POLYCYCLIC GROUPS : LOCAL AND GLOBAL ORBITS OF ALGEBRAIC GROUPS

MARQUES SOPHIE

In the following, we consider a $\mathbb{Q}$-group $\mathcal{G}$ such that the polynomial equations defining $\mathcal{G}$ as a subset of $GL_m(\mathbb{C})$ all have integer coefficients and a $\mathbb{Q}$-rational representation $\rho : \mathcal{G} \to GL_m(\mathbb{C})$ such that the rational expressions which define this map are polynomials with integer coefficients.

For a positive integer $r$, $\mathcal{G}(\mathbb{Z}/r\mathbb{Z})$ will denote the set of all matrices in $GL_n(\mathbb{Z}/r\mathbb{Z})$ whose entries satisfy this equations over $\mathbb{Z}/r\mathbb{Z}$ and $\bar{\rho} : \mathcal{G}(\mathbb{Z}/r\mathbb{Z}) \to M_m(\mathbb{Z}/r\mathbb{Z})$ the reduction of $\rho$ mod $r$.

1. LOCAL ORBIT OF $\mathcal{G}$ IN $\mathbb{Q}^n$

1.1. First main theorem. The $\mathbb{Q}$-rational representation $\rho$ define an action of $\mathcal{G}$ on the vector space $\mathbb{C}^n$, in particular, an action of $\mathcal{G}(\mathbb{Z})$ on $\mathbb{Q}^n$.

Definition (Proposition) 1.1. Let $a$ and $b$ in $\mathbb{Q}^n$. We say that $a$, $b$ are in the same local orbit of $\mathcal{G}$ if one of this two equivalent conditions are satisfied:

1. for all $r$ positive integer, there exists a matrix $g_r \in \mathcal{G}(\mathbb{Z}/r\mathbb{Z})$ such that $a\bar{\rho}(g_r) = b$ where $a = a$ mod $r$.
2. for every prime $p$, there exists $g_p \in \mathcal{G}(\mathbb{Z}/p\mathbb{Z})$ such that $\rho(g_p) = b$.

The goal is first to prove the following main theorem:

Theorem 1.2. Every local orbit of $\mathcal{G}$ in $\mathbb{Q}^n$ is the union of finitely many orbits of $\mathcal{G}(\mathbb{Z})$.

1.2. Sketch of proof of the first main theorem. Let $c$ be the local orbit of $\mathcal{G}(\mathbb{Q})$ in $\mathbb{Q}^n$, $c \in C$ and denote $\mathcal{H}$ the stabilizer of $c$ in $\mathcal{G}$.

First, we can establish the following proposition (next section).

Proposition 1.3. Every local $\mathcal{G}$-orbit in $\mathbb{Q}^n$ is contained in the union of finitely many orbits of $\mathcal{G}(\mathbb{Q})$.

Denote $\mathcal{G}^\infty := \prod_p \mathcal{G}(\mathbb{Z}_p)$. In view of this proposition, to prove the main theorem, it remains to show the following lemma:

Lemma 1.4. If for each $b$ and $c$ in $C$, there exists $g \in \mathcal{G}(\mathbb{Q})$ and $\hat{g} \in \mathcal{G}^\infty$ such that $b\rho(g) = c = b\rho(\hat{g})$ (resp. $\mathcal{G}$ meets only finitely many orbits of $\mathcal{G}(\mathbb{Z})$).

Proof. Denote $\mathcal{G}(\mathbb{A}_f) := \{\hat{g} = (g_p) \in \prod_p \mathcal{G}(\mathbb{Q}_p) | g_p \in \mathcal{G}(\mathbb{Z}_p), \text{ for almost all prime } p\}$ the adele group of $\mathcal{G}$ and $\mathcal{D} := \mathcal{H}(\mathbb{Q})\backslash \mathcal{H}(\mathbb{A}_f)/\mathcal{H}^\infty$ the double coset.

We can consider the intersection $\mathcal{G}^\infty \cap \mathcal{G}(\mathbb{Q})$ in $\mathcal{G}(\mathbb{A}_f)$ and check that $\mathcal{G}^\infty \cap \mathcal{G}(\mathbb{Q}) = \mathcal{G}(\mathbb{Z})$.

