A Strong Tits Alternative

Andrii Dmytryshyn

Erasmus Mundus Master ALGANT

University of Bordeaux 1 and University of Padua

Supervisor

Professor Yuri Bilu

2011

Acknowledgements

First of all I would like to thank to my thesis advisor Prof. Yuri Bilu for his meaningful explanations and discussions which uncovered beauty of mathematics to me, for sincere communication that encouraged me a lot, for answers on my questions, and useful remarks. It was a real pleasure to work with Prof. Bilu!

I am very thankful to Prof. Vladimir V. Sergeichuk for his enormous impact in my mathematical education and in my life in general. His suggestions and critique always help me and he teaches me a lot.

I owe my deepest gratitude to my family and friends for their permanent support and love.

A special thank to my ALGANT friends: Aglaia, Andy, Farhad, Francesco, Jyoti, Liu, Long, Mark, Martin, Massimo, Nikola, Novi, Olga, Oleksii, Rene, Tuhin, Velibor ... for a common work and shared time.

This thesis would not have been possible without a financial support of European Commission and perfectly organized ALGANT program by the consortium of universities. It is also gratefully acknowledged.

Thank you!

Contents

Chapter 1

Introduction

Tits's alternative is one of the most powerful results describing the structure of finitely generated linear groups. It tells that a linear group either has a non-abelian free subgroup or is virtually solvable (see Section 2.2 for more details). However in case of not virtually solvable group Classical Tits's alternative does not tell us where to search for generators of a free group and tells just about an existence in the group.

By $GL_d(K)$ we denote a general linear group, i.e. the group of $d \times d$ nonsingular matrices over a field K and let F be a subset of $GL_d(K)$ such that $1 \in F$. E. Breuillard found the constant N that depends only on d and but neither on the field K nor on the the set F such that the generators are precisely products of N elements from F. This thesis is devoted to study the result for $SL_2(K)$ and related results that are presented mainly in Breuillard [2011], see also Breuillard [2008b], Breuillard [2008a]. Let us state the main result in general precisely.

Theorem 1.0.1 (strong uniform Tits Alternative)**.** *For every $d \in \mathbb{N}$ there is $N = N(d) \in \mathbb{N}$ such that if K is any field and F a finite symmetric subset of $GL_d(K)$ containing 1 then either F^N contains two elements which generate a nonabelian free group, or the group generated by F is virtually solvable (i.e. contains a finite index solvable subgroup).*

The proof of this theorem allows us, in principle, to find the constant N. Due to Grigorchuk and de la Harpe's examples Grigorchuk and de la Harpe [2001] $N = N(d)$ tends to infinity with d.

The proof of Theorem 1.0.1 is divided into an arithmetic and a geometric steps. After a careful check that all estimates are indeed uniform over all local fields the geometric step is based on a "ping-pong method".

The arithmetic step in Theorem 1.0.1 relies on the following result which is interesting by itself too. This result can be seen as a non abelian version of the well-known Lehmer conjecture (unsolved problem in mathematics attributed to Lehmer (1933)) from number theory. Some preliminary definitions that might be needed are available in the Section 2.4.

Theorem 1.0.2 (Height Gap Theorem)**.** *There is a positive constant $\varepsilon = \varepsilon(d) > 0$ such that if F is a finite subset of $GL_d(\overline{\mathbb{Q}})$ generating a non virtually solvable subgroup Γ then $\widehat{h}(F) > \varepsilon$.*

Chapter 2

Preliminary Information

In this chapter we recall the results from different branches of mathematics. Some of them are classical (”ping-pong lemma”, Tits alternative, and Lehmer conjecture) and the other are very recent (escape from subvarieties). All these results we will use in the next chapters.

2.1 Group Theory

Let us recall some definitions.

Definition 2.1.1. *Let G be a group with a subgroup H, and let*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = H$$

be a series of subgroups with each G_i a normal subgroup of G_{i-1}. Such a series is called a **subnormal series***.*

If in addition, each G_i is a normal subgroup of G, then the series is called a **normal series***.*

Definition 2.1.2. *A group G is* solvable *if it has a subnormal series*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

where all the quotient groups G_i/G_{i+1} are abelian.

Definition 2.1.3. *A group G is called* **virtually solvable** *if it has a solvable subgroup of finite index.*

Remark 2.1.4. *The adverb "virtually" is used not only in this case: for example, there are also virtually abelian, virtually nilpotent groups etc. In general for a given property P, the group G is said to be virtually P if there is a finite index subgroup $H \leq G$ such that H has property P. A group G is P by-finite if it has a normal subgroup of finite index with the property P.*

If property P is inherited by subgroups of finite index, being virtually P is equivalent to being P-by-finite (see Baumslag et al. [2009], p.5, Lemma 6).

Let G be a finitely generated group with generating set S (closed under inverses). For $g = a_1 a_2 \dots a_m \in G$, $a_i \in S$, let $l(g, S)$ be the minimum value of m. Define

$$\gamma(n, S) = \mid \{g \in G : l(g, S) \leq n\} \mid .$$

The function γ is called the **growth function** for G with generating set S. If γ is either

(a) bounded above by a polynomial function,

(b) bounded below by an exponential function, or

(c) neither,

then this condition is preserved under changing the generating set for G. Respectively, then, G is said to have

(a) **polynomial growth**,

(b) **exponential growth**, or

(c) **intermediate growth**.

For a survey on the topic, see Grigorchuk [1991].

Groups with exponential growth will be important for us (see Remark 2.1.7) thus we give the definitions precisely.

Definition 2.1.5. *A group G with finite generating set S has exponential growth if*

$$h(G, S) = \liminf_{n \to \infty} \frac{1}{n} \log(|\gamma(n, S)|) > 0.$$

Definition 2.1.6. *G has uniform exponential growth if*

$$h(G) = \inf\{h(G, S) : S \text{ finite set of generators for } G\} > 0.$$

Remark 2.1.7. *Finitely generated subgroups of $GL_n(K)$ which are not virtually solvable have uniform exponential growth (see Eskin et al. [2005]).*

Lemma 2.1.8 (Ping-pong Lemma for subgroups)**.** *Let G be a group acting on a set Ω and let A and B be two subgroups. Suppose that there exist nonempty sets $S_1, S_2 \subset \Omega$ such that*

1. *$S_1 \cap S_2 = \emptyset$;*
2. *$S_2 a \subset S_1$ and $S_1 b \subset S_2$ for all nontrivial $a \in A$ and $b \in B$;*
3. *for all $a \in A$, $S_1 a \cap S_1 \neq \emptyset$.*

Then the subgroup $< A, B >$ generated by A and B is the free product $A * B$.

Proof. It is enough to show that no product $g = a_1 b_1 \cdot \ldots \cdot a_k b_k$ (with $k \geq 1$ and nontrivial $a_i \in A$ and $b_i \in B$) is equal to 1. Indeed, by 3. there exists $\delta \in S_1$ such that $\delta a_1 \in S_1$. Then 2. shows that $\delta g \in S_2$ and so 1. proves that $g \neq 1$. □

The name "ping-pong lemma" is motivated by the fact that, in the above argument, the point $\delta a_1 b_1 \ldots a_k b_k$ bounces like a ping-pong between the sets S_1 and S_2.

We will use another variant of this lemma which is given below.

