Lecture 1

Motivation: some basic problems.

1) Let $Q(x) = \sum_{i,j=1}^{d} a_{ij} x_i x_j$, $a_{ij} \in \mathbb{R}$, be a nondegenerate quadratic form.

For $g \in GL_d(\mathbb{R})$, $Q^g(x) = Q({}^t g \cdot x)$.

Q_1 and Q_2 are equivalent (over $\mathbb{R}$ / over $\mathbb{Z}$) if

$Q_1^g = Q_2$ for some ($g \in GL_d(\mathbb{R})$ / $g \in GL_d(\mathbb{Z})$).

Linear algebra $\Rightarrow$ Every quadratic form is equivalent over $\mathbb{R}$ to $x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_d^2$.

Problem: which quadratic forms are equivalent over $\mathbb{Z}$?

2) $Q(x)$ = a quadratic form with rational coefficients.

Problem: Describe the set $X(\mathbb{Z})$ of integral solutions of $Q(x) = n$.

$G = \{ g \in GL_d(\mathbb{C}) : Q^g = Q \} = O_Q(\mathbb{C})$

↑ orthogonal group

Answer: If Q is nondegenerate and $n \neq 0$, $X(\mathbb{Z})$ is union of finitely many orbits of $G(\mathbb{Z})$.

Algebraic & arithmetic groups

Def A subgroup $G < GL_d(\mathbb{C})$ is called *algebraic* if $G = \{g \in GL_d(\mathbb{C}) : P_1(g) = \dots = P_s(g) = 0\}$ where $P_1, \dots P_s \in \mathbb{C}[x_{ij} : i,j = \overline{1,d}]$.

It is *defined over* $\mathbb{Q}$ if P_i's can be choosen to have coefficients in $\mathbb{Q}$.

examples: $SL_d(\mathbb{C}) = \{g : \det(g) = 1\}$

$O(Q) = \{g : Qg = Q\}$, Q - quadratic form.

$Sp_{2d}(\mathbb{C}) = \{g : {}^t g \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} g = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\}$

Def $\Gamma_1, \Gamma_2 < G$ are *comensurable* if $\Gamma_1 \cap \Gamma_2$ has finite index in Γ_1 and Γ_2.

Def A subgroup $\Gamma < GL_d(\mathbb{C})$ is called *arithmetic* if Γ is comensurable with $G(\mathbb{Z})$ where G is an algebraic group defined over $\mathbb{Q}$.

Lemma. Let $\Gamma_1 < G_1$ and $\Gamma_2 < G_2$ be arithmetic subgroups of algebraic groups, defined over $\mathbb{Q}$, and $\varphi : G_1 \to G_2$ an isomorphism, defined over $\mathbb{Q}$. Then $\varphi(\Gamma_1)$ is comensurable with Γ_2.

Proof. We have $\varphi(g)_{ij} - \delta_{ij} = P_{ij}(g_{ij} - \delta_{ij})$, where P_{ij}'s are rational polynomials such that $P_{ij}(0, \dots 0) = 0$, since $\varphi(id) = id$

Let $m = [$ common denominator of coefficients of p_{ij}'s $]$

$\Gamma_1(m) = \{\gamma \in \Gamma_1 : \gamma = id \pmod m\}$

$\Gamma_1(m)$ a congruence subgroup of Γ_1.

Then $\varphi(\gamma)_{ij} - \delta_{ij} \in \mathbb{Z}$ for $\gamma \in \Gamma_1(m)$.

Hence, $\varphi(\Gamma_1(m)) \subset G_2(\mathbb{Z})$.

This implies that $\varphi(\Gamma_1(m)) \cap \Gamma_2 \underset{f.i.}{\leqslant} \varphi(\Gamma_1(m)) \underset{f.i.}{\leqslant} \varphi(\Gamma_1)$.

In particular, $\varphi(\Gamma_1) \cap \Gamma_2 \underset{f.i.}{\leqslant} \varphi(\Gamma_1)$.

Applying the same argument to φ^{-1}, we deduce that $\varphi^{-1}(\Gamma_2) \cap \Gamma_1$ has finite index in $\varphi^{-1}(\Gamma_2)$.

Then $\Gamma_2 \cap \varphi(\Gamma_1)$ has finite index in Γ_2. ∎

Preview of main results

1) Reduction theory (Borel – Harish-Chandra)

For a scalar product $\langle \cdot, \cdot \rangle$ on $\mathbb{C}^d$,

$$\langle g \cdot u, v \rangle = \langle u, g^* v \rangle.$$

Def. An algebraic group $G < GL_d(\mathbb{C})$ is called *reductive* if $G^* < G$ for a scalar product.

