Introduction to arithmetic groups

Dave Witte Morris

University of Lethbridge, Alberta, Canada
http://people.uleth.ca/~dave.morris
Dave.Morris@uleth.ca

KAIST Geometric Topology Fair (January 11–13, 2010)

Abstract. Arithmetic groups are fundamental groups of locally symmetric spaces. We will see how they are constructed, and discuss some of their important properties. For example, although the $\mathbb{Q}$-rank of an arithmetic group is usually defined in purely algebraic terms, we will see that it provides important information about the geometry and topology of the corresponding locally symmetric space. Algebraic technicalities will be pushed to the background as much as possible.

Introduction to Arithmetic Groups 1

What is a superrigid subgroup?

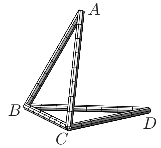
1. rigidity of linkages
2. group-theoretic superrigidity
3. the analogy
4. examples of superrigid subgroups
5. why superrigidity implies arithmeticity
6. some geometric consequences of superrigidity
   - Mostow Rigidity Theorem
   - vanishing of the first Betti number

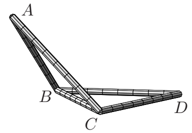
For further reading, see the references in [D. W. Morris, What is a superrigid subgroup?, in Timothy Y. Chow and Daniel C. Isaksen, eds.: *Communicating Mathematics.* American Mathematical Society, Providence, R.I., 2009, pp. 189–206. http://arxiv.org/abs/0712.2299].

---

1. Rigidity of linkages

Example (two joined triangles)

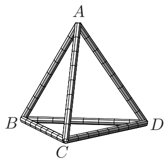




A——B B——C B——D A——C C——D

This is not rigid.
I.e., it can be deformed (a "hinge").

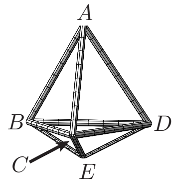
Example (Tetrahedron)

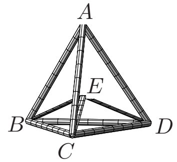


A——B	A——C	A——D
B——C	B——D	C——D

This is **rigid** (cannot be deformed).

Example (add a small tetrahedron)

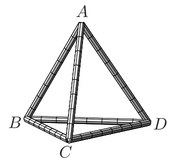




A——B	A——C	A——D
B——C	B——D	C——D
B—E	C—E	D—E

This is rigid.

However, it is not **superrigid**:
if it is taken apart, it can be reassembled incorrectly.



A——B	A——C	A——D
B——C	B——D	C——D

A tetrahedron *is* superrigid: the combinatorial description determines the geometric structure.

Combinatorial superrigidity

Make a copy of the object,
according to the combinatorial rules.
The copy is the exact same shape as the original.

This talk: analogue in group theory

---

2. Group-theoretic superrigidity

Group homomorphism $\phi\colon \mathbb{Z} \to \mathbb{R}^d$
(i.e., $\phi(m+n) = \phi(m) + \phi(n)$)
$\Rightarrow \phi$ extends to a homomorphism $\hat{\phi}\colon \mathbb{R} \to \mathbb{R}^d$.
Namely, define $\hat{\phi}(x) = x \cdot \phi(1)$.

Check:

- $\hat{\phi}(n) = \phi(n)$
- $\hat{\phi}(x+y) = \hat{\phi}(x) + \hat{\phi}(y)$
- $\hat{\phi}$ is continuous
  (only allow continuous homomorphisms)

Group homomorphism $\phi\colon \mathbb{Z}^k \to \mathbb{R}^d$
$\Rightarrow \phi$ extends to a homomorphism $\hat{\phi}\colon \mathbb{R}^k \to \mathbb{R}^d$.

Proof.

Use standard basis $\{e_1, \ldots, e_k\}$ of $\mathbb{R}^k$.
Define $\hat{\phi}(x_1, \ldots, x_k) = \sum x_i\, \phi(e_i)$.
("linear trans can do anything to a basis")
Linear transformation
$\Rightarrow$ homomorphism of additive groups $\square$

Group Representation Theory:
study homomorphisms into *Matrix Groups.*
$\mathrm{GL}(d, \mathbb{C}) = d \times d$ matrices over $\mathbb{C}$
with nonzero determinant.
This is a group under multiplication.

Group homomorphism $\phi\colon \mathbb{Z} \to \mathrm{GL}(d, \mathbb{R})$
(i.e., $\phi(m+n) = \phi(m) \cdot \phi(n)$)
$\not\Rightarrow$ extends to homomorphism $\hat{\phi}\colon \mathbb{R} \to \mathrm{GL}(d, \mathbb{R})$.
(Only allow *continuous* homos.)

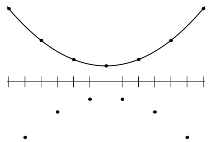
Proof by contradiction.

Spse $\exists$ homo $\hat{\phi}\colon \mathbb{R} \to \mathrm{GL}(d, \mathbb{R})$
with $\hat{\phi}(n) = \phi(n)$ for all $n \in \mathbb{Z}$.
$\hat{\phi}(0) = \mathrm{Id}$ $\quad\Rightarrow \det(\hat{\phi}(0)) = \det(\mathrm{Id}) = 1 > 0$
$\mathbb{R}$ connected $\quad\Rightarrow \hat{\phi}(\mathbb{R})$ connected
$\Rightarrow \det(\hat{\phi}(\mathbb{R}))$ connected in $\mathbb{R}^\times = \mathbb{R} - \{0\}$
$\Rightarrow \det(\hat{\phi}(\mathbb{R})) > 0$
$\Rightarrow \det(\phi(1)) > 0$
Maybe $\det(\phi(1)) < 0$. $\quad\rightarrow\leftarrow$ $\square$

Group homomorphism $\phi\colon \mathbb{Z} \to \mathrm{GL}(d,\mathbb{R})$
$\not\Rightarrow$ extends to homomorphism $\hat\phi\colon \mathbb{R} \to \mathrm{GL}(d,\mathbb{R})$.
Because: maybe $\det(\phi(1)) < 0$.

$\det(\phi(2)) = \det(\phi(1+1)) = \big(\det(\phi(1))\big)^2 > 0$.
In fact, $\det(\phi(\text{even})) > 0$.

May have to ignore odd numbers:
restrict attention to even numbers.



May have to ignore odd numbers:
restrict attention to even numbers.

