Geometry of Nilpotent and Solvable Groups

Cornelia Druţu

Lecture 8: End of proof of Tits' Theorem. Gromov's Theorem

Case 2. Let $\Gamma \leq SL(n, \mathbb{C})$ be relatively compact.

Let S be a finite generating set of Γ, $S = S^{-1}$, $1 \not\in S$.

In what follows we denote $SL(n, \mathbb{C})$ by G.

N.B. Do not confuse with the notation in the previous lectures, where G denoted the Zariski closure of Γ in $SL(n, \mathbb{K})$.

Let $\mathbb{F}$ be the subfield of $\mathbb{C}$ generated by the entries of the matrices s with $s \in S$.

Step 1. We prove that we may reduce to the case when $\mathbb{F}$ is a finite algebraic extension of $\mathbb{Q}$.

To that end consider the set of all homomorphisms $Hom(\Gamma, G)$.

Let $S = \{s_1, s_2, ..., s_k\}$. Consider a presentation of Γ, $\Gamma = \langle S \mid R \rangle$, with R possibly infinite. Recall that all relations $r \in R$ are words in the alphabet S, and that Γ is entirely determined by the relations $r = 1$, $\forall r \in R$.

Every homomorphism $\varphi : \Gamma \to G$ is completely determined by the images $M_i = \varphi(s_i)$.

Conversely, every set of matrices $M_1, ..., M_k$ satisfying all the relations $r(M_1, ..., M_k) = \mathrm{Id}_n$ for all $r \in R$, determine a homomorphism $\varphi : \Gamma \to G$.

Thus we may identify $Hom(\Gamma, G)$ with the following subset of G^k :

$$Z = \left\{ (M_1, ..., M_k) \in G^k \; ; \; r(M_1, ..., M_k) = \mathrm{Id}_n \, , \, \forall r \in R \right\} .$$

Note that Z is a Zariski closed subset in G^k. Moreover all the polynomials defining Z have rational coefficients in the entries of $M_1, ..., M_k$, since $r(M_1, ..., M_k)$ are all products of matrices in $\{M_1, ..., M_k\}$.

Reassuring (but useless in our context) remark: since $\mathbb{Q}[X_1, ..., X_n]$ is a noetherian algebra, finitely many polynomial equations will suffice to define Z, even though R might have been infinite.

Number Theory Lemma: Let Z be a Zariski closed set in $\mathbb{C}^m$ defined by polynomial equations with rational coefficients. The set $Z \cap \overline{\mathbb{Q}}^m$ is dense in Z with respect to the usual topology on $\mathbb{C}^m$.

Here $\overline{\mathbb{Q}}$ denotes the field of all the numbers algebraic over $\mathbb{Q}$.

Corollary 1. *In $Hom(\Gamma, G)$, $G = SL(n, \mathbb{C})$, the following set is dense:*

$$\{\rho : \Gamma \to G \text{ homomorphism } \mid \rho(s) \text{ have algebraic entries for all } s \in S\} .$$

In particular consider the inclusion representation $\rho : \Gamma \to G$.

By the above there exists a sequence of homomorphisms $\rho_i : \Gamma \to G$ such that for every $s \in S$, $\rho_i(s)$ has all entries algebraic numbers, ρ_i converging to ρ in the compact-open topology.

It is enough to prove Tits' Theorem for all $\rho_i(\Gamma)$:

- if some $\rho_i(\Gamma)$ contains a copy of F_2, the free group on two generators, then Γ itself contains a copy of F_2 ($\rho_i(\Gamma)$ is a quotient of Γ);
- if all $\rho_i(\Gamma)$ are virtually solvable then $\rho(\Gamma) = \Gamma$ is virtually solvable.

The second statement can be deduced from the following.

Theorem 2. *If $\Lambda \leq GL(n, \mathbb{C})$ is virtually solvable then there exists Λ_1 subgroup of index at most $I(n)$ in Λ such that Λ_1 is a solvable group of derived length at most $D(n)$.*

Step 2. Now we reduced the proof to the case of $\Gamma \leq GL(n, \mathbb{C})$, Γ relatively compact, all entries of matrices in Γ contained in some field $\mathbb{F}$, finite algebraic extension of $\mathbb{Q}$.

Goal: By a Number Theory trick we want to reduce this case to Case 1, when Γ was unbounded.

We consider norms on $\mathbb{F}$.

Non-archimedean norms: these are norms $\nu : \mathbb{F} \to \mathbb{R}_+$ s.t. instead of the triangle inequality $\nu(a+b) \leq \nu(a) + \nu(b)$ the following stronger inequality is satisfied:

$$\nu(a+b) \leq \max(\nu(a), \nu(b)).$$

Example: Let $\mathbb{F} = \mathbb{Q}$, fix a prime number p.

Every $x \in \mathbb{Q}$ can be written as $x = p^k \frac{m}{n}$, where $k \in \mathbb{Z}$ and p does not divide either m or n. Define

$$\nu(x) = p^{-k} .$$

This norm is called a p-adic norm on $\mathbb{Q}$, and it is non-archimedean.