Lemma 2.1.9 (Ping-pong Lemma)**.** *Let G be a group acting on a set X. Let $a_1, \ldots, a_k$ be elements of G, where $k \geq 2$. Suppose there exist pairwise disjoint nonempty subsets $X_1^+, \ldots, X_k^+$ and $X_1^-, \ldots, X_k^-$ of X with the following properties:*

$$(X_i^-)^c a_i \subseteq X_i^+ \text{ for } i = 1, \ldots, k,$$

$$(X_i^+)^c a_i^{-1} \subseteq X_i^- \text{ for } i = 1, \ldots, k,$$

where by $(Y)^c$ we denote the completion of $Y \subset X$ to X. Then the subgroup $H =< a_1, \ldots, a_k > \leq G$ generated by $a_1, \ldots, a_k$ is free with free basis $\{a_1, \ldots, a_k\}$.

Proof. The proof of this lemma is analogous to the proof of Ping-pong Lemma for subgroups above.

To simplify the argument, we will prove the statement under the following assumption:

$$X \neq \bigcup_{i=1}^{k} (X_i^+ \cup X_i^-). \tag{2.1}$$

Choose a point x in X such that

$$x \notin \bigcup_{i=1}^{k}(X_i^+ \cup X_i^-).$$

To show that H is free with free basis $a_1, \ldots, a_k$ it suffices to prove that every nontrivial freely reduced word in the alphabet $A = a_1, \ldots, a_k, a_1^{-1}, \ldots, a_k^{-1}$ represents a nontrivial element of G.

Let w be such a freely reduced word, that is, $w = b_n b_{n-1} \ldots b_1$, where $n \geq 1$, where each b_j belongs to A and where w does not contain subwords of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$. Induction on j shows that for every $j = 1, \ldots, n$ we have

$$b_j b_{j-1} \ldots b_1 x \in \bigcup_{i=1}^{k}(X_i^+ \cup X_i^-).$$

Thus

$$wx \in \bigcup_{i=1}^{k}(X_i^+ \cup X_i^-).$$

Therefore $wx \neq x$ and hence $w \neq 1$ in G, as required.

The argument for the general case is similar to the one given below but requires more careful analysis. Without the assumption (2.1) we may choose x from some set such that wx is in the same set but we can always find another element on which w acts nontrivially. □

2.2 Tits Alternative: Classical Variant

The Tits alternative, named for Jacques Tits, is an important theorem about the structure of finitely generated linear groups. Originally it was stated by Tits in the form below in Tits [1972].

Theorem 2.2.1 (Tits Tits [1972]). *Over a field of characteristic* 0*, a linear group either has a non-abelian free subgroup or possesses a solvable subgroup of finite index.*

Every finite group of order less than 60, every abelian group, and every subgroup of a solvable group are solvable. There is a table of solvable groups of order up to 242 (Betten 1996, Besche and Eick 1999).

The condition that a group is a subgroup of GL_n is essential. There are many famous groups that do not satisfy the Tits alternative:

Thompson's group F. A finite presentation of F is given by the following expression:

$$\langle A, B | [AB^{-1}, A^{-1}BA] = [AB^{-1}, A^{-2}BA^2] = \mathrm{id} \rangle$$

where $[x, y] = xyx^{-1}y^{-1}$ is the usual group theory commutator. Alternatively F has the infinite presentation:

$$\langle x_0, x_1, x_2 \ldots | x_k^{-1} x_n x_k = x_{n+1} \quad for \quad k < n \rangle.$$

Burnside's group $B(m, n)$ for $n \geq 665$, odd. It is a free group of rank m and exponent n.

Grigorchuk group. It is a finitely generated infinite group constructed by Rostislav Grigorchuk that provided the first example of such a group of intermediate growth.

This means that these groups are not linear.

2.3 Elements of Matrix Analysis

Let k be a local field of characteristic 0. Let $|| \cdot ||_k$ be the standard norm on k^d which is the canonical Euclidean (resp. Hermitian) norm if $k = \mathbb{R}$ (resp. $\mathbb{C}$) and the sup norm ($||(x_1, \ldots, x_d)||_k = \max\{|x_1|_k, \ldots, |x_d|_k\}$) if k is non Archimedean. We will also denote by $|| \cdot ||_k$ the operator norm induced on $M_d(k)$ by the standard norm $|| \cdot ||_k$ on k^d.

Let Q be a bounded subset of matrices in $M_d(k)$. We set

$$||Q||_k = \sup_{g \in Q} ||g||_k$$

and call it the norm of Q. Let $\overline{k}$ be an algebraic closure of k. It is well known (see

Lang's Algebra Lang [1983]) that the absolute value on k extends to a unique absolute value on $\overline{k}$. Hence the norm $||\cdot||_k$ also extends in a natural way to $\overline{k}^d$ and to $M_d(\overline{k})$. This allows one to define the *minimal norm* of a bounded subset Q of $M_d(k)$ as

$$E_k(Q) = \inf_{x \in GL_d(\overline{k})} ||xQx^{-1}||_k$$

We will also need to consider the *maximal eigenvalue* of Q namely

$$\Lambda_k(Q) = \max\{|\lambda|_k | \lambda \in \mathrm{spec}(q), q \in Q\}$$

where $\mathrm{spec}(q)$ denotes the set of eigenvalues (the spectrum) of q in $\overline{k}$. Define

$$Q^n = Q \cdot \ldots \cdot Q = \{A_1 \cdot \ldots \cdot A_n | A_i \in Q, i = 1..n\}.$$

Finally let $R_k(Q)$ be the *spectral radius* of Q

$$R_k(Q) = \lim_{n\to\infty} ||Q^n||_k^{1/n}$$

the limit exists because for $n = tq + r, n \in \mathbb{N}$ we have

$$||Q^n||^{\frac{1}{n}} \leq ||(Q^t)^{\frac{n-r}{t}}||^{\frac{1}{n}} ||Q^r||^{\frac{1}{n}} = ||Q^t||^{\frac{1}{t} - \frac{r}{nt}} ||Q^r||^{\frac{1}{n}} \tag{2.2}$$

by letting n tend to $+\infty$ for every t we have

$$\limsup_{n\to\infty} ||Q^n||^{\frac{1}{n}} = R(Q) \leq ||Q^t||^{\frac{1}{t}}$$

therefore $\limsup_{n\to\infty} ||Q^n||^{\frac{1}{n}} = \lim_{n\to\infty} ||Q^n||^{\frac{1}{n}}$. Note that these arguments also tell us that the limit coincides with $\inf_{n\in\mathbb{N}} ||Q^n||_k^{\frac{1}{n}}$. The quantities defined above are related to one another.

Obviously from the definitions that $E_k(Q) \leq ||Q||_k$ and $\Lambda_k(Q) \leq R_k(Q)$.

Lemma 2.3.1. *For any $n \in \mathbb{N}$ the following holds:*

$$\Lambda_k(Q^n) \geq \Lambda_k(Q)^n, \quad E_k(Q^n) \leq E_k(Q)^n, \quad R_k(Q^n) = R_k(Q)^n.$$

Proof. The following inclusion for sets ensures the first inequality.

$$\{|\lambda|_k^n, \lambda \in \operatorname{spec}(q), q \in Q\} \subseteq \{|\lambda|_k, \lambda \in \operatorname{spec}(q), q \in Q^n\}$$

For the second one we have

$$E_k(Q^n) = ||gQ^{nt}g^{-1}||^{\frac{1}{t}} = ||gQ^tg^{-1} \cdot \ldots \cdot gQ^tg^{-1}||^{\frac{1}{t}} \leq ||gQ^tg^{-1}||^{\frac{n}{t}} = E_k(Q)^n.$$

The last equality is also clear

$$R_k(Q^n) = \lim_{t\to\infty} ||Q^{tn}||^{\frac{1}{t}} = \lim_{p\to\infty} ||Q^p||^{\frac{n}{p}} = R_k(Q)^n, \text{ where } t = \frac{p}{n}.$$

$\square$

Corollary 2.3.2. *Collecting together all obtained information we have*

$$\Lambda_k(Q)^n \leq \Lambda_k(Q^n) \leq R_k(Q^n) = R_k(Q)^n \leq E_k(Q^n) \leq E_k(Q)^n. \tag{2.3}$$

2.4 Height and Lehmer Conjecture

For any rational prime p (or $p = \infty$) let us fix an algebraic closure $\overline{\mathbb{Q}}_p$ of the field of p-adic numbers $\mathbb{Q}_p$ (if $p = \infty$; set $\mathbb{Q}_\infty = \mathbb{R}$ and $\overline{\mathbb{Q}}_\infty = \mathbb{C}$). We take the standard normalization of the absolute value on $\mathbb{Q}_p$ (i.e. $|p|_p = \frac{1}{p}$). It admits a unique extension to $\overline{\mathbb{Q}}_p$, which we denote by $|\cdot|_p$.

