An introduction to arithmetic groups

Lizhen Ji
CMS, Zhejiang University
Hangzhou 310027, China
&
Dept of Math, Univ of Michigan
Ann Arbor, MI 48109

June 27, 2006

Plan.

1. Examples of arithmetic groups

2. Definition of arithmetic groups

3. Basic properties of arithmetic groups

4. Discrete (lattice) subgroups of Lie groups

5. Rigidities of lattices and locally symmetric spaces

6. Compactifications of locally symmetric spaces

7. Spectral theory of automorphic forms

8. Large scale geometry of discrete groups

9. Cohomology of arithmetic groups

The most basic example of arithmetic groups is $\mathbb{Z}$, the ring of integers.

(Recall that by arithmetic, one means the study of integers).

So it is natural that $\mathbb{Z}$ is an arithmetic group.

When we consider $\mathbb{Z}$ as an arithmetic group, we consider it as a subgroup of $\mathbb{R}$. $\mathbb{Z} \subset \mathbb{R}$. This embedding is important since we can for the quotient $\mathbb{Z}\backslash\mathbb{R}$. The Poisson summation formula relates the spectral theory and the lengths of closed geodesics. It is fundamental in many applications.

$\mathbb{Z}$ is an infinite cyclic group. A natural generalization is $\mathbb{Z}^n$, the free *abelian* group on n-generators.

The Poisson formula for $\mathbb{Z}^n$ and other lattices in $\mathbb{R}^n$ is crucial to recent work on lattice sphere packing.

A non-abelian generalization $SL(2,\mathbb{Z})$

$$SL(2,\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}, ad-bc=1\}.$$

This is often called the modular group.

It is an arithmetic subgroup of the Lie group $SL(2,\mathbb{R})$.

A further generalization is $SL(n,\mathbb{Z}) \subset SL(n,\mathbb{R})$, $n \geq 2$.

Another important example is the sympletic modular group $Sp(n,\mathbb{Z})$, an arithmetic subgroup of

$$Sp(n,\mathbb{R}) = \{g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \mid A,B,C,D \text{ are } n \times n \text{ matrices}$$

$$g^t \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} g = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}\}.$$

Definition of Arithmetic groups

The above examples suggest the following procedure to get arithmetic groups.

1. Start with a Lie group $\mathbf{G}(\mathbb{R})$.

2. Take the subgroup of *integral* elements $\mathbf{G}(\mathbb{Z})$.

To make this procedure precise, we need the notion of algebraic groups.

A topological group G

It is a group and also a topological space such that the group operations:

Product $G \times G \to G, (g_1, g_2) \to g_1 g_2$,

and the **inverse** $G \to \mathbf{G}, g \to g^{-1}$,

are continuous maps.

(Morphisms in the category of topological spaces).

A Lie group G

It is a group and a manifold such that the group operations are smooth maps (actually being continuous is sufficient, Hilbert's fifth problem).

Algebraic group

It is a group and a variety such that the group operations are morphisms between varieties.

Recall that an affine variety V is a subspace of $\mathbb{C}^n$ defined by polynomial equations.

$V = \{x \in \mathbb{C}^n \mid P_i(x) = 0, i \in I\}$.

If the coefficients of all P_i, $i \in I$, belong to $\mathbb{Q}$, the variety V is said to be defined over $\mathbb{Q}$.

Example. $GL(n) = GL(n, \mathbb{C})$ is an affine variety defined over $\mathbb{Q}$.

Clearly, it is a subspace of the affine space $M_n(\mathbb{C})$ of $n \times n$-matrices. $M_n(\mathbb{C}) = \mathbb{C}^{n^2}$.

$GL(n, \mathbb{C}) = \{g \in M_n(\mathbb{C}) \mid \det g \neq 0\}$.

But this does not show that $GL(n, \mathbb{C})$ is an affine algebraic group.

