construct all fin-gen. non-ab free gp this way.

2) $a, b \in \mathbb{Z} > 0$, $G := SO(ax^2 + by^2 - z^2, \mathbb{R}) \cong SO(2, 1)$ isogenous to

Recall: if $(0, 0, 0)$ is the only integral solution to $ax^2 + by^2 = z^2$, then

$G_{\mathbb{Z}}$ is a coapt arith subgp of G

3) Restriction of scalars

- $F \neq \mathbb{Q}$ totally real number field, e.g. $\mathbb{Q}[\sqrt{2}]$

- $a, b \in F^+$ s.t. $\sigma(a) < 0, \sigma(b) < 0 \forall \sigma \in S^{\infty} \setminus \{\text{id}\}$

- \mathcal{O}_F ring of integers

- $G := SO(ax^2 + by^2 - z^2, \mathbb{R}) \cong SO(2, 1)$

$\Rightarrow G_{\mathcal{O}_F}$ is a coapt arith subgp of G

4) $h := \text{diag}(\sqrt{a}, \sqrt{b}, 1) \Rightarrow h^{-1} G h = SO(2, 1)$

Prop. Up to commensurability and conjugation 2) and 3) are the only cospets of $SL(2, \mathbb{R})$.

Pf: Step 1: we know that there are

- an alg number field $F \subset \mathbb{R}$ with ring of integers \mathcal{O}_F
- $H \subseteq SL(2, \mathbb{R})$ simple, connected, defined over F
- an isogeny $\varphi: H \rightarrow SL(2, \mathbb{R})$ s.t. $\varphi(H\mathcal{O}_F)$ is commensurable to our arithmetic lattice Γ .

Goal: $H \cong SO(B, F)$ where B is a bilinear form of the form 2) or 3).

We need some Lie theory (see App. A.6)

$$\begin{aligned} \mathfrak{h} &= \text{Lie algebra of } H = T_e H \quad (\text{e.g. the Lie algebra of } SL(2, \mathbb{R}) \text{ is} \\ &= \text{Lie algebra of } SO(2, 1) \quad \mathfrak{sl}(2, \mathbb{R}) = \{X \in \text{Mat}_{2 \times 2}(\mathbb{R}) \mid \text{tr}(X) = 0\}) \\ &\cong \mathbb{R}^3 \end{aligned}$$

$H \curvearrowright \mathfrak{h}$ by the adjoint representation:

$$\text{Ad}(g) := \mathfrak{h} \rightarrow \mathfrak{h} \quad \text{defined by} \quad \text{Ad}(g)(v) := (d\psi_g)(v)$$

$$\text{where } \psi_g: H \rightarrow H \text{ is given by } \psi_g(h) = ghg^{-1}.$$

Computational shows that $\text{Ad}(g)(X) = gXg^{-1} \quad \forall g \in H \quad \forall X \in \mathfrak{h}$

The Lie algebra \mathfrak{h} comes with a Lie bracket

$$[-, -]: \mathfrak{h} \times \mathfrak{h} \rightarrow \mathfrak{h} \quad \text{defined by} \quad [X, Y] = XY - YX \quad \forall X, Y \in \mathfrak{h}$$

This gives us a representation $\text{ad}: \mathfrak{h} \rightarrow \text{End } \mathfrak{h}$ given by

$$\text{ad}(X)(Y) = [X, Y].$$

We obtain a bilinear form called the Killing form:

$$\begin{aligned} \kappa: \mathfrak{h} \times \mathfrak{h} &\rightarrow \mathbb{R} \\ (X, Y) &\mapsto \text{tr}(\text{ad}(X) \cdot \text{ad}(Y)) \end{aligned}$$

Fact: $\text{Ad}(g)$ preserves $\kappa \quad \forall g \in H$ and Ad is an isogeny.

Step 2: NTS κ has the correct form.

$$\text{Write } \kappa(x, x) = ax_1^2 + bx_2^2 + cx_3^2. \quad \text{Need: } a, b, c \in F^+$$

Know: $SO(\kappa, 1)$ is isog. to $SO(2, 1) \rightarrow$ get: $a, b, -c \in F^+$.

$$\text{Divide by } c \Rightarrow \kappa(x, x) = ax_1^2 + bx_2^2 - x_3^2$$

Step 3. $\forall \sigma \neq \text{id} : \sigma(a), \sigma(b) < 0$

Know: $\Delta(H_0)$ invd lattice in $\prod_{\sigma \in S^\infty} H^\sigma$ and proj. in H^{id} lattice

$\Rightarrow H^\sigma$ cpt $\forall \sigma \neq \text{id} \rightarrow H^\sigma \cong \text{SO}(2,1) \quad \forall \sigma \neq \text{id}$

$\Rightarrow \sigma(a), \sigma(b), \sigma(-1)$ have the same sign $\Rightarrow \sigma(a), \sigma(b) < 0$.

Prop. $\text{SL}(2, \mathbb{Z})$ is the only non-cppt arithl subgroup of $\text{SL}(2, \mathbb{R})$ up to conjugation and commensurability.

Pf. Work with $\text{SO}(2,1)$. Goal: prove that $\text{SO}(2,1)_{\mathbb{Z}}$ is the "only" non-cppt arithl subgroup of $\text{SO}(2,1)$.

Know: $\exists G < \text{SL}(l, \mathbb{R})$ simple for some l s.t. G is defined over some number field F and $\exists \varphi: G \rightarrow \text{SO}(2,1)$ isogeny s.t. $\varphi(G_{O_F})$ is comm to Γ .

Pf of prev. Prop. $\Rightarrow G = \text{SO}(B, \mathbb{R})$ where $B: \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ bilinear form of signature $(2,1)$.

NTS: G is defined over \mathbb{Q} .

Recall from the original def of arithl gps: $\exists K'$ cpt s.t.

$$G' = G \times K' < \text{SL}(l, \mathbb{R}), \quad G' \text{ defined over } \mathbb{Q}, \quad \Gamma K' = G'_{\mathbb{Z}} K'$$

$N =$ Zariski closure of unipotent elts in $G'_{\mathbb{Z}}$

K' cpt. $\Rightarrow N \subseteq G$

$$N \text{ is normalised by } G'_{\mathbb{Z}} \xrightarrow[\text{density}]{\text{Borel}} N \triangleleft G \xrightarrow{G \text{ simple}} N = G.$$

G is the Zariski closure of a group defined over $\mathbb{Z} \Rightarrow G$ is def. / \mathbb{Q} .

Step 2. Have: $G = \text{SO}(B, \mathbb{R})$. Want: $B(x,x) = x_1^2 + x_2^2 - x_3^2$

Γ not cppt $\Rightarrow B$ is isotropic over $F \Rightarrow \exists u \in F^3 \setminus \{0\} : B(u,u) = 0$.

Choose $v \in F^3 \setminus \{0\}$ s.t. $B(u,v) \neq 0$

By adding a multiple of u wma $B(v,v) = 0$.

Choose $w \in F^3 \setminus \{0\}$ s.t. $B(w,u) = B(w,v) = 0$.

Multiplying B with scalars preserves everything \Rightarrow wma $B(w,w) = 2B(v,v) = 1$.

$\rightarrow B$ has the desired form wrt. the basis $\{w, u+v, u-v\}$.