Analogously, may need to restrict to multiples of 3
(or 4 or 5 or ...)
Restrict attention to multiples of N.
{multiples of N} is a subgroup of $\mathbb{Z}$
"Restrict attention to a finite-index subgroup"

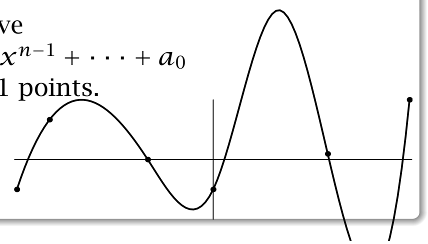
Proposition

Group homomorphism $\phi\colon \mathbb{Z}^k \to \mathrm{GL}(d,\mathbb{R})$
$\Rightarrow \phi$ *"almost" extends to homo* $\hat\phi\colon \mathbb{R}^k \to \mathrm{GL}(d,\mathbb{R})$
such that $\hat\phi(\mathbb{R}^k) \subset \overline{\phi(\mathbb{Z}^k)}$. (*"Zariski closure"*)

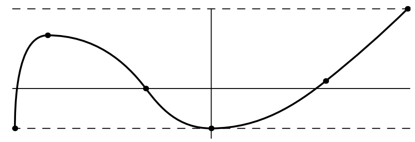
This means $\mathbb{Z}^k$ is *superrigid* in $\mathbb{R}^k$.

Lagrange interpolation

$\exists$ polynomial curve
$y = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$
through any $n+1$ points.



Idea: Zariski closure is like *convex hull*.



Proposition ("$\mathbb{Z}^k$ is superrigid in $\mathbb{R}^k$")

Group homomorphism $\phi\colon \mathbb{Z}^k \to \mathrm{GL}(d,\mathbb{R})$
$\Rightarrow \phi$ *"almost" extends to homo* $\hat\phi\colon \mathbb{R}^k \to \mathrm{GL}(d,\mathbb{R})$
such that $\hat\phi(\mathbb{R}^k) \subset \overline{\phi(\mathbb{Z}^k)}$. (*"Zariski closure"*)

$\hat\phi(\mathbb{R}^k) \subset \overline{\phi(\mathbb{Z}^k)}$: image of ϕ controls image of $\hat\phi$.
Good properties of $\phi(\mathbb{Z})$ carry over to $\hat\phi(\mathbb{R})$.

Example: If all matrices in $\phi(\mathbb{Z})$ commute,
then all matrices in $\hat\phi(\mathbb{R})$ commute.

Example: If all matrices in $\phi(\mathbb{Z})$ fix a vector v,
then all matrices in $\hat\phi(\mathbb{R})$ fix v.

Generalize to nonabelian groups.

3. The analogy

Combinatorial superrigidity

Make copy of object, obeying combinatorial rules.
The copy is the exact same shape as the original.

Maybe not exactly the same object:
may be rotated from the original position;
may be translated from original position.
These are trivial modifications:
rotations and translations are symmetries of the whole universe (Euclidean space $\mathbb{R}^3$).

Same result can be obtained with the original object by moving the whole universe to a new position.

Combinatorial superrigidity

"If the object can be moved somewhere,
then the whole universe can be moved there."

Γ is a *superrigid* subgroup of the group G means:
homomorphism $\phi\colon \Gamma \to \mathrm{GL}(d,\mathbb{R})$ extends
to homomorphism $\hat\phi\colon G \to \mathrm{GL}(d,\mathbb{R})$

Group-theoretic superrigidity

Make a copy of Γ as a group of matrices.
The same copy of Γ can be obtained by moving all of G into a group of matrices.

4. Superrigid subgroups

Example. $\mathbb{Z}^k$ is superrigid in $\mathbb{R}^k$.
Generalize to nonabelian groups.

$\mathbb{Z}^k$ is a (cocompact) *lattice* in $\mathbb{R}^k$. I.e.,

- $\mathbb{R}^k$ is a (simply) connected group ("Lie group")
- $\mathbb{Z}^k$ is a discrete subgroup
- all of $\mathbb{R}^k$ is within a bounded distance of $\mathbb{Z}^k$
  $\exists C,\ \forall x \in \mathbb{R}^k,\ \exists m \in \mathbb{Z}^k,\quad d(x,m) < C$.

If can replace $\mathbb{Z}^k$ with Γ and $\mathbb{R}^k$ with G,
then Γ is a (cocompact) *lattice* in G.

Lie groups are of three types:

- solvable (many normal subgrps, e.g., abelian)
- simple ("no" normal subgroups, e.g., $\mathrm{SL}(k,\mathbb{R})$)
- combination (e.g., $G = \mathbb{R}^k \times \mathrm{SL}(k,\mathbb{R})$)
  More or less: $\Gamma = \mathbb{Z}^k \times \mathrm{SL}(k,\mathbb{Z})$
  (Γ has a solvable part and a simple part)

Today: we consider *solvable* groups.

Definition

A connected subgroup G of $\mathrm{GL}(d,\mathbb{C})$ is *solvable* if it is upper triangular

$$G \subset \begin{bmatrix} \mathbb{C}^\times & \mathbb{C} & \mathbb{C} \\ 0 & \mathbb{C}^\times & \mathbb{C} \\ 0 & 0 & \mathbb{C}^\times \end{bmatrix}$$

(or is after a change of basis).

Example

All abelian groups are solvable.

Proof.

Every matrix can be triangularized over $\mathbb{C}$.
Pairwise commuting matrices can be simultaneously triangularized. $\square$

Examples of lattices

$$G = \begin{bmatrix} 1 & \mathbb{R} & \mathbb{R} & \mathbb{R} \\ 0 & 1 & \mathbb{R} & \mathbb{R} \\ 0 & 0 & 1 & \mathbb{R} \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \Gamma = \begin{bmatrix} 1 & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 0 & 1 & \mathbb{Z} \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$\overline{\Gamma} = G$ superrigid

$$G = \begin{bmatrix} \mathbb{R}^+ & 0 & 0 \\ 0 & \mathbb{R}^+ & 0 \\ 0 & 0 & \mathbb{R}^+ \end{bmatrix} \qquad \Gamma = \begin{bmatrix} 2^{\mathbb{Z}} & 0 & 0 \\ 0 & 2^{\mathbb{Z}} & 0 \\ 0 & 0 & 2^{\mathbb{Z}} \end{bmatrix}$$

$\overline{\Gamma} = G$ superrigid

$$G = \begin{bmatrix} 1 & \mathbb{R} & \mathbb{C} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \Gamma = \begin{bmatrix} 1 & \mathbb{Z} & \mathbb{Z}+\mathbb{Z}i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$\overline{G} = G$ $\qquad$ $\overline{\Gamma} = G$ $\qquad$ superrigid

$$G' = \begin{bmatrix} 1 & t & \mathbb{C} \\ 0 & 1 & 0 \\ 0 & 0 & e^{2\pi i t} \end{bmatrix} \qquad \overline{G'} = \begin{bmatrix} 1 & \mathbb{R} & \mathbb{C} \\ 0 & 1 & 0 \\ 0 & 0 & \mathbb{T} \end{bmatrix}$$

$$\Gamma' = \begin{bmatrix} 1 & \mathbb{Z} & \mathbb{Z}+\mathbb{Z}i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \Gamma.$$

Γ is a lattice in both G and G'.