For every norm ν on $\mathbb{F}$ consider the completion of $\mathbb{F}$ with respect to ν, denoted $\mathbb{F}_\nu$.

Define also the ring of integers $O_\nu = \{x \in \mathbb{F}_\nu \mid \nu(x) \leq 1\}$.

In the example above the completion $\mathbb{Q}_\nu$ is the field of p-adic numbers.

Archimedean norms: Every $\sigma \in \text{Galois}(\mathbb{F}/\mathbb{Q})$ defines an embedding

$$\sigma : \mathbb{F} \to \mathbb{C} , x \mapsto \sigma(x) .$$

The pull-back of the norm on $\mathbb{C}$ via σ is an archimedean norm on $\mathbb{F}$.

In this case $\mathbb{F}_\nu$ is $\mathbb{R}$ or $\mathbb{C}$.

Consider $N(\mathbb{F})$ = set of norms ν on $\mathbb{F}$ such that $\nu|_{\mathbb{Q}}$ is the standard absolute value or a p-adic norm.

Example: $\mathbb{F} = \mathbb{Q}$. Then $N(\mathbb{Q})$ = the set composed of the absolute value and all the p-adic norms.

Note that for all $x \in \mathbb{Q}$, $x \in O_\nu$ with finitely many exceptions, equivalently $\nu(x) > 1$ only for finitely many $\nu \in N(\mathbb{Q})$ (possibly the absolute value, and all ν_p for p prime dividing the denominator).

The same is true in general:

Proposition 3. *Let $\mathbb{F}$ be a finite algebraic extension of $\mathbb{Q}$. For every $x \in \mathbb{F}$, $\nu(x) > 1$ only for finitely many $\nu \in N(\mathbb{F})$.*

Definition 4. The ring of *adeles* corresponding to $\mathbb{F}$ is the *restricted product*

$$\mathbb{A}(\mathbb{F}) \leq \prod_{\nu \in N(\mathbb{F})} \mathbb{F}_\nu,$$

i.e. the subset of the direct product which consists of points whose projection to F_ν belongs to O_ν for all but finitely many ν's.

Theorem 5. *The image of the diagonal embedding $\mathbb{F} \hookrightarrow \mathbb{A}(\mathbb{F})$, $f \mapsto (f)_{\nu \in N(\mathbb{F})}$, is a discrete subset in $\mathbb{A}(\mathbb{F})$ endowed with the product topology.*

See the book of S. Lang "Algebraic Numbers", Chapter 6, Theorem 1.

We had Γ subgroup in $SL(n, \mathbb{F})$, where $\mathbb{F}$ is a finite algebraic extension of $\mathbb{Q}$. The diagonal embedding above defines an embedding

$$\Gamma \hookrightarrow \prod_{\nu \in N(\mathbb{F})} SL(n, \mathbb{F}_\nu)$$

with discrete image.

If for every ν the image of Γ in $SL(n, \mathbb{F}_\nu)$ is relatively compact then (by Tychonoff Theorem) Γ is relatively compact in $\prod_{\nu \in N(\mathbb{F})} SL(n, \mathbb{F}_\nu)$. But since it is also discrete, it must be finite. This yields a contradiction, when Γ is infinite.

Thus, if Γ is infinite then there exists $\nu \in N(\mathbb{F})$ such that the embedding $\Gamma \hookrightarrow SL(n, \mathbb{F}_\nu)$ is unbounded. Thus we are back to Case 1. The proof in this case works, with very few modifications, when replacing $\mathbb{R}$ or $\mathbb{C}$ by an arbitrary complete field with a norm.

The proof of Tits' Alernative Theorem is now complete. $\square$

Theorem 6 (Gromov's Theorem)**.** *If Γ finitely generated has polynomial growth then Γ is virtually nilpotent.*

If we could reduce to the case when $\Gamma \leq GL(n, \mathbb{C})$ then we could use Tits' Alernative Theorem.

This can be done by using the following consequence of the Montgomery-Zippin Theorem.

Theorem 7 (Montgomery-Zippin). *Input: a metric space.*

Let X be a metric space that is

- *complete;*
- *connected, locally connected;*
- *proper (i.e. all balls are compact);*
- *of finite Hausdorff dimension.*

Output: an 'almost linear' group.

If $H = Isom(X) = \{f : X \to X \mid f \text{ bijection}, d(f(x), f(y)) = d(x,y)\}$ acts transitively on X then H has finitely many connected components, and for the connected component H_0 containing the identity element there exists a homomorphism $\varphi : H_0 \to GL(n, \mathbb{C})$ with $\ker \varphi \le Z(H_0)$.