Now we define the height function on the field of algebraic numbers $\overline{\mathbb{Q}}$ (for more details see Bilu et al.). To explain the motivation and nature of the function we introduce the definition step by step.

- First we define the height of a non-zero $\alpha \in \mathbb{Z}$ by $H(\alpha) = |\alpha|$ and $H(0) = 1$.
- On rational numbers, the absolute value is no longer adequate: there exist infinitely many rational numbers of bounded absolute value. To obtain finiteness, one should bound both the numerator and the denominator. Thus, for $\alpha = a/b \in \mathbb{Q}$, where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, we define $H(\alpha) = \max\{|a|, |b|\}$.

- Next, we wish to extend this definition to all algebraic numbers. One idea is to observe that $bX - a$ is the minimal polynomial of the rational number a/b over $\mathbb{Q}$. Hence, for $\alpha \in \overline{\mathbb{Q}}$ and also for a polynomial $P(X) \in \mathbb{Z}[X]$ one may define $H(\alpha) = H(P) = \max\{|a_0|, \ldots, |a_n|\}$, where $P(X) = a_n X^n + \ldots + a_0$ is the primitive minimal polynomial of α over $\mathbb{Z}$.

However this definition is not convenient to deal with.

The modern definition of height (due to A. Weil) is motivated by the following observation: the height of a rational number $\alpha = a/b$, originally defined as $\max\{|a|, |b|\}$, satisfies the identity

$$H(\alpha) = \prod_{v \in V_{\mathbb{Q}}} \max\{1, |\alpha|_v\}$$

where $V_{\mathbb{Q}}$ is the set of all equivalence classes of valuations on $\mathbb{Q}$.

Absolute Weil's height is the logarithm of right-hand side of this identity, properly generalized to number fields. Now we make some preparation to give a formal definition of the height. Let K be a number field. Let V_K be the set of equivalence classes of valuations on K. For $v \in V_K$ let K_v be the corresponding completion which is a finite extension of $\mathbb{Q}_p$ for some prime p. We normalize the absolute value on K_v to be the unique one that extends the standard absolute value on $\mathbb{Q}_p$. Namely $|x|_v = |N_{K_v|\mathbb{Q}_p}(x)|_p^{\frac{1}{n_v}}$ where $n_v = [K_v : \mathbb{Q}_p]$. We identify $\overline{K}_v$, the algebraic closure of K_v with $\overline{\mathbb{Q}}_p$. For $x \in K$ absolute logarithmic Weil's height the following quantity

$$h(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ |x|_v.$$

The height of x does not depend on K. For example, it is the same in all extensions of K.

We will use of the following basic inequalities valid for any two algebraic numbers x and y: $h(xy) \leq h(x) + h(y)$ and $h(x+y) \leq h(x) + h(y) + \log 2$.

Let us similarly define the height of a matrix $A \in M_d(K)$ by

$$h(A) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||A||_v$$

and the height of a finite set F of matrices in $M_d(K)$ by

$$h(F) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||F||_v,$$

where $n_v = [K_v : \mathbb{Q}_v]$. Note that for $v \in V_K$ we will use the subscript v instead of K_v in the quantities $E_v(F) = E_{K_v}(F)$, $\Lambda_v(F) = \Lambda_{K_v}(F)$, etc. We define the minimal height of F as:

$$e(F) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ E_v(F)$$

and the arithmetic spectral radius (or normalized height) of F

$$\widehat{h}(F) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ R_v(F).$$

Let V_f be the set of finite places and V_∞ the set of infinite places.For any height h, we also set $h = h_\infty + h_f$, where h_∞ is the infinite part of h (i.e. the part of the sum over the infinite places of K) and h_f is the finite part of h (i.e. the part of the sum over the finite places of K). Note again that these heights are well defined independently of the number field K such that $F \subset M_d(K)$. The above terminology is motivated in Section 3.3.

Definition 2.4.1. *Mahler measure of $P(x) = a_0 \prod_{i=1}^n (x - \alpha_i)$ is*

$$M_1(P) = |a_0| \prod_i \max(1, |\alpha_i|).$$

Recall that for $\alpha \in \overline{\mathbb{Q}}$ with a primitive minimal polynomial $P(X) \in \mathbb{Z}[X]$ we have $H(\alpha) = H(P) = \prod_{v \in V_{\mathbb{Q}}} \max\{1, |\alpha|_v\}$. Now we explain relations between $M_1(P)$ and $h(P)$ (or $H(P)$). Let $P(x) \in \mathbb{Z}[x]$ be a minimal primitive polynomial of $\alpha \in \overline{\mathbb{Q}}$. From the product formula and and from considering the Newton polygons of the irreducible factors (of degree n_v) of P over $\mathbb{Q}_p$ we have

$$|a_0| = \prod_{p<\infty} |a_0|_p^{-1} = \prod_{p<\infty} \prod_{v|p} \max(1, |\alpha|_v^{n_v}), \alpha \in \overline{\mathbb{Q}}.$$

Then from [Waldschmidt, 2000, pp. 74-79], Bombieri and Gubler [2006] we have $M_1(P) = \prod_v \max(1, |\alpha|_v^{n_v})$ thus

$$H(P)^n = M_1(P) \text{ therefore } h(\alpha) = h(P) = \frac{\log M_1}{n} = \sum_v \log^+ |\alpha|_v^{\frac{n_v}{n}}. \tag{2.4}$$

Note also that for every coefficient $a_i, i = 1, \dots, n$ of $P(x)$ we have

$$|a_i| \leq \binom{n}{i} M_1(P), \tag{2.5}$$

so there exist $C = C(n) \in \mathbb{Q}$ where $n = \deg P$, such that

$$\frac{1}{C} H(P) \leq M_1(P) \leq CH(P).$$

The first inequality follows from (2.5) immediately when the second is a fundamental result that is called Mahler inequality.

Conjecture 2.4.2 (Lehmer conjecture). *Mahler measure of any integral polynomial $P(x)$, that is not a product of cyclotomic polynomials, is bounded from below by a constant strictly bigger then* 1.

More specifically

$$M_1(P(x)) \geq M_1(x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1) \approx 1.1763.$$

Essentially, to disprove this conjecture, one should for every $\varepsilon > 0$ find a polynomial $P(x) \in \mathbb{Z}[x]$ that is not a product of cyclotomic polynomials, such that $M_1(P(x)) < 1 + \varepsilon$.

In terms of height the conjecture states that the Weil height $h(x)$ of an algebraic number that is not a root of unity must be bounded below by $\frac{\varepsilon_0}{deg(x)}$, where ε_0 is an absolute positive constant.