$\overline{\Gamma} = G \neq \overline{G'}$ so $\overline{\Gamma} \neq \overline{G'}$. Γ is *not* superrigid in G'.

E.g., id map $\phi\colon \Gamma \to \Gamma$ does not extend to $\hat{\phi}\colon G' \to \overline{\Gamma}$.
($\overline{\Gamma} = G$ is abelian but G' is not abelian.)

Proposition

Γ superrigid in G $\Rightarrow \overline{\Gamma} = \overline{G}$ $\quad$ (mod $\overline{Z(G)}$).

Proof.
The inclusion $\Gamma \hookrightarrow \mathrm{GL}(d,\mathbb{R})$)
must extend to $G \hookrightarrow \mathrm{GL}(d,\mathbb{R})$ with $G \subset \overline{\Gamma}$. □

Theorem (converse)
Lattice Γ in solv grp G is superrig iff $\overline{\Gamma} = \overline{G}$ (mod $\overline{Z(G)}$).

$\overline{\Gamma} \neq \overline{G'}$: some of the rotations associated to G' do not come from rotations associated to Γ.

$$\mathrm{rot}\begin{bmatrix} \alpha & * \\ 0 & \beta \end{bmatrix} = \begin{bmatrix} \frac{\alpha}{|\alpha|} & 0 \\ 0 & \frac{\beta}{|\beta|} \end{bmatrix}$$

Corollary
A lattice Γ in a Lie group G is "superrigid" iff
- $\overline{\Gamma} = \overline{G}$ $\quad$ (mod $\overline{Z(G)}\cdot$ (cpct ss normal subgrp))
- *and simple part of* Γ *is "superrigid."*

Theorem (Margulis Superrigidity Theorem)
All lattices in $\mathrm{SL}(n,\mathbb{R})$ *are "superrigid" if* $n \geq 3$.
Similar for other simple Lie groups, $\mathbb{R}$-rank ≥ 2.

Corollary (Margulis Arithmeticity Theorem)
Every lattice in $\mathrm{SL}(n,\mathbb{R})$ *is "arithmetic" if* $n \geq 3$.
(like $\mathrm{SL}(n,\mathbb{Z})$)
Only way to make a lattice: take integer points
(*and minor modifications*)

---

5. Why superrigidity implies arithmeticity

Let Γ be a superrigid lattice in $\mathrm{SL}(n,\mathbb{R})$.
We wish to show $\Gamma \subset \mathrm{SL}(n,\mathbb{Z})$,
i.e., want every matrix entry to be an integer.

First, let us show they are algebraic numbers.
Suppose some $\gamma_{i,j}$ is transcendental.
Then $\exists$ field auto ϕ of $\mathbb{C}$ with $\phi(\gamma_{i,j}) = ???$.

$$\text{Define} \quad \tilde{\phi}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{bmatrix}.$$

So $\tilde{\phi}\colon \Gamma \to \mathrm{GL}(n,\mathbb{C})$ is a group homo.
Superrigidity: $\tilde{\phi}$ extends to $\hat{\phi}\colon \mathrm{SL}(n,\mathbb{R}) \to \mathrm{GL}(n,\mathbb{C})$.
There are uncountably many different ϕ's,
but $\mathrm{SL}(n,\mathbb{R})$ has only finitely many n-dim'l rep'ns.

Γ is a superrigid lattice in $\mathrm{SL}(n,\mathbb{R})$
and every matrix entry is an algebraic number.

Second, show matrix entries are rational.
Fact. Γ is generated by finitely many matrices.
Entries of these matrices generate a field extension of $\mathbb{Q}$ of finite degree. $\quad$ "algebraic number field"
So $\Gamma \subset \mathrm{SL}(n,F)$. For simplicity, assume $\Gamma \subset \mathrm{SL}(n,\mathbb{Q})$.

Third, show matrix entries have no denominators.
Actually, show denominators are bounded.
(Then finite-index subgrp has no denoms.)
Since Γ is generated by finitely many matrices,
only finitely many primes appear in denoms.
So suffices to show each prime occurs to bdd power.

Γ is a superrigid lattice in $\mathrm{SL}(n,\mathbb{R})$
and every matrix entry is a rational number.
Show each prime occurs to bdd power in denoms.

This is the conclusion of *p-adic superrigidity*:

Theorem (Margulis)
If Γ is a lattice in $\mathrm{SL}(n,\mathbb{R})$, $\quad$ *with $n \geq 3$,*
and $\phi\colon \Gamma \to \mathrm{SL}(k,\mathbb{Q}_p)$ is a group homomrphism,
then $\phi(\Gamma)$ has compact closure.
I.e., $\exists k$, no matrix in $\phi(\Gamma)$ has p^k in denom.

Summary of proof:
1. $\mathbb{R}$-superrigidity $\Rightarrow$ matrix entries "rational"
2. $\mathbb{Q}_p$-superrigidity $\Rightarrow$ matrix entries $\in \mathbb{Z}$

Some consequences of superrigidity

Let Γ be the fundamental group of a locally symmetric space M that has finite volume.
We always assume $\widetilde{M}$ has no compact or flat factors, and is complete.
Also assume M is irreducible: $M \neq M_1 \times M_2$.
Assume Γ is superrigid.

Topology of M determines its geometry:

Corollary (Mostow Rigidity Theorem)
If $\Gamma \cong$ fund group Γ' of finite-vol loc symm space M',
then M is isometric to M' $\quad$ (*up to normalizing constant*).

More generally, if $\Gamma \hookrightarrow \Gamma'$, then $M \hookrightarrow M'$ as a totally geodesic subspace (up to finite covers).

Γ = superrig fund grp of fin-vol loc symm space M.