We need another embedding

$$GL(n,\mathbb{C}) \hookrightarrow M_n(\mathbb{C}) \times \mathbb{C} = \mathbb{C}^{n^2+1}$$

$$g \mapsto (g, (\det g)^{-1}).$$

Under this embedding, $GL(n,\mathbb{C})$ is identified with the affine subspace $\{(m,z) \in M_n(\mathbb{C}) \times \mathbb{C} \mid \det m \ z = 1\}$.

Clearly, this variety is defined over $\mathbb{Q}$ (in fact, over $\mathbb{Z}$). The group operations are polynomial functions of the matrix entries and z.

Therefore, $GL(n) = GL(n,\mathbb{C})$ is an affine algebraic group defined over $\mathbb{Q}$.

$SL(n)$ and $Sp(n)$ are also algebraic groups defined over $\mathbb{Q}$.

Affine algebraic groups are often called *matrix groups* once an embedding into $GL(n)$ is chosen.

Definition. An algebraic group is said to be defined over $\mathbb{Q}$ if the variety is defined over $\mathbb{Q}$ and the group operations are morphisms defined over $\mathbb{Q}$.

The polynomial equations which define the group often come from the fact that the group preserves some structures. For example, $SL(n)$ preserves the volume form.

Let $\mathbf{G}$ be an algebraic group defined over $\mathbb{Q}$. Then $\mathbf{G}(\mathbb{Q}) = \mathbf{G}(\mathbb{C}) \cap GL(n, \mathbb{Q})$ is well-defined.

Usually we specify an embedding $\mathbf{G} \subset GL(n, \mathbb{C})$. Then we can define

$\mathbf{G}(\mathbb{Z}) = \mathbf{G}(\mathbb{Q}) \cap GL(n, \mathbb{Z})$.

$\mathbf{G}(\mathbb{Z})$ depends on the embedding $\mathbf{G} \subset GL(n, \mathbb{C})$.

Definition. A subgroup Γ of $\mathbf{G}(\mathbb{Q})$ is called an **arithmetic subgroup** if it is **commensurable with** $\mathbf{G}(\mathbb{Z})$, i.e., the intersection $\Gamma \cap \mathbf{G}(\mathbb{Z})$ has finite index in both Γ and $\mathbf{G}(\mathbb{Z})$. In particular, $\mathbf{G}(\mathbb{Z})$ and its subgroups of finite index are arithmetic groups.

$\mathbb{Z}$ and $SL(2, \mathbb{Z})$ satisfy these conditions here.

Fact: The class of arithmetic subgroups is well-defined and independent of the embedding $\mathbf{G} \subset GL(n, \mathbb{C})$. (Though $\mathbf{G}(\mathbb{Z})$ depends on the embedding.)

Basic properties of Arithmetic groups as abstract groups

Let $\Gamma \subset \mathbf{G}(\mathbb{Q})$ be an arithmetic subgroup. In many (most) cases, arithmetic subgroups are infinite.

Facts: 1. Γ is finitely generated.

2. Γ is finitely presented.

Finite generations means: there are finitely many elements $\gamma_1, \cdots, \gamma_n$ such that every element of Γ can be written as products of these elements.

In other words, let F_n be the free group on n generators. Then there is a surjective map

$F_n \to \Gamma$.

Finite presentations mean: there are only finitely many (non-redundant) relations between the generators $\gamma_1, \cdots, \gamma_n$.

In other words, the kernel of the morphism $F_n \to \Gamma$ is finitely generated. Hence there is an exact sequence

$$F_m \to F_n \to \Gamma \to \{1\},$$

where m is the number of relations.

There are other finiteness conditions.

Fact. Every arithmetic subgroup Γ has a torsion-free subgroup Γ' of finite index, $[\Gamma, \Gamma'] < +\infty$.

It often allows one to assume that Γ is torsion-free.

Question. How to prove these properties?

Amswer. Use the action of Γ on suitable spaces.

This is the general principle: groups are understood through actions. For example, a very basic type of action is given by representation theory. Certainly the representation theory is important.