2.5 Escape from Subvarieties

The aim of this section is to prove Proposition 2.5.5 which is known as "escape from subvarieties" and was proved by Eskin, Mozes, and Oh (see Eskin et al.

[2005]). This result is explained also in Gill. We will use this result in sections 3.3 and 4.2.

The dimension $\dim(X)$ of an irreducible variety X is the length k of the longest chain $\{x\} = X_0 \subset X_1 \subset \cdots \subset X_k = X$ of irreducible subvarieties of X. An irreducible component of a variety V is an irreducible subvariety of V not contained in any other irreducible subvariety of V. If the irreducible components of a variety V all have the same dimension, we say V is pure dimensional, and define the dimension $\dim(V)$ of V to be that of any of its irreducible components.

The degree $\deg(V)$ of a pure-dimensional variety V of dimension r in n-dimensional affine or projective space is its number of intersection points with a generic linear variety of dimension $n-r$. (Here generic means outside a variety of positive codimention.) It remains to see how to define the dimension and the degree of a variety V when V is not irreducible. We simply define $\mathrm{d}(V)$ to be the dimension of the irreducible subvariety of V of largest dimension. As for the degree, it will be best to see it as a vector: we define the degree $\overrightarrow{\deg}(V)$ of an arbitrary variety V to be

$$(d_0, d_1, \ldots, d_k, 0, 0, 0, \ldots),$$

where $k = \dim(V)$ and d_j is the degree of the union of the irreducible components of V of dimension j.

First we recall the following theorem:

Theorem 2.5.1 (Generalized Bezout theorem)**.** *Let $X_1, X_2, \ldots, X_s$ be puredimensional varieties over $\mathbb{C}$ and let $Z_1, Z_2, \ldots, Z_t$ be the irreducible components of $X_1 \cap X_2 \cap \cdots \cap X_s$. Then*

$$\sum_{i=1}^{t} \deg Z_i \leq \prod_{j=1}^{s} \deg X_j$$

(see [Schinzel, 2000, p. 519]).

Let $\Gamma \subset GL_n(\mathbb{C})$ be any finitely generated subgroup and let H denote the Zariski closure of Γ, which is assumed to be Zariski connected. Let $Y = \cup_{i=1}^{n} Y_i \subset H$ be an algebraic variety where $Y_i, 1 \leq i \leq n$ are the irreducible components of

Y. Denote by $\mathrm{irr}(Y)$ the number of irreducible components of Y, by $\mathrm{irr}_{\mathrm{md}}(Y)$ the number of irreducible components of Y of the maximal dimension $\mathrm{d}(Y)$ and by $\mathrm{mdeg}(Y)$ the maximal degree of an irreducible component of Y. Let S be any given finite generating set of Γ.

Lemma 2.5.2. *If* $\mathrm{irr}_{\mathrm{md}}(Y) = 1$ *then there exists an element* $s \in S$ *such that the variety* $Z = Y \cap sY$ *satisfies* $\mathrm{d}(Z) < \mathrm{d}(Y)$.

Proof. Without loss of generality we may assume that Y_1 is the unique irreducible component of maximal dimension. If for every $s \in S$ we have $sY_1 = Y_1$ then it would follow that Y_1 is invariant under the group generated by S. However as this subgroup is Zariski dense and Y_1 is a proper closed subvariety it follows that this is impossible; hence there is some $s \in S$ such that $sY_1 \neq Y_1$. It follows that $\mathrm{d}(sY \cap Y) < \mathrm{d}(Y)$. □

Lemma 2.5.3. *Let* Y *be a proper subvariety of* H. *There exists an* $s \in S$ *such that for* $Z = Y \cap sY$ *either* $\mathrm{d}(Z) < \mathrm{d}(Y)$ *or* $\mathrm{irr}_{\mathrm{md}}(Z) < \mathrm{irr}_{\mathrm{md}}(Y)$.

Proof. Consider the set M of all maximal dimension irreducible components of Y. If every element of S would have mapped this set into itself it would have been $< S >$-invariant and this would contradict the assumption that $\Gamma =< S >$ is Zariski dense whereas Y is a Zariski closed proper subset. Hence there is some $s \in S$ so that for some element $Y_i \in M$ and $sY_i \notin M$ and it follows that for $Z = Y \cap sY$ either $\mathrm{d}(Z) < \mathrm{d}(Y)$ or $\mathrm{irr}_{\mathrm{md}}(Z) < \mathrm{irr}_{\mathrm{md}}(Y)$. □

Lemma 2.5.4. *Let* Y *be a proper subvariety of* H. *Then there exists an integer* $m \in \mathbb{N}$ *(depending only on* $\mathrm{irr}_{md}(Y)$*) and a sequence of* m *elements* $s_0, s_1, \ldots, s_{m-1}$ *of* S *so that if we define the following sequence of varieties* $V_0 = Y$ *and*

$$V_{i+1} = V_i \cap s_i V_i, \quad 0 \leq i \leq m-1,$$

then V_m *satisfies* $\mathrm{d}(V_m) < \mathrm{d}(Y)$. *Moreover* $\mathrm{irr}(V_m)$ *as well as* $\mathrm{mdeg}(V_m)$ *are also bounded above by constants depending only on* $\mathrm{irr}(Y)$ *and* $\mathrm{mdeg}(Y)$.

Proof. We shall be applying Theorem 2.5.1 to the intersections of pairs of irreducible varieties. Namely, let $W = \cup_{i=1}^{n} W_i$ be the decomposition of a Zariski closed variety W into irreducible components. Then we have

$$\widetilde{W} = W \cap sW = \cup_{i,j=1}^{n} W_i \cap sW_j.$$

Thus given $n = \mathrm{irr}(W)$ and $\mathrm{mdeg}(W)$ we have an estimate both on $irr(\widetilde{W})$ as well as on $\mathrm{mdeg}(\widetilde{W})$. Combining this observation with Lemmas 2.5.2 and 2.5.3 one can deduce the result. $\square$

Proposition 2.5.5. *Let $\Gamma \subset GL_n(\mathbb{C})$ be any finitely generated subgroup and let H denote the Zariski closure of Γ, which is assumed to be Zariski connected. For any proper subvariety X of H, there exists $N \geq 1$(depending on X) such that for any finite generating set S of Γ, we have*

$$\gamma(N, S) \not\subset X.$$

Proof. By repeated application of Lemma 2.5.4 at most $\mathrm{d}(X)+1$ times we find elements $w_1, w_2, \ldots, w_t \in \gamma(n, S)$, where $n \geq 2$ is bounded in terms of the constant depending only on $\mathrm{irr}(X)$ and $\mathrm{mdeg}(X)$, so that $\cup_{i=1}^{t} w_i X = \emptyset$. If $\gamma(n, S)$ were contained in X, then it would follow that $e \in \cup_{i=1}^{t} w_i X$, as $\gamma(n, S) = \gamma(n, S)^{-1}$ and hence $w_i^{-1} \in \gamma(n, S)$ for each $1 \leq i \leq t$. Therefore we have $\gamma(n, S) \not\subset X$. $\square$

We reformulate Proposition 2.5.5 in more convenient form for us.

Lemma 2.5.6 (see Breuillard [2011]). *Let K be a field, $d \in \mathbb{N}$. For every $m \in \mathbb{N}$ there is $N \in \mathbb{N}$ such that if X a K algebraic subvariety of $GL_d(K)$ such that the sum of the degrees of the geometrically irreducible components of X is at most m, then for any subset $\sum \subset GL_d(K)$ containing* Id *and generating a subgroup which is not contained in $X(K)$, we have $\sum^N \nsubseteq X(K)$.*

Chapter 3

Sets of Matrices and Height Gap Theorem

In this chapter we describe properties of sets of matrices that satisfy some conditions. After using them we deduce properties of height and prove Height gap theorem 3.3.1.