Corollary
The first Betti number of M vanishes: $H^1(M;\mathbb{R}) = 0$.

Remark
It is conjectured [Thurston] that if M is a finite-volume hyperbolic manifold, then
$H^1(\widehat{M};\mathbb{R}) \neq 0$, for some finite cover $\widehat{M}$.

So it is believed that the fundamental group of a hyperbolic manifold is never superrigid
(although most hyperbolic mflds are Mostow rigid).

Introduction to Arithmetic Groups 2

- examples
- relation to locally symmetric spaces $M = X/\Gamma$
- compactness criterion (two versions)
- basic group-theoretic properties
  - congruence subgroups
    - residually finite
    - virtually torsion free (Selberg's Lemma)
  - finitely presented

For further reading, see D. W. Morris, *Introduction to Arithmetic Groups.*
http://people.uleth.ca/~dave.morris/books/IntroArithGroups.html
More advanced:
M. S. Raghunathan, *Discrete Subgroups of Lie Groups*, Springer, 1972.
V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, 1993.

Examples of arithmetic groups

Let Γ be an *arithmetic group*:

$\Gamma = \mathrm{SL}(3,\mathbb{Z}) = \{\, 3\times 3$ integer matrices of det $1\,\}$
(or subgroup of finite index)

or $\Gamma \doteq \mathrm{SO}(1,3;\mathbb{Z}) = \mathrm{SO}(1,3) \cap \mathrm{SL}(4,\mathbb{Z})$
$= \{\, g \in \mathrm{SL}(4,\mathbb{Z}) \mid g\, I_{1,3}\, g^T = I_{1,3} \,\}$ $\quad I_{1,3} = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}$

or ...

$\Gamma = G_{\mathbb{Z}} := G \cap \mathrm{SL}(n,\mathbb{Z})$ for suitable $G \subset \mathrm{SL}(n,\mathbb{R})$.

Theorem ("Reduction Theory")
For suitable $G \subset \mathrm{SL}(n,\mathbb{R})$, Γ is a lattice in G:
1. *Γ is discrete, and*
2. *$\Gamma\backslash G$ has finite volume* *(maybe compact).*

Relation to locally symmetric spaces

Recall
$X = \mathbb{R}^n$ is a *symmetric space.*
1. X is *homogeneous*: $\mathrm{Isom}(X)$ is transitive on X
2. $\exists\, \phi \in \mathrm{Isom}(X)$, ϕ has an isolated fixed point:
   $\phi(x) = -x$ fixes only 0.

Example
$X = \mathbf{H}^n$ is also a symmetric space.
$(\mathrm{Isom}(\mathbf{H}^n) \approx \mathrm{SO}(1,n))$

Exercise
X = symmetric space (connected), $G = \mathrm{Isom}(X)^\circ$
$\implies X = G/K$, K compact.

---

symmetric space $X = G/K$, K compact

Definition
M is a *locally symmetric space* (complete):
universal cover of M is a symmetric space.
I.e., $M = \Gamma\backslash X$, $\Gamma \subset \mathrm{Isom}(M)$ discrete (& torsion-free).

Example
$G = \mathrm{Isom}(\mathbb{R}^n)^\circ = \mathbb{R}^n \rtimes \mathrm{SO}(n)$, $K = \mathrm{SO}(n)$
$\implies X = \mathbb{R}^n$.
Let $\Gamma = \mathbb{Z}^n \subset G$, so $M = \mathbb{Z}^n\backslash\mathbb{R}^n = \mathbb{T}^n$.

Example
$G = \mathrm{SO}(1,n)^\circ$, $K = \mathrm{SO}(n)$ $\implies X = \mathbf{H}^n$.
Let $\Gamma = \mathrm{SO}(1,n;\mathbb{Z})$, so $M = \Gamma\backslash\mathbf{H}^n$ = hyperbolic mfld.

---

locally symmetric space $M = \Gamma\backslash X$, $X = G/K$

Best mflds are *compact*. Next best: *finite volume.*

Recall
Γ is a *lattice* in G: Γ is discrete, and $\Gamma\backslash G$ has finite volume.

Proposition
Γ is a torsion-free lattice in G, $X = G/K$
$\implies M = \Gamma\backslash X$ is locally symmetric of finite volume.

So lattices are the fundamental groups
of finite-volume locally symmetric spaces.
And arithmetic groups are the lattices
that are easy to construct.

$M = \Gamma\backslash X$, $X = G/K$, Γ a lattice in G

Henceforth, assume X has:
- no flat factors: $X \neq X_1 \times \mathbb{R}^n$
- no compact factors: $X \neq X_1 \times$ compact

Then G *is semisimple* with no compact factors and trivial center.

Fundamental grp provides topological info about any space.
For locally symmetric spaces, it does much more:
usually completely determines all of the topology and geometry.

Mostow Rigidity Theorem

Theorem (Mostow Rigidity Theorem)
Suppose M_1 and M_2 are finite-volume locally symm. Assume
- *$\dim M_1 > 2$, and*
- *M_1 is irreducible: $M_1 \not\approx M' \times M''$ (up to finite covers).*

If $\Gamma_1 \cong \Gamma_2$, then $M_1 \cong M_2$ (modulo a normalizing constant).

- Every aspect of the geometric structure of M is reflected as an algebraic property of the fundamental group Γ.
- The *geometric category* of irreducible locally symmetric spaces with dim > 2 is *equivalent to* the *algebraic category* of "irreducible" lattices in appropriate semisimple Lie groups.

Compactness criterion

Observation
For $M = \Gamma\backslash X$ with $X = G/K$:
M is compact iff $\Gamma\backslash G$ is compact.
(Because $M = \Gamma\backslash G/K$ and K is compact.)

Say Γ is a *cocompact* lattice in G.

Proposition
$\Gamma\backslash G$ is not compact iff
$\exists g_1, g_2, g_3, \ldots \in G$ *and*
$\exists \gamma_1, \gamma_2, \gamma_3, \ldots \in \Gamma^\times = \Gamma - \{e\}$, *such that*
$g_i^{-1}\gamma_i g_i \to e$.

$\Gamma\backslash G$ not compact iff $\exists g_i, \gamma_i$, $g_i^{-1}\gamma_i g_i \to e$

Proof ($\Leftarrow$).
Suppose $\Gamma\backslash G$ is compact.
For $a, b \in G$, let $a^b = a^{-1}ba$ ("conjugation of b by a").
Since $\Gamma\backslash G$ is compact, $\exists$ cpct C with $\Gamma C = G$.