To study $SL(2,\mathbb{Z})$ and its subgroups, the action of $SL(2,\mathbb{R})$ on

$\mathbb{H}^2 = SL(2,\mathbb{R})/SO(2) = \{x+iy \mid y > 0, x \in \mathbb{R}\}$, the upper half plane, is fundamental.

In fact, $SL(2,\mathbb{R})$ acts transitively on $\mathbb{H}^2$ and the stabilizer is $SO(2)$.

$SO(2) = S^1$ is a maximal compact subgroup, i.e., not contained properly in another compact subgroup of $SL(2,\mathbb{R})$.

Let $G = \mathbf{G}(\mathbb{R})$ be the real locus, a Lie group with finitely many connected components.

Let $K \subset G$ be a maximal compact subgroup, and $X = G/K$ endowed with a G-invariant metric (translate an inner product on $T_oX = \mathfrak{g}/\mathfrak{k}$ to other points).

Assume from now on that $\mathbf{G}$ is a semisimple algebraic group.

Then G is a semi-simple Lie group,

and X is a symmetric space of noncompact type (of nonnegative curvature and simply connected).

Γ acts properly on $X = G/K$,

i.e., for any compact subset $K \subset X$,

$\{\gamma \in \Gamma \mid \gamma K \cap K \neq \emptyset\}$ is finite.

Definition. For any $x \in X$, $\Gamma_x = \{\gamma \in \Gamma \mid \gamma x = x\}$ is called the stabilizer of x in Γ.

Since the Γ-action is proper, Γ_x is finite.

If for every $x \in X$, Γ_x is trivial, the action of Γ is called fixed-point free.

Fact. If Γ is torsion-free, i.e., does not contain any element of finite order, then Γ acts freely.

Fact. The quotient $\Gamma\backslash X$ is a Hausdorff space. If Γ is torsion-free, then $\Gamma\backslash X$ is a manifold.

If Γ is not torsion-free, then $\Gamma\backslash X$ is an orbifold (or V-manifold).

The quotient space $\Gamma\backslash X$ often occurs naturally as the moduli space in number theory, algebraic geometry etc.

To understand $\Gamma\backslash X$, an important concept is the notion of fundamental domains.

Definition. An open subset Ω of X is called a **fundamental domain** for the Γ-action on X if

(1) $\Gamma\overline{\Omega} = X$.

(2) For every $x \in \Omega$, $\Gamma x \cap \Omega = \{x\}$

(3) For every $x \in \overline{\Omega}$, $\Gamma c \cap \overline{\Omega}$ is finite.

Basically, $\Gamma\backslash X$ is obtained from $\overline{\Omega}$ by identifying some points on the boundary of Ω.

So $\Omega \to \Gamma\backslash X$ is injective, and $\Omega \to \Gamma\backslash X$ is surjective.

Fact. If there are only finitely many $\gamma_1, \cdots, \gamma_n$ such that $\gamma_i\overline{\Omega} \cap \overline{\Omega} \neq \emptyset$, then Γ is generated by $\gamma_1, \cdots, \gamma_m$.

Example. Let $\Gamma = SL(2,\mathbb{Z})$, $G = SL(2,\mathbb{R})$, $X = \mathbb{H}$. Then a well-known fundamental domain for Γ is as follows.

Corollary. $SL(2,\mathbb{Z})$ is generated by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$,

Corollary. The quotient $\Gamma\backslash\mathbb{H}$ is noncompact and has finite area.

The theory of finding a good fundamental domain is called the **reduction theory**.

In general, it is very difficult to find a fundamental domain.

Instead we need the notion of fundamental sets.

Definition. A subset Σ of X is called a **fundamental set** for the Γ-action on X if

(1) $\Gamma\Sigma = X$,

(2) for every $\gamma_0 \in \Gamma$, $\{\gamma \in \Gamma \mid \gamma\Sigma \cap \Sigma \neq \gamma_0\emptyset\}$ is finite.