3.1 Spectral Radius Lemma for Several Matrices

Lemma 3.1.1. *Let L be a field and Q a subset of $M_2(L)$ such that Q and Q^2 consist of nilpotent matrices. Then there is a basis (u, v) of L^2 such that $Qu = 0$ and $Qv \subset Lu$.*

Proof. For any $A, B \in Q$ we have $A^2 = B^2 = (AB)^2 = 0$. It follows, unless A or B are zero, that $kerA = ImA$ and $kerB = ImB$. Also if $AB \neq 0$ we get $kerB = ker(AB) = Im(AB) = ImA$ while if $AB = 0$ then $ImB = kerA$. So at any case $kerA = ImA = kerB = ImB$. So we have proved that the kernels and images of non zero elements of Q coincide and are equal to some line Lu say. Pick $v \in L^2 \backslash \{Lu\}$ then (u, v) forms the desired basis. □

The condition from the previous lemma that Q and Q^2 consist of nilpotent matrices is in fact very strong. It actually means that the set of matrices consists of matrices proportional to a one fixed nilpotent matrix.

Corollary 3.1.2. *Let L be a field and Q a subset of $M_2(L)$ such that Q and Q^2 consist of nilpotent matrices then there exists a nilpotent matrix N such that $Q \subseteq \{\lambda N : \lambda \in L\}$.*

Corollary 3.1.3. *The product of two nilpotent 2×2 matrices is nilpotent if and only if it is zero.*

A **principal ideal domain** is an integral domain where every ideal is a principal ideal. In a principal ideal domain, an ideal (p) is maximal if and only if p is irreducible. An ideal of a commutative ring is said to be irreducible if it cannot be written as a finite intersection of ideals properly containing it.

A **discrete valuation ring** R is a principal ideal domain with exactly one nonzero maximal ideal M. Any generator t of M is called a **uniformizer** or **uniformizing element** of R; in other words, a uniformizer of R is an element $t \in R$ such that $t \in M$ but $t \notin M^2$.

Given a discrete valuation ring R and a uniformizer $t \in R$, every element $z \in R$ can be written uniquely in the form $u \cdot t^n$ for some unit $u \in R$ and some nonnegative integer $n \in \mathbb{Z}$. The integer n is called the **order** of z, and its value is independent of the choice of uniformizing element $t \in R$.

Lemma 3.1.4. *Let k be a local field with ring of integers O_k and uniformizer π. Let $A = (a_{ij}) \in M^2(O_k)$ such that $\det(A)$ belong to (π^2) and $a_{11}, a_{22}, a_{21} \in (\pi)$ while $a_{12} \in O_k^\times$. Then $a_{21} \in (\pi^2)$.*

Proof. We have $a_{12}a_{21} = a_{11}a_{22} - det(A) \in (\pi^2)$ and $a_{12} \in O_k^\times$, hence $a_{21} \in (\pi^2)$. ☐

Lemma 3.1.5. *Let k be a local field with ring of integers O_k and uniformizer π together with an absolute value $|\cdot|_k$, which is (uniquely) extended to an algebraic closure $\overline{k}$ of k. Let Q be a subset of $M_2(O_k)$ such that $\Lambda_k(Q)$ and $\Lambda_k(Q^2)$ are both $\leq |\pi|_k$. Then there is $T \in GL_2(k)$ such that $TQT^{-1} \subset \pi M_2(O_k)$.*

Proof. Projecting Q to $M_2(L)$ where L is the residue field $L = O_k/(\pi)$ the matrices from Q and Q^2 become nilpotent. By Corollary 3.1.2 we have $Q|_L = \{\lambda N\}$

which implies that

$$Q \subseteq \{\lambda N + \pi A : \lambda \in k, A \in M_2(k)\}.$$

Clearly that we can find the transformation P such that PQP^{-1} consists of matrices $A = (a_{ij}) \in M_2(O_k)$ with $a_{11}, a_{22}, a_{21} \in (\pi)$ and $a_{12} \in O_k^{\times}$. Using the condition $\Lambda_k(Q) \leq |\pi|_k$ we have $\det A \leq \Lambda_k(Q)^2 \leq |\pi|_k^2$. Hence by Lemma 3.1.4, $a_{21} \in (\pi^2)$. Let $T = \mathrm{diag}(\pi, 1) \in GL_2(k)$. Then clearly $TQT^{-1} \subset \pi M_2(O_k)$. □

Remark 3.1.6. *If $Id \in Q$ then $\Lambda_k(Q) \leq \Lambda_k(Q^2)$.*

Definition 3.1.7. *Let X and Y be two non-empty subsets of a metric space (M, d). We define their Hausdorff distance $d_H(X, Y)$ by*

$$d_H(X, Y) = \max\{\sup_{x \in X} \inf_{y \in Y} d(x, y), \sup_{y \in Y} \inf_{x \in X} d(x, y)\}.$$

Equivalently

$$d_H(X, Y) = \inf\{r > 0, X \subset Y_r \text{ and } Y \subset X_r\}$$

where

$$X_r = \bigcup_{x \in X} \{z \in M, d(z, x) \leq r\}.$$

Proposition 3.1.8. *Let (S, d) be a compact metric space and*

$$X := \{K \subset S, K \text{ is compact}\}.$$

Then (X, d_H) is a compact metric space.

Proof. Suppose that (X, d_H) is not compact. Then for X there exists an open cover $\bigcup U_i$ that does not have a finite subcover. This means that for every finite subcover there exists $K \in X$ not covered by it. Therefore there exists $x \in K \subset S$ not covered. Now consider $\bigcup \widetilde{U}_i$ where

$$\widetilde{U}_i = \bigcup_{V_k \in U_i} V_k.$$

$\bigcup \widetilde{U}_i$ is a cover for S. We do not have a finite subcover for S either. This is a contradiction with the compactness of S. □

The following lemma ensures us that we can always find a matrix in a set Q^2 whose maximal eigenvalue is not much smaller than square of the minimal norm of the set. Elements with large eigenvalues will be used as generators of a free group in a "ping-pong method" (see Section 4.1).

Lemma 3.1.9 (Spectral Radius Lemma). *Let Q be a bounded subset of $M_2(k)$*

(a) if k is non Archimedean, then $\Lambda_k(Q^2) = E_k(Q)^2$;

(b) if k is Archimedean, there is a constant $c \in (0,1)$ independent of Q such that $\Lambda_k(Q^2) \geq c^2 E_k(Q)^2$.

Proof. (a): From Section 2.3 and in particular from Lemma 2.3.1 we have

$$\Lambda_k(Q)^2 \leq \Lambda_k(Q^2) \leq E_k(Q^2) \leq E_k(Q)^2.$$

Assume that $\Lambda_k(Q^2) < E_k(Q)^2$. Then we have also $\Lambda_k(Q) < E_k(Q)$. Extending the field k, we may assume that

$$\Lambda_k(Q^2) \leq |\pi|_k E_k(Q)^2, \quad \Lambda_k(Q) \leq |\pi|_k E_k(Q),$$

where π is a primitive element of k. Put $y = \min\{||gQg^{-1}|| : g \in GL_2(k)\}$ The existence of the minimum is assured by the discreteness of the absolute value on k. Replacing Q by a conjugate and multiplying it by a suitable scalar, we may assume that $||Q|| = y = 1$. Then both $\Lambda_k(Q)$ and $\Lambda_k(Q^2)$ do not exceed $|\pi|_k$, and Lemma 3.1.5 implies that for some $g \in GL_2(k)$ we have $||gQg^{-1}|| \leq |\pi|_k < 1$, contradicting the minimal choice of y.