C is compact and $\Gamma^\times$ is discrete, hence closed,
so $(\Gamma^\times)^C$ is closed.

Therefore

$$e \in \overline{g_i^{-1}\gamma_i g_i} \subset \overline{(\Gamma^\times)^G} = \overline{(\Gamma^\times)^{\Gamma C}}$$
$$= \overline{((\Gamma^\times)^\Gamma)^C} = \overline{(\Gamma^\times)^C} = (\Gamma^\times)^C \not\ni e. \quad \rightarrow\leftarrow \quad \square$$

$\Gamma \backslash G$ not compact iff $\exists g_i, \gamma_i,\ g_i^{-1}\gamma_i g_i \to e$

Corollary

$\mathrm{SL}(2,\mathbb{Z}) \backslash \mathrm{SL}(2,\mathbb{R})$ is not compact.

Proof.

Let $g_i = \begin{bmatrix} i & \\ & 1/i \end{bmatrix}$ and $\gamma_i = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$. Then

$$g_i^{-1}\gamma_i g_i = \begin{bmatrix} 1/i & \\ & i \end{bmatrix}\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}\begin{bmatrix} i & \\ & 1/i \end{bmatrix} = \begin{bmatrix} 1 & 1/i^2 \\ & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ & 1 \end{bmatrix} = e.$$ □

Similarly, $\mathrm{SL}(n,\mathbb{Z}) \backslash \mathrm{SL}(n,\mathbb{R})$ is not compact (if $n \geq 2$).

$\Gamma \backslash G$ not compact iff $\exists g_i, \gamma_i,\ g_i^{-1}\gamma_i g_i \to e$

Corollary (Godement Criterion)

$\Gamma \backslash G$ is compact iff Γ has no unipotent elements.

Definition

$u \in \mathrm{SL}(n,\mathbb{R})$ is *unipotent*: $(u - \mathrm{Id})^n = 0$.

Equivalently, 1 is the only eigenvalue of u, so

u is conjugate to $\begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$

Corollary (Godement Criterion)

$\Gamma \backslash G$ not cpct iff Γ has nontrivial unipotent elements.

Proof ($\Rightarrow$).

$\exists\, g_i \in G$ and $\gamma_i \in \Gamma^\times$ with $g_i^{-1}\gamma_i g_i \to \mathrm{Id}$.

1. Char poly of Id is $\det(\lambda - \mathrm{Id}) = (\lambda - 1)^n$.
2. $\gamma_i \in \mathrm{SL}(n,\mathbb{Z}) \implies$ char poly of γ_i has $\mathbb{Z}$ coeffs.
3. Similar matrices have same characteristic poly, so the char poly of $g_i^{-1}\gamma_i g_i$ also has $\mathbb{Z}$ coeffs.
4. char poly of $g_i^{-1}\gamma_i g_i \to$ char poly of Id and both have $\mathbb{Z}$ coefficients. So the two char polys are equal (if i is large).
5. Therefore, the char poly of γ_i is $(\lambda - 1)^n$.

So the only eigenvalue of γ_i is 1. □

Corollary (Godement Criterion)

$\Gamma \backslash G$ not cpct iff Γ has nontrivial unipotent elements.

The proof of the other direction ($\Leftarrow$) depends on a fundamental fact from Lie theory:

Theorem (Jacobson-Morosov Lemma)

If u is any unipotent element of G
(connected semisimple Lie group in $\mathrm{SL}(n,\mathbb{R})$)
then there is a continuous homomorphism
$\rho\colon \mathrm{SL}(2,\mathbb{R}) \to G$ *with* $\rho\left(\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}\right) = u.$

Proof of Godement ($\Leftarrow$) | Let $\gamma_i = u \in \Gamma$ and $g_i = \rho\left(\begin{bmatrix} i & \\ & 1/i \end{bmatrix}\right)$.

Congruence Subgroups

We will use a construction known as
"congruence subgroups"
to prove two basic properties of arithmetic groups.

1. Γ is residually finite
2. Γ is virtually torsion-free

Proposition

Γ is residually finite:
$\forall \gamma \in \Gamma^\times$, $\exists$ *finite-index subgrp* $H < \Gamma$, $\gamma \notin H$.

Proof.

$\gamma - \mathrm{Id} \neq 0$, so $\exists (\gamma - \mathrm{Id})_{ij} \neq 0$.
Choose $N \nmid (\gamma - \mathrm{Id})_{ij} = \gamma_{ij} - \mathrm{Id}_{ij}$.
Ring homo $\mathbb{Z} \to \mathbb{Z}_N$ yields $\mathrm{SL}(n,\mathbb{Z}) \to \mathrm{SL}(n,\mathbb{Z}_N)$.
Let $\rho_N\colon \Gamma \to \mathrm{SL}(n,\mathbb{Z}_N)$ be the restriction to Γ.
Since $\mathbb{Z}_N$ finite, obvious that $\mathrm{SL}(n,\mathbb{Z}_N)$ is finite.
Let $H = \ker \rho_N$. Then $\Gamma/H \cong \mathrm{img}(\rho_N)$ is finite.
So H is a finite-index subgroup.
By choice of N, $\rho_N(\gamma)_{ij} \neq \rho_N(\mathrm{Id})_{ij}$, so $\rho_N(\gamma) \neq \mathrm{Id}$.
So $\gamma \notin \ker(\rho_N) = H$. □

Terminology: $\ker(\rho_N)$ is a (principal) *congruence subgroup* of Γ.

Proposition (Selberg's Lemma)

Γ is virtually torsion-free:
$\exists$ *finite-index subgrp* $H < \Gamma$, *H is torsion-free.*
(no nontrivial elements of finite order)

Proof.

Define $\rho_3\colon \Gamma \to \mathrm{SL}(n,\mathbb{Z}_3)$ and let $H = \ker(\rho_3)$.
It suffices to show H is torsion-free.
Let $h \in H$, write $h = \mathrm{Id} + 3^k T$, $T \not\equiv 0 \pmod 3$.

$$\begin{aligned} h^m &= (\mathrm{Id} + 3^k T)^m \\ &= \mathrm{Id} + m(3^k T) + \binom{m}{2} 3^{2k} T^2 + \cdots \\ &\equiv \mathrm{Id} + 3^k m T \pmod{3^{k+\ell+1}} \quad \text{if } 3^\ell \mid m \\ &\not\equiv \mathrm{Id} \pmod{3^{k+\ell+1}} \quad \text{if } 3^{\ell+1} \nmid m. \end{aligned}$$ □

Finite presentation

Proposition

Γ is finitely presented:
$\Gamma = \langle \gamma_1, \gamma_2, \ldots, \gamma_m \mid w_1, w_2, \ldots, w_r \rangle$.