We will define a map : $\psi : C \to \mathcal{D}$. For each $b \in C$, let $g_b \in \mathcal{G}(\mathbb{Q})$ and $\hat{g}_b \in \mathcal{G}^\infty$ as in (resp. $\mathcal{G}$) and put $\hat{h}_b := g_b^{-1}\hat{g}_b \in \mathcal{G}(\mathbb{A}_f)$, one can prove that $\hat{h}_b \in \mathcal{H}(\mathbb{A}_f)$ and that the map $\psi : C \to \mathcal{D}$

$b \mapsto \mathcal{H}(\mathbb{Q})\hat{h}_b \cdot \mathcal{H}^\infty$

is well defined (resp. $\mathcal{H}(\mathbb{Q})\hat{h}_b \cdot \mathcal{H}^\infty$ doesn’t depend in the choices of $g_b$ and $\hat{g}_b$).

Then, in view of this observations, one can prove the following lemma:

Lemma 1.5. The fibers of $\psi$ are exactly the orbits of $\mathcal{G}(\mathbb{Z})$ in $C$. 
Finally, the main theorem is a direct consequence of this theorem of Borel

**Theorem 1.6** (Conséquence du théorème 7.1, Borel and Serre (1964)). For every $\mathcal{Q}$-group $\mathcal{H}$, the set $\mathcal{H}(\mathcal{Q})/\mathcal{H}(\mathcal{A}_f)/\mathcal{H}^\infty$ is finite.

1.3. **Sketch of proof of the proposition 1.3.** Let $\mathcal{C}$ be the local orbit of $\mathcal{G}(\mathcal{Q})$ in $\mathcal{Q}^m$, $c \in \mathcal{C}$ and denote $\mathcal{H}$ the stabilizer of $c$ in $\mathcal{G}$.

1. For $k$ a field, $\bar{k}$ a algebraic closure of $k$, $\Gamma_k := \text{Gal}(\bar{k}/k)$, denote $Z^1(k, \mathcal{H}) := Z^1(\Gamma_k, \mathcal{H}(\bar{Q}))$ the set of the 1-cocycles, denote $\sim$ the usual equivalence relation on $Z^1(k, \mathcal{H})$, $H^1(k, \mathcal{H}) := Z^1(k, \mathcal{H})/\sim$ the first cohomology group. Choose $\bar{Q}_p$ containing $\bar{Q}$, pour tout premier $p$, so that $\mathcal{H}(\bar{Q}) \leq \mathcal{H}(\bar{Q}_p)$ and consider the restriction map $r_p : \Gamma_{Q_p} \rightarrow \Gamma_Q$. We can check that the map

$$w : H^1(Q, \mathcal{H}) \rightarrow \prod_p H^1(Q_p, \mathcal{H})$$

which associate to $[\sigma]$ the class of one element $\sigma$ of $Z^1(Q, \mathcal{H})$, the product over the prime $p$ of the class $[\sigma_p]$ of $\sigma_p := \sigma \circ r_p$ element of $Z^1(Q_p, \mathcal{H})$ is well defined. And the important result for our purpose is the following theorem due to Borel and Serre :

**Theorem 1.7** (Théorème 7.1, Borel and Serre (1964)). The map $w$ has finite fibers.

2. We will define a map $\theta : C \rightarrow H^1(Q, \mathcal{H})$. For this, first, one can establish the following proposition which is a consequence of the Hilbert’s Nullstellansatz :

**Proposition 1.8.** If $a, b \in Q^m$ lie in the same orbit $\mathcal{G}(Q_p)$, for some prime $p$, then they lie in the same orbit of $\mathcal{G}(\bar{Q})$.