(b): It is enough to give a proof for a compact set because we can approximate any set by compacts set. We prove it by contradiction, if such a c did not exist, then we may find a sequence of Q_n such that $\frac{\Lambda_k(Q_n^2)}{E_k(Q_n)^2} \to 0$, in the Hausdorff metric. We can change Q_n into $\frac{Q_n}{E_k(Q_n)}$ and thus obtain a sequence of compact sets in $M_2(k)$ such that $E_k(Q_n) = 1$ with $\Lambda_k(Q_n^2) \to 0$ and $\Lambda_k(Q_n) \to 0$ and passing to a limit, we obtain a compact subset Q of $M_2(k)$ which exists by Proposition 3.1.8 such that $\Lambda_k(Q^2) = \Lambda_k(Q) = 0$ while $E_k(Q) = 1$ By Corollary 3.1.2, we can transform Q to a subset of

$$\left\{ \begin{bmatrix} 0 & \lambda \\ 0 & 0 \end{bmatrix}, where \quad \lambda \in L \right\}$$

thus $E_k(Q) = 0$. This is a contradiction. $\square$

Remark 3.1.10. *Note that the proof of (b) is not effective because of a compactness argument.*

An analogous result with almost the same proof holds in general (see Breuillard [2008a]).

Lemma 3.1.11 (Spectral Radius Formula for Q)**.** *Let Q be a bounded subset of $M_d(k)$.*

(a) if k is non Archimedean, there is an integer $q \in [1, d^2]$ such that $\Lambda_k(Q^q) = E_k(Q)^q$.

(b) if k is Archimedean, there is a constant $c = c(d) \in (0, 1)$ independent of Q and an integer $q \in [1, d^2]$ such that $\Lambda_k(Q^q) \geq c^q E_k(Q)^q$.

Proposition 3.1.12. *Let Q be a bounded subset of $M_2(k)$. We have*

$$R_k(Q) = \lim_{n\to\infty} E_k(Q^n)^{\frac{1}{n}} = \inf_{n\in\mathbb{N}} E_k(Q^n)^{\frac{1}{n}} = \lim_{n\to\infty} \Lambda_k(Q^{2n})^{\frac{1}{2n}} = \sup_{n\in N} \Lambda_k(Q^n)^{\frac{1}{n}}.$$

Moreover if k is non Archimedean, $R_k(Q) = E_k(Q)$, while if k is Archimedean, then $cE_k(Q) \leq R_k(Q) \leq E_k(Q)$, where c is the constant from Lemma 3.1.9 (b).

Proof. First we prove the first equality. Since $E_k(Q^n) \leq ||Q^n||_k$ for every $n \in \mathbb{N}$ then $E_k(Q^n)^{\frac{1}{n}} \leq R_k(Q)$. On the other hand,

$$R_k(Q) = R_k(gQg^{-1}) \leq ||gQg^{-1}||_k$$

for every $g \in GL_2(\overline{k})$. Hence $R_k(Q) \leq E_k(Q)$ and for every $n \in \mathbb{N}$ we have $R_k(Q)^n = R_k(Q^n) \leq E_k(Q^n)$, hence $R_k(Q) \leq \liminf E_k(Q^n)^{\frac{1}{n}}$. Thus $\lim E_k(Q^n)^{\frac{1}{n}}$ exists and equals $R_k(Q)$. For $n > 1, n \in \mathbb{N}$ we have

$$||gQ^{nt}g^{-1}||^{\frac{1}{nt}} = ||gQ^tg^{-1}gQ^tg^{-1} \cdot \ldots \cdot gQ^tg^{-1}||^{\frac{1}{nt}} \leq ||gQ^tg^{-1}||^{\frac{1}{t}}.$$

Thus the second equality is clear.

It is also clear that as $\Lambda_k(Q^n) \leq E_k(Q^n)$ we have

$$\limsup \Lambda_k(Q^{2n})^{\frac{1}{2n}} \leq \limsup \Lambda_k(Q^n)^{\frac{1}{n}} \leq R_k(Q).$$

By Lemma 3.1.9 $\Lambda_k(Q^2)^{\frac{1}{2}} \geq cE_k(Q)$ (where $c = 1$ if k is non Archimedean) thus

$$\Lambda_k(Q^{2n})^{\frac{1}{2n}} \geq c^{\frac{1}{n}} E_k(Q^n)^{\frac{1}{n}} \geq c^{\frac{1}{n}} R_k(Q)$$

which forces $\liminf \Lambda_k(Q^{2n})^{\frac{1}{2n}} \geq R_k(Q)$ Hence from two inequalities above we have that $\lim_{n\to+\infty} \Lambda_k(Q^{2n})^{\frac{1}{2n}}$ exists and equals $R_k(Q)$. Since for every $n, p \in \mathbb{N}$ we have $\Lambda_k(Q^{np}) \geq \Lambda_k(Q^p)^n$ and thus

$$\Lambda_k(Q^{np})^{\frac{1}{np}} \geq \Lambda_k(Q^p)^{\frac{1}{p}}$$

by letting n tend to $+\infty$ we indeed get $R_k(Q) = \sup_{p\in\mathbb{N}} \Lambda_k(Q^p)^{\frac{1}{p}}$.

By Lemma 2.3.1 have for any $q \in \mathbb{N}$ that $\Lambda_k(Q^q)^{\frac{1}{q}} \leq R_k(Q) \leq E_k(Q)$. If k is non Archimedean, then this combined with Lemma 3.1.9 (a) shows the desired identity. If k is Archimedean, then Lemma 2.3.1 gives $\Lambda_k(Q^q) \leq R_k(Q)^q$, which when combined with Lemma 3.1.9 (b) and (2.3) gives

$$E_k(Q) \geq R_k(Q) \geq \Lambda_k(Q^2)^{\frac{1}{2}} \geq cE_k(Q).$$

□

Remark 3.1.13. *Define $F \subset GL_2(\mathbb{C})$ as follows*

$$F = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \right\}.$$

For this set we have

$$\lim_{n\to\infty} \Lambda_k(Q^{2n})^{\frac{1}{2n}} = 1 \neq 0 = \lim_{n\to\infty} \Lambda_k(Q^{2n+1})^{\frac{1}{2n+1}}.$$

Thus $2n$ in Theorem 3.1.12 is essential.

Note also that if Q belongs to $SL_2(k)$ then $E_k(Q) \geq R_k(Q) \geq \Lambda_k(Q) \geq 1$ and all three quantities remain unchanged if we add Id to Q. The following lemma explains what happens if these quantities are close or equal to 1.

A similar result with a similar proof holds in general (see Breuillard [2008a]).

Proposition 3.1.14. *Let Q be a bounded subset of $M_d(k)$ such that $1 \in Q$. We have*

$R_k(Q) = \lim_{n\to\infty} E_k(Q^n)^{\frac{1}{n}} = \inf_{n\in\mathbb{N}} E_k(Q^n)^{\frac{1}{n}}$

$R_k(Q) = \lim_{n\to\infty} \Lambda_k(Q^n)^{\frac{1}{n}} = \sup_{n\in N} \Lambda_k(Q^n)^{\frac{1}{n}}$

Moreover if k is non Archimedean, $R_k(Q) = E_k(Q)$, while if k is Archimedean, then $cE_k(Q) \leq R_k(Q) \leq E_k(Q)$, where c is the constant from Lemma 3.1.11 (b).