Proof of finite generation.

Fund grp of any *compact* mfld is finitely generated:
$\pi\colon \widetilde{M} \to M$, $\exists$ cpct $C \subset \widetilde{M}$, $\pi(C) = M$.
Let $S = \{\, \gamma \in \Gamma \mid \gamma C \cap C \neq \varnothing \,\}$. ($\Gamma$ prop disc, so S finite!)
Then $\Gamma = \langle S \rangle$:
Given $\gamma \in \Gamma$. Since M is connected, $\exists$ chain
$C, \gamma_1 C, \gamma_2 C, \ldots, \gamma_n C = \gamma C$, with $\gamma_k C \cap \gamma_{k+1} C \neq \varnothing$.
So $\gamma_1 \in S$, $\gamma_1^{-1}\gamma_2 \in S, \ldots, \gamma_n^{-1}\gamma \in S$.
Therefore $\gamma = \gamma_1(\gamma_1^{-1}\gamma_2)\cdots(\gamma_n^{-1}\gamma) \in \langle S \rangle$. □

Γ is finitely generated (if M is compact)
because $S = \{\, \gamma \in \Gamma \mid \gamma C \cap C \neq \varnothing \,\}$ is finite.

For noncompact case, can construct a nice *fundamental domain* for Γ in X:
$\Gamma C = X$, $\{\, \gamma \in \Gamma \mid \gamma C \cap C \neq \varnothing \,\}$ is finite.
Furthermore, C is open.

- Finite generation follows from above argument.
- Finite presentation follows from a more sophisticated argument
  (since X is connected, locally connected, and simply connected)
  [Platonov-Rapinchuk, Thm. 4.2, p. 195]

Introduction to Arithmetic Groups 3

- noncompactness via isotropic vectors
- $\mathbb{Q}$-rank and the asymptotic cone
- cocompact arithmetic subgroups of $\mathrm{SO}(1,n)$
  (restriction of scalars)

For further reading, see D. W. Morris, *Introduction to Arithmetic Groups.*
http://people.uleth.ca/~dave.morris/books/IntroArithGroups.html
More advanced:
V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory,* Academic Press, 1993.
C. Maclachlan and A. Reid, *The Arithmetic of Hyperbolic 3-Manifolds,* Springer, 2002.

Noncompactness via isotropic vectors

Example

$\Gamma = \mathrm{SO}(1,3;\mathbb{Z})$ is an arithmetic subgroup of $\mathrm{SO}(1,3)$.
(provides hyperbolic 3-manifold $M = \Gamma\backslash\mathbf{H}^3$)

Is M compact?

Proposition

Spse $Q(\vec{x})$ is a (nondegenerate) *quadratic form over $\mathbb{Z}$*
(e.g., $Q(x_1,x_2,x_3) = x_1^2 - 3x_2^2 - 7x_3^2$)
Let $G = \mathrm{SO}(Q)$ and $\Gamma = \mathrm{SO}(Q;\mathbb{Z})$.
Then $\Gamma\backslash G$ is not compact $\iff$
$\exists$ isotropic $\mathbb{Q}$-vectors: $Q(v) = 0$ with $v \neq 0$.

$G = \mathrm{SO}(Q)$ and $\Gamma = \mathrm{SO}(Q;\mathbb{Z})$.
$\Gamma\backslash G$ is *not* compact $\iff$ $\exists v \in (\mathbb{Q}^n)^\times,\ Q(v) = 0$.

Proof ($\Rightarrow$).

Godement Criterion: $\exists$ unipotent $u \in \Gamma$.
Jacobson-Morosov (over $\mathbb{Q}$):

$\exists\ \rho\colon \mathrm{SL}(2,\mathbb{Q}) \to G_{\mathbb{Q}}$ with $\rho\left(\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}\right) = u$.

Let $a = \rho\left(\begin{bmatrix} 2 & \\ & 1/2 \end{bmatrix}\right)$.

Algebraic Group Thry: a is diagonalizable over $\mathbb{Q}$,
so a has eigenvector $v \in \mathbb{Q}^n$ with eigenval $\lambda \neq \pm 1$.
Then $Q(v) = Q(a^k v) = Q(\lambda^k v) = \lambda^{2k} Q(v) \to 0$.
So $Q(v) = 0$. □

$G = \mathrm{SO}(Q)$ and $\Gamma = \mathrm{SO}(Q;\mathbb{Z})$.
$\Gamma\backslash G$ is *not* compact $\iff$ $\exists v \in (\mathbb{Q}^n)^\times,\ Q(v) = 0$.

Example

$\Gamma = \mathrm{SO}(1,3;\mathbb{Z}) \implies \Gamma\backslash\mathbf{H}^3$ is *not* compact.

Proof: $Q(x_0,x_1,x_2,x_3) = x_0^2 - x_1^2 - x_2^2 - x_3^2$,
so $Q(1,1,0,0) = 1^1 - 1^2 - 0^2 - 0^2 = 0$.

Example

Let $Q(\vec{x}) = 7x_0^2 - -x_1^2 x_2^2 - x_3^2$ and $\Gamma = \mathrm{SO}(Q;\mathbb{Z})$.
Then $\Gamma\backslash\mathbf{H}^3$ is compact.

Proof: 7 is *not* a sum of 3 squares (in $\mathbb{Q}$),
so Q has no isotropic vectors.

Example

Let $Q(\vec{x}) = 7x_0^2 - x_1^2 - x_2^2 - x_3^2$ and $\Gamma = \mathrm{SO}(Q;\mathbb{Z})$.
Then $\Gamma\backslash\mathbf{H}^3$ is compact. (bcs 7 is not a sum of 3 squares)

Recall: Every positive integer is a sum of 4 squares.
So this method will not construct compact hyperbolic n-manifolds for $n > 3$.

Fact from Number Theory

If $Q(x_1,\ldots,x_n)$ is a quadratic form over $\mathbb{Z}$,
with $n \geq 5$, and Q is isotropic over $\mathbb{R}$,
then Q is isotropic.