So the map $\Sigma \to \Gamma\backslash X$ is surjective and finite-to-one.

The reduction theory was developed by Siegel, Borel, Harish-Chandra etc.

If $\Gamma\backslash X$ is compact, it is easy to construct a fundamental set. In fact, there exists a fundamental set given by a compact set Σ_0.

The difficulty lies in the case when $\Gamma\backslash X$ is noncompact.

For the example of $SL(2,\mathbb{Z})$, the noncompact part of the fundamental domain is a vertical strip.

This is the so-called **Siegel set**.

In general, a fundamental set is given by the union of finitely many Siegel sets.

Such a fundamental set is not a fundamental domain. This can be seen clearly in the example of $SL(2,\mathbb{Z})$.

Corollary $\Gamma\backslash X$ has finite volume. Γ is finitely generated and presented.

Discrete subgroups of Lie groups and arithmeticity

Let G be a Lie group with finitely many connected components. A subgroup $\Gamma \subset G$ is called a discrete subgroup if the induced (subspace)topology on Γ from $\mathbf{G}$ is discrete.

Then the multiplication of Γ on G gives a proper action.

Clearly, arithmetic subgroups are discrete subgroups (since $\mathbb{Z}$ is a discrete subgroup of $\mathbb{R}$.)

But the converse is certainly not true.

If G is a noncompact semi-simple Lie group, then for any $\gamma \in G$, the subgroup generated by γ is a discrete subgroup, but never an arithmetic subgroup.

The reason is that it is not a lattice.

This may not be so interesting.

More interesting example.

Let S_g be a compact Riemann surface of genus $g \geq 2$.

By the uniformization theorem, there is a discrete subgroup $\Gamma \subset SL(2, \mathbb{R})$ such that

$S_g = \Gamma \backslash \mathbb{H}$.

Fact. For most S_g, Γ is not an arithmetic subgroup.

Why? There are only countably infinitely many arithmetic subgroups.

On the other hand, there are uncountably infinitely many Riemann surfaces of genus g (there are $6g-6$ parameters to describe the variation of the complex structure).

Question. When is a discrete subgroup an arithmetic subgroup?

For simplicity, assume that G is simple (non-abelian) Lie group.

As mentioned above, if Γ is an arithmetic subgroup, then the volume of $\Gamma\backslash X$ is finite.

Definition. A discrete subgroup Γ of G is called a *lattice (or cofinite discrete subgroup)* if $\Gamma\backslash G$ has finite volume.

Question. If Γ is a lattice in G, (the necessary condition is satisfied), when is Γ an arithmetic subgroup?

As mentioned above, when $G = SL(2, \mathbb{R})$, the conclusion is not true. Rank of $SL(2, \mathbb{R})$ is 1.

Arithmeticity. If the rank of G is at least 2, then every lattice is an arithmetic subgroup.

Comments on arithmetic subgroups of Lie groups

Since a Lie group may not be equal to the real locus of an algebraic group, we need a more general definition of arithmetic subgroups.

Let G be a Lie group, $\Gamma \subset G$ be a discrete subgroup. Γ is called an *arithmetic subgroup* of G if there exists an algebraic group $\mathbf{H}$ defined over $\mathbb{Q}$ and a Lie group homomorphism

$\varphi : G \to \mathbf{H}(\mathbb{R})$ whose kernel is compact such that the image $\varphi(\Gamma)$ is an arithmetic subgroup of $\mathbf{H}(\mathbb{Q})$.

Rank of G

Let $X = G/K$ be the symmetric space associated with G as above.

The rank of G is the maximal dimension of flat subspaces in X, i.e., the maximal dimension of $\mathbb{R}^r$ which can be isometrically embedded into X, $\mathbb{R}^r \hookrightarrow X$.

Example. For $G = SL(n, \mathbb{R})$, the rank is equal to $n - 1$.

Why is the assumption that rank is at least 2 is important?