For a real number w, let M_w denote the unique simply connected surface (real 2-dimensional Riemannian manifold) with constant curvature w. Denote by D_w the diameter of M_w, which is $+\infty$ if $w < 0$ and $\frac{1}{\sqrt{w}}$ for $w > 0$.

Let (X, d) be a geodesic metric space, i.e. a metric space for which every two points $x, y \in X$ can be joined by a geodesic segment, an arc length parametrized continuous curve. Let $\triangle$ be a triangle in X with geodesic segments as its sides. $\triangle$ is said to satisfy the $CAT(w)$ inequality if there is a comparison triangle $\triangle'$ in the model space M_w, with sides of the same length as the sides of $\triangle$, such that distances between points on $\triangle$ are less than or equal to the distances between corresponding points on $\triangle'$. The geodesic metric space (X, d) is said to be a $CAT(w)$ space if every geodesic triangle $\triangle$ in X with perimeter less than $2D_w$ satisfies the $CAT(w)$ inequality.

Remark 3.1.15.

- *Any $CAT(w)$ space (X, d) is also a $CAT(l)$ space for all $l > w$. In fact, the converse holds: if (X, d) is a $CAT(l)$ space for all $l > w$, then it is a $CAT(w)$ space.*
- *n-dimensional Euclidean space with its usual metric is a $CAT(0)$ space.*
- *n-dimensional hyperbolic space $\mathbb{H}^n$ with its usual metric is a $CAT(-1)$ space, and hence a $CAT(0)$ space as well.*

Define
$$L = \left\{ \begin{bmatrix} a & b \\ \bar{b} & c \end{bmatrix} \text{ such that } b \in \mathbb{C} \text{ and } a, c \in \mathbb{R} \right\}$$
and
$$\mathbb{H} = \{A \in L \text{ such that } \det A = 1 \text{ and } a, c > 0\}.$$

Note that for $P \in SL_2(\mathbb{C})$ and $A \in \mathbb{H}$ we have the group action

$$P(A) := PAP^*$$

where $P^* = \overline{P}^T$. Note also that $\mathbb{H}$ can be represented as $H^3 = \mathbb{C} \times (0, +\infty)$ due to

$$\mathbb{H} \to H^3,$$
$$\begin{bmatrix} a & b \\ \bar{b} & c \end{bmatrix} \mapsto \frac{b+j}{c}.$$

Using this representation we have the action of $PSL_2(\mathbb{C})$ on H^3 that may be written as

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} (z+tj) = \frac{(\alpha z+\beta)\overline{(\gamma z+\delta)} + \alpha\overline{\gamma}t^2 + tj}{|\gamma z+\delta|^2 + |\gamma|^2 t^2}$$

where $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in PSL_2(\mathbb{C})$ and $(z+tj) \in H^3$.

Lemma 3.1.16 (Linear growth of displacement squared)**.** *Suppose k is Archimedean (i.e. $k = \mathbb{R}$ or $\mathbb{C}$). Then we have for every $n \in N$ and every bounded subset Q of $SL_2(k)$ containing* Id*,*

$$E_k(Q^n) \geq E_k(Q)^{\sqrt{\frac{n}{4}}} \tag{3.1}$$

Moreover,

$$\log R_k(Q) \geq c_1 \log E_k(Q) \min\{1, \log E_k(Q)\}$$

for some constant $c_1 > 0$. In particular $E_k(Q) = 1$ if and only if $R_k(Q) = 1$.

Proof. We use non-positive curvature of hyperbolic space $\mathbb{H}^3$.

For $x \in \mathbb{H}^3$ set $L(Q,x) = \max_{g\in Q} d(gx,x)$ and $L(Q) = \inf_x L(Q,x)$. Fix $\varepsilon > 0$, set $\ell_n := L(Q^n) = 2\log E_k(Q^n)$, and let r_n be the infimum over $x \in \mathbb{H}^3$ of the smallest radius of a closed ball containing $Q^n x$ Note first that $r_n \leq \ell_n$. We now prove (3.1). Fix $\varepsilon > 0$ and let $x, y \in H^3$ be such that $Q^{n+1}x$ is contained in a ball of radius $r_{n+1} + \varepsilon$ around y. Let $q \in Q$ be arbitrary. Since Q contains Id we have $Q^n x \subset Q^{n+1}x$, and $qQ^n x$ lies in the two balls of radius $r_{n+1} + \varepsilon$ centered around qy and around y. By the CAT(0) inequality for the median (see Remark 3.1.15), the intersection of the two balls is contained in the ball B of radius $t := \sqrt{(r_{n+1}+\varepsilon)^2 - d(qy,y)^2/4}$ centered around the midpoint m between y and qy. Translating by q^{-1} we get that $Q^n x$ lies in the ball of radius t centered at $q^{-1}m$. In particular $r_n \leq t$. This means $d(qy,y)^2 \leq 4((r_{n+1}+\varepsilon)^2 - r_n^2)$. Since $q \in Q$ and $\varepsilon > 0$ were arbitrary, we obtain $\ell_1^2 \leq 4(r_{n+1}^2 - r_n^2)$. Summing over n, we get $n\ell_1^2 \leq 4r_n^2 \leq 4\ell_n^2$, hence (3.1). But by Lemma 3.1.9 (b), $\Lambda_k(Q^{2n}) \geq c^2 E_k(Q^n)^2$, hence

$$R_k(Q) \geq \Lambda_k(Q^{2n})^{\frac{1}{2n}} \geq c^{\frac{1}{n}} E_k(Q)^{\sqrt{\frac{1}{4n}}}.$$

Optimizing in n, we obtain the desired bound. ☐

An analogous result with almost the same proof holds in general (see Breuillard [2008a]).

Lemma 3.1.17 (growth of displacement)**.** *Suppose k is Archimedean (i.e. $k = \mathbb{R}$ or $\mathbb{C}$). Then we have for every $n \in \mathbb{N}$ and every bounded subset Q of $SL_2(k)$ containing* Id*,*

$$E_k(Q^n) \geq E_k(Q)^{\sqrt{\frac{n}{4d}}} \tag{3.2}$$

Moreover,

$$\log R_k(Q) \geq c_1 \log E_k(Q) \min\{1, \log E_k(Q)\} \tag{3.3}$$

for some constant $c_1 = c_1(d) > 0$.

3.2 Properties of Matrix Heights

In this section, we prove some properties of matrix heights. We prove them for any dimension.

Proposition 3.2.1. *Let F be a finite subset of $M_d(\mathbb{Q})$. Then*

(a) $\widehat{h}(F) = \lim_{n\to+\infty} \frac{1}{n} h(F^n) = \inf_{n\in\mathbb{N}} \frac{1}{n} h(F^n)$,

(b) $e_f(F) = \widehat{h}_f(F)$ and $e(F) + \log c \leq \widehat{h}(F) \leq e(F)$ where c is the constant in Lemma 2.1 (b),

(c) $\widehat{h}(F^n) = n\widehat{h}(F)$ and $\widehat{h}(F \cup \{Id\}) = \widehat{h}(F)$,

(d) $\widehat{h}(xFx^{-1}) = \widehat{h}(F)$ if $x \in GL_d(\overline{\mathbb{Q}})$.

Proof. We will use results of Section 2.3 and Proposition 3.1.14.

(a) Since F is finite, there are only finitely many places v such that $||F||_v > 1$. For each such place we have

$$\frac{1}{n}\log^+ ||F^n||_v \to \log^+ R_v(F)$$

hence $\frac{1}{n}h(F^n) \to \widehat{h}(F)$.