Need to do something more sophisticated.
(Return to this later: "restriction of scalars")

$\mathbb{Q}$-rank and the asymptotic cone

$G = \mathrm{SO}(Q)$ and $\Gamma = \mathrm{SO}(Q;\mathbb{Z})$.
$\Gamma\backslash G$ is *not* compact $\iff$ $\exists v \in (\mathbb{Q}^n)^\times,\ Q(v) = 0$.

Definition

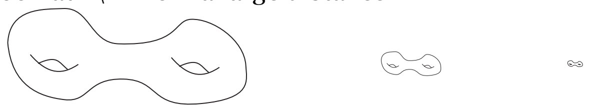
Let $\Gamma = \mathrm{SO}(Q;\mathbb{Z})$.
- $V \subset \mathbb{Q}^n$ is *totally isotropic* if $Q(V) = 0$.
- $\mathbb{Q}$-rank(Γ) = max dim tot isotrop $\mathbb{Q}$-subspace.

Example

Suppose $\mathbb{Q}$-rank$(\Gamma) = 0$. Then $\nexists$ isotropic $\mathbb{Q}$-vector.
so $M = \Gamma\backslash X$ is compact.

Example

Suppose $\mathbb{Q}$-rank$(\Gamma) = 0$. Then $\nexists$ isotropic $\mathbb{Q}$-vector.
so $M = \Gamma\backslash X$ is compact.
Look at $\Gamma\backslash X$ from a large distance.



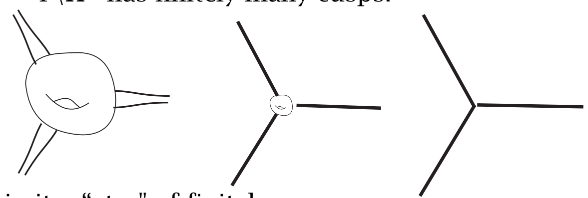
$\Gamma\backslash X$ compact $\Rightarrow$ limit is a point.
$\therefore$ dimension of limit $= 0 =$ $\mathbb{Q}$-rank(Γ).

Definition

asymptotic cone of metric space (M,d)
$= \lim_{t\to\infty}\left((M, \tfrac{1}{t}d), m_0\right)$.

Example

Spse $\Gamma \subset \mathrm{SO}(1,n)$, and $\Gamma\backslash\mathbf{H}^n$ not compact.
$\Gamma\backslash\mathbf{H}^n$ has finitely many cusps.



Limit = "star" of finitely many rays.
$\therefore$ dimension of limit $= 1 =$ $\mathbb{Q}$-rank(Γ).

Theorem (Hattori)

Asymptotic cone of $\Gamma\backslash X$ is a simplicial complex whose dimension is $\mathbb{Q}$-rank(Γ).

Theorem (Hattori)

Asymptotic cone of $\Gamma\backslash X$ is a simplicial complex whose dimension is $\mathbb{Q}$-rank(Γ).

More precisely, the asymptotic cone of $\Gamma\backslash X$ is equal to the cone on the "Tits building" of parabolic $\mathbb{Q}$-subgroups of G.

Remark

$\Gamma\backslash X$ is *quasi-isometric* to its asymptotic cone.

Remark

Another important application of $\mathbb{Q}$-rank:
cohomological dimension of $\Gamma = \dim X - \mathbb{Q}$-rank$(\Gamma)$
(if Γ is torsion-free)

Cocompact lattices in $\mathrm{SO}(1,n)$

Example

Let

- $\alpha = \sqrt{2}$,
- $Q(\vec{x}) = x_0^2 - \alpha x_1^2 - \alpha x_2^2 - \cdots - \alpha x_n^2$,
- $G = \mathrm{SO}(Q) \cong \mathrm{SO}(1,n)$,
- $\Gamma = G_{\mathbb{Z}[\alpha]} = G \cap \mathrm{SL}(n+1, \mathbb{Z}[\alpha])$.

Then Γ is a cocompact arithmetic subgroup of G.

Later: why Γ is an arithmetic subgroup.

Key observation for compactness

Q has no isotropic $\mathbb{Q}(\alpha)$-vectors.

$\alpha = \sqrt{2}$, $Q(\vec{x}) = x_0^2 - \alpha x_1^2 - \alpha x_2^2 - \cdots - \alpha x_n^2$

Key observation for compactness

Q has no isotropic $\mathbb{Q}(\alpha)$-vectors.

Proof.

Suppose $Q(v) = 0$.

Galois auto of $\mathbb{Q}(\alpha)$: $(a + b\alpha)^\sigma = a - b\alpha$.

$$Q^\sigma(\vec{x}) = x_0^2 + \alpha x_1^2 + \alpha x_2^2 + \cdots + \alpha x_n^2.$$

$$\begin{aligned} 0 &= Q(v)^\sigma \\ &= (v_0^\sigma)^2 + \alpha(v_1^\sigma)^2 + \cdots + \alpha(v_n^\sigma)^2 \\ &= Q^\sigma(v^\sigma). \end{aligned}$$

Since all coefficients of Q^σ are positive, must have $v^\sigma = 0$.

So $v = 0$. □

More general

- $\alpha_0, \alpha_1, \ldots, \alpha_n$ algebraic integers, s.t.
  - $\alpha_0 > 0$ and $\alpha_1, \alpha_2, \ldots, \alpha_n < 0$,
  - $\forall$ Galois aut σ of $\mathbb{Q}(\alpha_0, \ldots, \alpha_n)$, $\alpha_0^\sigma, \ldots, \alpha_n^\sigma$ all have the same sign (all positive or all negative).

Then

- $G = \mathrm{SO}(\alpha_0 x_0^2 + \cdots + \alpha_n x_n^2; \mathbb{R}) \cong \mathrm{SO}(1,n)$,
- $\Gamma = G_{\mathbb{Z}[\alpha_0,\ldots,\alpha_n]}$ is a cocpct arith subgrp of G.

If n is even, this construction provides *all* of the cocompact arithmetic subgroups of $\mathrm{SO}(1,n)$.

For n odd, also need $\mathrm{SO}(Q;$ **quaternion algebra**$)$
(And $n = 7$ has additional "triality" subgroups.)

Definition of arithmeticity

Recall

Arithmetic subgroup:

$\Gamma = G_{\mathbb{Z}} := G \cap \mathrm{SL}(n,\mathbb{Z})$ for suitable $G \subset \mathrm{SL}(n,\mathbb{R})$.

We always assume G is semisimple, connected.