If the group Γ would appear as subgroup of $H = Isom(X)$ as above then we would be done because:

- we would replace Γ by $\Gamma \cap H_0$ subgroup of finite index;
- $\varphi(\Gamma) \le GL(n, \mathbb{C})$ has polynomial growth (as quotient of Γ) $\Rightarrow$ (by Tits' Theorem) $\varphi(\Gamma)$ is solvable $\Rightarrow$ (by Milnor-Wolf Theorem) $\varphi(\Gamma)$ is virtually nilpotent.

  Thus we have the short exact sequence

$$1 \to K \to \Gamma \to \varphi(\Gamma) = N \to 1\,,$$

  where $K \le Z(\Gamma)$ and N is virtually nilpotent.

  Replace Γ by a finite index subgroup so that N becomes nilpotent.

  In Lecture 5, page 5 we proved:

  Lemma 8. *If G is finitely generated and of sub-exponential growth and there exists a short exact sequence*

$$1 \to A \to G \to H \to 1\,,$$

  with A abelian and H polycyclic, then A is finitely generated, equivalently G is polycyclic.

  In our case this gives Γ polycyclic, hence virtually nilpotent, by Wolf's Theorem.

What is the space X ?

What about a Cayley graph $\mathcal{G} = Cayley(\Gamma, S)$?

All the hypotheses of Theorem 7 are satisfied except the one requiring a transitive action of $\mathrm{Isom}(X)$ on X. Of course, the group itself Γ acts transitively on the set of vertices. But if we take only the set of vertices we loose the connectedness.

Gromov's idea was to rescale a Cayley graph, i.e to consider $\mathcal{G}$ with the metric $\frac{1}{n}\mathrm{d}$. The set of vertices becomes 'more and more dense', hence the action of Γ becomes 'closer and closer to a transitive action'. Thus, when considering a limit of $\left(\mathcal{G}\,,\,\frac{1}{n}\mathrm{d}\right)$ as $n \to \infty$ we might obtain a metric space and an action as in Theorem 7.

For instance when $\Gamma = \mathbb{Z}^2$ and $\mathcal{G}$ is the Cayley graph with respect to the generators $\{(\pm 1, 0), (0, \pm 1)\}$, $\left(\mathcal{G}\,,\,\frac{1}{n}\mathrm{d}\right)$ is the planar grid with edges of length $\frac{1}{n}$, and the limit should be $\mathbb{R}^2$, which obviously satisfies the hypotheses of Theorem 7.

For every group Γ, we consider $\mathcal{G} = Cayley(\Gamma, S)$ and we construct a limit of $\left(\mathcal{G}\,,\,\frac{1}{n}\mathrm{d}\right)$.

Construction of the limit space

We need the following device to construct the limit space.

An ultrafilter on a set I is a finitely additive measure ω defined on $\mathcal{P}(I)$ (the power set of I), taking only values zero and one and such that $\omega(I) = 1$.

Example: Let x be a point in I. Then we can define $\delta_x(A)$ to be 1 if $x \in A$ and 0 if $x \notin A$. It is easy to see that δ_x is an ultrafilter.
Such an ultrafilter is called principal.

Lemma 9. *An ultrafilter ω is non-principal iff $\omega(F) = 0$ for every finite subset F of I.*

The proof is easy to see if we reformulate: ω is principal iff there exists a finite set F such that $\omega(F) = 1$.

Fix an ultrafiter ω on $\mathbb{N}$ (all ultrafilters that we consider from now on are on $\mathbb{N}$).

Definition 10. Given a sequence (x_n) in a topological space, its ω-limit is a point $x \in X$ such that for every open set U containing x,

$$\omega\left(\{n \in \mathbb{N} \mid x_n \in U\}\right) = 1\,.$$

If ω is principal, i.e. $\omega = \delta_{n_0}$, for some $n_0 \in \mathbb{N}$, the ω-limit of every sequence (x_n) is the element x_{n_0}.

Lemma 11. *If a sequence (x_n) is contained in K compact and Hausdorff separated, and ω is an ultrafilter, then (x_n) has a unique ω-limit in K.*

Proof. Uniqueness of the limit follows easily from the Hausdorff property. We prove existence.

Assume that no point in K is ω-limit of (x_n). Then every $z \in K$ is contained in an open set U_z such that

$$\omega\left(\{n \in \mathbb{N} \mid x_n \in U_z\}\right) = 0\,.$$

$K \subseteq \bigcup_{z\in K} U_z$ and K compact, hence there exist $z_1, ..., z_m$ in K such that

$$K \subseteq U_{z_1} \cup U_{z_2} \cup \cdots \cup U_{z_m}\,.$$

$(x_n) \subseteq K \Rightarrow \mathbb{N} = I_1 \cup I_2 \cup \cdots \cup I_m$, where

$$I_j = \{n \in \mathbb{N} \mid x_n \in U_{z_j}\}\,.$$

$\omega(I_j) = 0$ for all j implies $\omega(\mathbb{N}) = 0$, contradiction. □

Exercise. When ω is a non-principal ultrafilter, the ω-limit of a sequence (x_n) contained in a compact is the actual limit of a subsequence.