Under this assumption, the flat subspaces of X are highly related and these structure make the spaces very rigid. Part of the Tits building theory.

Arithmeticity also holds for some rank one spaces.

In fact, except those of the real and complex hyperbolic spaces, lattices in other rank-1 groups are arithmetic by combining results of Corlette, Gromov-Schoen.

Non-arithmetic lattices acting on the real and complex hyperbolic spaces have been constructed by various people, for example, Gromov, Piateski-Shapiro, Mostow, Siu, Deligne etc.

It is not easy.

Importance: Arithmetic groups are easier to be understood.

How do arithmetic groups arise?

An important source is that many natural transformations and identifications are given by arithmetic groups.

Example. Given a quadratic form with integral coefficients $Q(x, y) = ax^2 + 2bxy + cy^2$, a natural question is when an integer n can be represented by the quadratic form $Q(x, y)$,

$n = Q(x, y)$ has integral solutions.

Identify the quadratic form Q with the symmetric matrix $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$.

For any $g \in SL(2,\mathbb{Z})$, we can make a change of variable $[x,y] = [u,v]g$. Then the quadratic form $Q(x,y)$ becomes a new quadratic form corresponding to the matrix gAg^t.

Clearly, these two quadratic forms A and gAg^t represent the same set of integers.

We call such forms A and gAg^t equivalent.

The equivalence is given by $SL(2,\mathbb{Z})$.

Fact. The set of equivalent classes of positive quadratic forms with real coefficients and determinant 1 is naturally identified with $SL(2,\mathbb{Z})\backslash\mathbb{H}$.

A discrete subgroup Λ of $\mathbb{R}^n$ with a compact quotient $\Lambda\backslash\mathbb{R}^n$ is called a lattice.

If $\mathrm{vol}(\Lambda\backslash\mathbb{R}^n) = 1$, it is called *unimodular*.

The space of all unimodular lattices in $\mathbb{R}^n$ can be identified with $SL(n,\mathbb{Z})\backslash SL(n,\mathbb{R})$.

(Since $SL(n,\mathbb{R})$ acts transitively on the set of unimodular spaces, and the stabilizer of $\mathbb{Z}^n$ is $SL(n,\mathbb{Z})$.

Many other moduli spaces in number theory and algebraic grometry are also of the form $\Gamma\backslash X$, where Γ is arithmetic, X is a symmetric space.

Rigidity Phenomenon.

Locally symmetric spaces $\Gamma\backslash X$ are often very rigid due to their rich structures.

Question. How is the geometry of $\Gamma\backslash X$ determined by its topology?

$\pi_1(\Gamma\backslash X) = \Gamma, \quad \pi_i(\Gamma\backslash X) = \{1\}, i \geq 2.$

This implies that the topology (or the homotopy type of $\Gamma\backslash X$ is determined by $\pi_1 = \Gamma$.)

Mostow strong rigidity. If G is simple and not equal to $SL(2, \mathbb{R})$, and $\Gamma \subset G$ is a lattice subgroup. Then $\Gamma\backslash X$ is determined isometrically up to scaling by Γ.

Homotopy of $\Gamma_1\backslash X_1$ and $\Gamma_2\backslash X_2$ implies that they are isometric, basically, the same $G_1 = G_2$ and $\Gamma_1 = \Gamma_2$.

Topology implies **Geometry**

There are other notions of rigidity.

Another is the famous:

Borel conjecture: If two closed aspherical manifolds are homotopic, then they are homeomorphic.

Definition. A manifold M is called *aspherical* if for every $i \geq 2$, $\pi_i(M) = \{1\}$.

$\Gamma \backslash X$ is aspherical.

If both manifolds are locally symmetric spaces, then the Borel conjecture follows from the Mostow strong rigidity.

Compactifications of $\Gamma\backslash X$.

If $\Gamma\backslash X$ is noncompact, we need to compactify it for various purposes.

This is a long story.

Even when $X = \mathbb{H}$, there are several obviously different compactifications.