Thm. $G < GL_d(\mathbb{C})$ – reductive alg. group, defined over $\mathbb{Q}$

$X \subset \mathbb{C}^d$ – algebraic set, defined over $\mathbb{Q}$;

Assume that G acts transitively on X.

Then $X(\mathbb{Z})$ is a union of finitely many orbits of $G(\mathbb{Z})$

Def a *character* of alg. group $G \subset GL_d(\mathbb{C})$ is a polynomial homomorphism $\chi: G \to \mathbb{C}^\times$.

Thm. If G is an alg. group, defined over $\mathbb{Q}$, and $\exists$ characters $G \to \mathbb{C}^\times$ with infinite image, defined over $\mathbb{Q}$,

Then $\mathrm{vol}(G(\mathbb{R})/G(\mathbb{Z})) < \infty$.

examples: 1) $\mathrm{vol}(\mathbb{R}^d/\mathbb{Z}^d) < \infty$.

2) $\mathrm{vol}(SL_d(\mathbb{R})/SL_d(\mathbb{Z})) < \infty$.

3) Q = nondegenerate quad. form

$\mathrm{vol}(O_Q(\mathbb{R})/O_Q(\mathbb{Z})) < \infty$.

The group $O_Q(\mathbb{Z})$ is "large" — not obvious.

4) Dirichlet thm on units in number fields.

2) Structure of arithmetic groups.

Thm: Every arithmetic group is finitely generated, and defined by a finite number of relations.

Thm (Selberg lemma) Every arithmetic group has a torsion-free subgroup of finite index.

Thm (congruence subgroup property) $\Gamma = SL_d(\mathbb{Z})$, $d \geq 3$.
Then every finite index subgroup of Γ contains $\Gamma(m) = \{\gamma : \gamma = Id \pmod m\}$ for some m.

Thm (Margulis) $\Gamma = SL_d(\mathbb{Z})$, $d \geq 3$.
If $N \trianglelefteq \Gamma$, then N has finite index or finite.

Thm (Tits alternative) If $\Gamma < GL_d(\mathbb{C})$, then Γ contain a free group or a finite index soluble subgroup.

3) Rigidity properties

Thm (Margulis superRigidity ; special case)
$\Gamma = SL_d(\mathbb{Z})$, $d \geq 3$, $\varphi : \Gamma \to GL_N(\mathbb{C})$ - homomorphism

Then $\exists$ polynomial homomorphism $\widetilde{\varphi} : SL_d(\mathbb{C}) \to GL_N(\mathbb{C})$
and finite index subgroup $\Gamma' \leq \Gamma$ such that
$\varphi = \widetilde{\varphi}$ on Γ'.

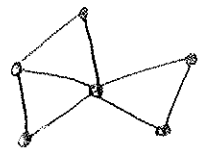
Def $\Gamma \leq G(\mathbb{R})$ is a lattice if Γ is discrete
and $\mathrm{vol}(G(\mathbb{R})/\Gamma) < \infty$.

examples: 1) $\mathbb{Z}^d \subset \mathbb{R}^d$
2) $SL_d(\mathbb{Z}) \subset SL_d(\mathbb{R})$.

Thm (Margulis arithmeticity)
Let Γ be a lattice in $SL_d(\mathbb{R})$, $d \geq 3$.
For simplicity, assume that $SL_d(\mathbb{R})/\Gamma$ is <u>not</u> compact.

Then $\exists$ an algebraic group G, defined over $\mathbb{Q}$,
polynomial map $\varphi : G(\mathbb{R}) \to SL_d(\mathbb{R})$
such that $\varphi(G(\mathbb{Z}))$ is commensurable with Γ.

4) Expander graphs



$\mathcal{G} = (V, E)$ - finite d-regular graph
(every vertex has d neighbours)

$A \subset V$, the boundary of A:
$\partial A = \{$ edges that connect E to $V \setminus E \}$.

Def. A family of d-regular graphs with
$\mathcal{G}_n = (V_n, E_n)$
$|V_n| \to \infty$ and d fixed is called
expander family if $\exists c > 0$:
$\forall A \subset V_n$, $|A| \leq \frac{1}{2}|V_n|$: $|\partial A| \geq c|A|$.

---

application: efficient communication networks.

Construction (Margulis)

$\mathcal{G}_n = \Gamma / \Gamma(n)$, $\Gamma = SL_N(\mathbb{Z})$, $N \geq 3$,
is an expander family.