Theorem

G is (almost) Zariski closed
(defined by polynomial functions on $\mathrm{Mat}_{n\times n}(\mathbb{R})$*)*

Example

$\mathrm{SL}(2,\mathbb{R}) = \{\, A \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \mid \det A = 1 \,\}$
and $\det A = a_{1,1}\, a_{2,2} - a_{1,2}\, a_{2,1}$ is a polynomial.

Definition

G is *defined over* $\mathbb{Q}$:
G is defined by polynomial funcs with coeffs in $\mathbb{Q}$.

Example

- $\mathrm{SL}(n,\mathbb{R})$ is defined over $\mathbb{Q}$.
- $\mathrm{SO}(1,n)$ is defined over $\mathbb{Q}$.
- Let $\alpha = \sqrt{2}$ and $Q(\vec{x}) = x_0^2 - \alpha x_1^2 - \alpha x_2^2$
  Then $G = \mathrm{SO}(Q)$ is *not* defined over $\mathbb{Q}$.
  (It is defined over $\mathbb{Q}[\alpha]$.)

Definition (starting point)

$G_{\mathbb{Z}}$ is an *arithmetic subgroup* of G
if *G is defined over* $\mathbb{Q}$.

Definition (starting point)

$G_{\mathbb{Z}}$ is an *arithmetic subgroup* of G
if *G is defined over* $\mathbb{Q}$.

Complete definition is more general; it ignores:

- compact factors of G, and
- differences by only a finite group.

Definition

Spse $G \times K \hookrightarrow \mathrm{SL}(n,\mathbb{R})$, defined over $\mathbb{Q}$, with K cpct.
Let Γ' = image of $(G \times K)_{\mathbb{Z}}$ in G.
Any subgroup Γ of G that is *commensurable* with Γ'
($\Gamma \cap \Gamma'$ has finite index in both Γ and Γ')
is an *arithmetic subgroup* of G.

Restriction of scalars

Recall

$\alpha = \sqrt{2}$, $Q(\vec{x}) = x_0^2 - \alpha x_1^2 - \alpha x_2^2 - \cdots - \alpha x_n^2$,
$G = \mathrm{SO}(Q;\mathbb{R})$, $\Gamma = \mathrm{SO}(Q;\mathbb{Z}[\alpha])$.

Want to show Γ is an arithmetic subgroup of G.

As an warm-up, let us show $\mathrm{SL}(2,\mathbb{Z}[\alpha])$ is $\cong$ an arithmetic subgroup of $\mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{R})$.

Example

- $\Gamma = \mathrm{SL}(2,\mathbb{Z}[\alpha])$, with $\alpha = \sqrt{2}$,
- $G = \mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{R})$,
- σ = Galois automorphism of $\mathbb{Q}[\alpha]$,
- $\Delta\colon \Gamma \to G\colon \gamma \mapsto (\gamma, \gamma^\sigma)$.

Then Γ^Δ is an arithmetic subgroup of G.

Outline of proof.

Since $\{1^\Delta, \alpha^\Delta\} = \{(1,1), (\alpha,-\alpha)\}$ is linearly indep,
$\exists\, T \in \mathrm{GL}(2,\mathbb{R})$ with $T(\mathbb{Z}[\alpha]^\Delta) = \mathbb{Z}^2$.
$\hat{T} = T \oplus T \in \mathrm{GL}(4,\mathbb{R})$ has $\hat{T}(\mathbb{Z}[\alpha]^\Delta)^2 = (\mathbb{Z}^2)^2 = \mathbb{Z}^4$.
So $(\hat{T}\,\Gamma^\Delta\,\hat{T}^{-1})(\mathbb{Z}^4) = \mathbb{Z}^4$, so $\hat{T}\,\Gamma^\Delta\,\hat{T}^{-1} \subset \mathrm{SL}(4,\mathbb{Z})$.

In fact, $\hat{T}\,\Gamma^\Delta\,\hat{T}^{-1} = \mathrm{SL}(4,\mathbb{Z}) \cap \hat{T}\,G\,\hat{T}^{-1}$, and $\hat{T}\,G\,\hat{T}^{-1}$ is defined over $\mathbb{Q}$
So Γ^Δ is an arithmetic subgroup of G. □

$\alpha = \sqrt{2}$, $Q(\vec{x}) = x_0^2 - \alpha x_1^2 - \alpha x_2^2 - \cdots - \alpha x_n^2$,
$G = \mathrm{SO}(Q;\mathbb{R})$, $\Gamma = \mathrm{SO}(Q;\mathbb{Z}[\alpha])$.

Want to show Γ is an arithmetic subgroup of G.

Idea of proof.

Galois aut of $\mathbb{Q}(\alpha)$: $(a + b\alpha)^\sigma = a - b\alpha$.
$G^\sigma = \mathrm{SO}(x_1^2 + x_2^2 + \alpha x_3^2 + \alpha x_4^2 + \alpha x_5^2) \cong \mathrm{SO}(5)$.
Map $\Delta\colon z \mapsto (z, z^\sigma)$ gives $\Gamma^\Delta \subset G \times G^\sigma$.
After change of basis (mapping $(\mathbb{Z}[\alpha]^\Delta)^n$ to $\mathbb{Z}^{2n}$),
we have $\Gamma^\Delta = \mathrm{SL}(n,\mathbb{Z}) \cap (G \times G^\sigma)$
so Γ^Δ is an arithmetic subgroup of $G \times G^\sigma$.
Can mod out the compact group G^σ,
so Γ is arithmetic subgroup of G. □

Restriction of scalars

Suppose

- G is defined over $\mathbb{Q}(\alpha)$ (algebraic number field),
- $\sigma_1, \ldots, \sigma_n \colon \mathbb{Q}(\alpha) \to \mathbb{C}$ are the noncon-jugate embeddings.

Then

- $G^* = G^{\sigma_1} \times G^{\sigma_2} \times \cdots \times G^{\sigma_n}$ is defined over $\mathbb{Q}$, and
- $G_{\mathbb{Z}[\alpha]}$ is isomorphic to $(G^*)_{\mathbb{Z}}$ via the map $\Delta \colon \gamma \mapsto (\gamma^{\sigma_1}, \gamma^{\sigma_2}, \ldots, \gamma^{\sigma_n})$.

We assume here that $\mathbb{Z}[\alpha]$ is the entire ring of integers of $\mathbb{Q}(\alpha)$.

Example: If $Q(\vec{x})$ has coefficients in $\mathbb{Q}(\alpha)$, then $\mathrm{SO}(Q; \mathbb{Z}[\alpha])$ is an arithmetic subgroup of a product of orthogonal groups.