1. Adding a point to each cusp neighborhood.

This is a Satake compactification.

2. Adding a circle to each cusp neighborhood so that the compactified space is a surface with boundary. This is the Borel-Serre compactification.

What's the use of them?

Other topics related to arithmetic subgroups

1. Large scale geometry

2. Spectral Theory of automorphic forms

This is the origin of the Langlands program.
The Poisson summation formula

The Selberg trace formula

3. Cohomology of arithmetic groups

Large scale geometry.

An important point of view emphasized by Gromov is to treat a group Γ as a metric space and study its large scale properties.

Word metric. Assume that Γ is finitely generated. Let S be a finite set of generators of Γ.

Then we define a word metric $d_S(\gamma_1, \gamma_2)$, which is equal to the minimum length of ${\gamma_1}^{-1}\gamma_2$ in terms of the generators.

This defines a left invariant metric on Γ.

Cayley graph of Γ

Each element of Γ gives a vertex, and two vertices γ_1, γ_2 are connected by an edge if and only if $\gamma_1^{-1}\gamma_2$ belongs to the set S of generators.

The Cayley graph has a natural metric, where every edge has length 1.

The metric space (Γ, d_S) is quasi-isometric to the Cayley graph.

In the second lecture in August, I will discuss some global geometry of (Γ, d_S).

Spectral Theory

The spectral theory of $\Gamma\backslash X$ and its relation to the geometry of $\Gamma\backslash X$ is important.

The most basic, but very important example is the **Poisson summation formula**. In this case, $\Gamma = \mathbb{Z}$ and $X = \mathbb{R}$.

For a rapidly decreasing function f, let $\widehat{f}$ be its Fourier transformation.

Then

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(2\pi n).$$

This gives a relation between the spectrum and geometry (lengths of geodesics) of the manifold $\mathbb{Z}\backslash\mathbb{R}$.

It has many applications, for example, the meromorphic continuation and functional equation of the Riemann zeta function

$\zeta(s) = \sum_{n \in \mathbb{Z}} \frac{1}{n^s}, \quad \text{Re}(s) > 1.$

For non-abelian groups such as $SL(2, \mathbb{Z})$, a vast generalization is given by the Selberg trace formula,

a very important tool in the modern theory of automorphic forms.

Cohomology of arithmetic groups

This is a vast field with many connections to topology, geometry, number theory and algebraic K-theory.

An important connection is that if Γ is torsion-free, then

$$H^*(\Gamma, \mathbb{Z}) = H^*(\Gamma \backslash X, \mathbb{Z}).$$

There are also several different kinds of cohomology theories.

Generalization of arithmetic subgroups

The ring $\mathbb{Z}$ of integers is certainly very important in number theory.

But there are also other rings, for example, the extended ring by inverting finitely many primes, $\mathbb{Z}[\frac{1}{p_1}, \cdots, \frac{1}{p_m}]$.

This is the so-called ring of S-integers.

(S stands for the set of primes $p_1, \cdots, p_m, \infty$).

Then we obtain S-arithmetic subgroups such as $SL(n, \mathbb{Z}[\frac{1}{p_1}, \cdots, \frac{1}{p_m}])$.

One **difference** with arithmetic subgroups is that arithmetic subgroups are discrete subgroups of (real) Lie groups,

but S-arithmetic subgroups are not discrete subgroups of Lie groups,

for example, $SL(2, \mathbb{Z}[\frac{1}{p}])$ is contained in $SL(2, \mathbb{R})$, but is not embedded as a discrete subgroup.

Instead, it is a discrete subgroup of $SL(2, \mathbb{R}) \times SL(2, \mathbb{Q}_p)$, where $\mathbb{Q}_p$ is the field of p-adic numbers.

Arithmetic subgroups act properly on suitable symmetric spaces, S-arithmetic subgroups act properly on products of symmetric spaces and buildings (as the symmetric spaces for p-adic groups).