As a result, for each $a \in C$, we have an element $g_a \in \mathcal{G}(Q)$ with $ap(g_a) = c$. Then, one can prove that the map $\Delta_a : \Gamma_Q \rightarrow \mathcal{H}(\bar{Q})$ which sends $a$ over $g_a^{-1}g_a$ well defined belongs to $Z^1(Q, \mathcal{H})$ and doesn’t depend on the choice of $g_a \in \mathcal{G}(Q)$. So, this define a map $\theta : C \rightarrow H^1(Q, \mathcal{H})$ mapping $a$ over $[\Delta_a]$ the class of $\Delta_a$ in $H^1(Q, \mathcal{H})$. Finally, one can prove without too much difficulties the following lemma :

**Lemma 1.9.** The fibers of $\theta$ are exactly the orbits of $\mathcal{G}(Q)$ in $C$.

3. By (1) and (2), the proposition follows. In fact, one can prove that $w(\theta(C)) \subset \prod_p H^1(Q_p, \mathcal{H})$ is reduced to one element the fibre of this element $\theta(C)$ is finite by (1) and the theorem is proved by (2).

2. **Second main theorem**

Let $a$ a ring of integer.

**Theorem 2.1.** Every orbit of $\mathcal{G}(a)$ meets only finitely many orbits of $\mathcal{G}(Z)$ in $Z^m$.

Since when we increase the ring $a$, $\mathcal{G}(a)$ only gets bigger, we can suppose from now that $k$ is normal in $Q$. Denote $\Gamma := \text{Gal}(k/Q)$, this group acts on $\mathcal{G}(a)$ and since $a \cup Q = Z$, the group of the invariant by this action is $\mathcal{G}(Z)$. For $c \in Z$, let $C := c\mathcal{P}(\mathcal{G}(a)) \cup Z^m$ and $\mathcal{H}$ be the stabilizer of $c$ in $\mathcal{G}.

Following the proof of the first theorem, one can define a map

$$\theta : C \rightarrow H^1(\Gamma, \mathcal{H}(a))$$

$$a \mapsto [\Delta_a]$$

such that its fibers are exactly the orbits of $\mathcal{G}(Z)$ in $C$. The theorem that we want to prove is then the consequence of the following result due to Borel and Serre.
Theorem 2.2. Let \( H \) be a \( \mathbb{Q} \)-group, \( k \) a finite normal extension field of \( \mathbb{Q} \) with ring of integers \( a \) and \( \Gamma = \text{Gal}(k|\mathbb{Q}) \) then \( H^1(\Gamma, H(a)) \) is finite.

Sketch of proof. In order to obtain this theorem, we need the following two lemma proved in Segal’s book. The first lemma gives a description of the cohomology group as a semi-direct product:

**Lemma 2.3.** Let \( H \) be a group, \( \Gamma \) a finite group acting on \( H \). Then there is a 1:1 correspondence between the set of the conjugacy classes of the complements to \( H \) in \( H \rtimes \Gamma \) and the set \( H^1(\Gamma, H) \).

The second lemma gives a condition sufficient such that the set of the conjugacy class describe in the previous lemma is finite:

**Lemma 2.4.** Let \( H \) be a group, \( \Gamma \) a finite group acting on \( H \). If \( H \rtimes \Gamma \) is isomorphic to an arithmetic group then there the set of the conjugacy classes of the complements to \( H \) in \( H \rtimes \Gamma \) is finite.

Finally, to prove the theorem it remains to prove the \( H(a) \rtimes \Gamma \) is isomorphic to an arithmetic group. For this, one can give a description of this group as a semi-direct product of matrix group over \( \mathbb{Z} \) denoted by \( H^+ \rtimes \Gamma^* \) using a \( \mathbb{Z} \) basis \( (u_1, ..., u_d) \) of \( a \) which permit to construct an embedding of \( \text{GL}_n(a) \) (resp. \( \text{GL}_n(k) \)) into \( \text{GL}_n(\mathbb{Z}) \) (resp. \( \text{GL}_n(\mathbb{Q}) \)). And then this semi-direct product is a arithmetic group by the following lemma:

**Lemma 2.5.** Let \( H \) be a subgroup of \( \text{GL}_n(\mathbb{Z}) \). \( H \) is a arithmetic group (in some \( \mathbb{Q} \)-group of degree \( n \)) if and only if \( H \) has finite index in its own closure in \( \text{GL}_n(\mathbb{Z}) \).

Indeed, since \( \Gamma^* \) is finite, it suffices to prove that \( H(a)^* \) is closed in \( \text{GL}_n(\mathbb{Z}) \) which is true since it can be describe as the zero set of polynomials which take value in \( \text{GL}_n(\mathbb{Q}) \).

3. References