The equality $\lim_{n\to+\infty} \frac{1}{n}h(F^n) = \inf_{n\in\mathbb{N}} \frac{1}{n}h(F^n)$ follows immediately from $\lim_{n\to\infty} ||F^n||^{\frac{1}{n}} = \inf_{n\in\mathbb{N}} ||F^n||_k^{\frac{1}{n}}$ (see (2.2)).

(b) We have $E_v(F) = R_v(F)$ if $v \in V_f$ hence $e_f(F) = \widehat{h}_f(F)$ while

$$cE_v(F) \leq R_v(F) \leq E_v(F) \text{ if } v \in V_\infty$$

hence

$$e_\infty(F) + \log c \leq \widehat{h}_\infty(F) \leq e_\infty(F).$$

(c) We have $R_v(F^n) = R_v(F)^n$ for every $n \in \mathbb{N}$ and every place v. Hence $\widehat{h}(F^n) = n\widehat{h}(F)$.

(d) Finally using $R_k(xFx^{-1}) = R_k(F)$ we obtain the last equality. $\square$

Proposition 3.2.2. *Let F be a finite subset of $M_d(\mathbb{Q})$ then*

(a) $e(xFx^{-1}) = e(F), x \in GL_d(\mathbb{Q})$,

(b) $e(F^n) \leq ne(F)$,

(c) If λ is an eigenvalue of an element of F then $h(\lambda) \leq \widehat{h}(F) \leq e(F)$,

(d) If $F \subset GL_d(\mathbb{Q})$ then $e(F \cup F^{-1}) \leq (2d-1)e(F)$ and $e(F \cup \{1\}) = e(F)$. If F is a subset of $SL_d(\mathbb{Q})$ then $e(F \cup F^{-1}) \leq (d-1)e(F)$.

Proof. The first three items are clear (see Section 2.3). For the last, observe that for any $x \in GL_d(K_v)$ we have

$$||x^{-1}||_v \leq \frac{1}{|\det(x)|_v}\left|\frac{\det(x)}{\lambda_d}\right|_v \leq \frac{1}{|\det(x)|_v}||x||_v^{d-1} \tag{3.4}$$

where λ_d is the minimal eigenvalue of x. Hence

$$||(F \cup F^{-1})||_v \leq ||F||_v^{d-1} \max\left\{\frac{1}{|\det(x)|_v}, x \in F \cup \{1\}\right\}$$

and

$$E_v(F \cup F^{-1}) \leq E_v(F)^{d-1} \max \left\{ \frac{1}{|\det(x)|_v}, x \in F \cup \{1\} \right\}.$$

So

$$\begin{aligned} e(F \cup F^{-1}) &\leq (d-1)e(F) + \max\{h(\det(x)^{-1}), x \in F \cup \{1\}\} \\ &= (d-1)e(F) + \max\{h(\det(x)), x \in F \cup \{1\}\} \\ &\leq (d-1)e(F) + \max\{h(\lambda_1) \cdot \ldots \cdot h(\lambda_d); \lambda_i \in \operatorname{spec}(x); i = 1, \ldots, d; x \in F \cup \{1\}\} \end{aligned}$$

i.e. $e(F \cup F^{-1}) \leq (2d-1)e(F)$. □

Remark 3.2.3. *Note that the equality in* (3.4) *(instead of inequality) is stated in the proof of this result in [Breuillard, 2008b, p.17]. This equality holds just for* $d = 2$ *and does not hold for* $d > 2$ *due to the following example:*

$$X := \begin{bmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in GL_3(\mathbb{Q}), \quad X^{-1} = \begin{bmatrix} \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

then $||X^{-1}||_v = 1 < \frac{9}{6} = \frac{1}{|\det(X)|_v}||X||_v^2$

We can also compare $e(F)$ and $\widehat{h}(F)$ when $\widehat{h}(F)$ is small:

Proposition 3.2.4. *For every* $\varepsilon > 0$ *there is* $\delta = \delta(d, \varepsilon) > 0$ *such that if* F *is a finite subset of* $SL_d(\mathbb{Q})$ *containing* 1 *with* $\widehat{h}(F) < \delta$*, then* $e(F) < \varepsilon$*. Moreover* $\widehat{h}(F) = 0$ *if and only if* $e(F) = 0$*.*

Proof. This follows immediately from Proposition 3.2.1 (b) and Proposition 3.2.5 below using them for $e_\infty(F) < 1$ we have

$$\begin{aligned} e^2(F) = (e_f(F) + e_\infty(F))^2 &\leq 2(e_f^2(F) + e_\infty^2(F)) \\ &\leq 2(\widehat{h}_f^2(F) + \frac{4}{c}\widehat{h}_\infty(F)) \leq 2(\delta^2 + \frac{4}{c}\delta) < 2(1 + \frac{4}{c})\delta \end{aligned}$$

and for $e_\infty \geq 1$ we have

$$e(F) = e_f(F) + e_\infty(F) \leq \widehat{h}_f(F) + \frac{4}{c}\widehat{h}_\infty(F) \leq (1 + \frac{4}{c})\delta.$$

□

Proposition 3.2.5. *Let c_1 be the constant from Lemma 3.1.11, then*

$$\widehat{h_\infty}(F) \geq \frac{c_1}{4} e_\infty(F) \min\{1, e_\infty(F)\}$$

for any finite subset F of $SL_d(\mathbb{Q})$ containing 1.

Proof. By Lemma 3.1.17 we have

$$\widehat{h_v}(F) \geq \frac{c_1}{4} e_v(F) \min\{1, e_v(F)\} \text{ for every } v \in V_\infty.$$

We may write

$$e_\infty(F) = \alpha e^+(F) + (1-\alpha) e^-(F)$$

where e^+ is the average of the e_v greater than 1 and e^- the average of the e_v smaller than 1. This means

$$e^+ \sum_{v \in V_\infty, e_v > 1} n_v = \sum_{v \in V_\infty, e_v > 1} n_v e_v$$

and similarly for e^-. Applying Cauchy-Schwarz, we have

$$\widehat{h_\infty}(F) \geq c_1(\alpha e^+ + (1-\alpha)(e^-)^2).$$

If $\alpha e^+(F) \geq \frac{1}{2} e_\infty(F)$, then $\widehat{h_\infty}(F) \geq \frac{c_1}{2} e_\infty(F)$, and otherwise $(1-\alpha)e^- \geq \frac{e_\infty}{2}$, hence

$$\widehat{h_\infty}(F) \geq c_1(1-\alpha)(e^-)^2 \geq \frac{c_1}{4} e_\infty^2.$$

At any case

$$\widehat{h_\infty}(F) \geq \frac{c_1}{4} e_\infty(F) \min\{1, e_\infty(F)\}.$$

□

3.3 Height Gap Theorem

In this section, we prove Theorem 3.3.1. This result can be seen as a non abelian version of Lehmer conjecture.

Theorem 3.3.1 (Height Gap Theorem)**.** *There is a positive constant $\varepsilon = \varepsilon(d) > 0$ such that if F is a finite subset of $GL_d(\overline{\mathbb{Q}})$ generating a non virtually solvable subgroup Γ then $\widehat{h}(F) > \varepsilon$. Moreover, if the Zariski closure of Γ is semisimple, then*

$$\widehat{h}(F) \leq \inf_{g \in GL_d(\overline{\mathbb{Q}})} h(gFg^{-1}) \leq C\widehat{h}(F)$$

for some absolute constant $C = C(d) > 0$.

Height gap theorem is stated above for any $d \in \mathbb{N}$ but it will be proved just for $d = 2$ (for a general case see Breuillard [2008a]). So we hereafter assume $d = 2$.

We may assume that $F = \{Id, A, B\}$ with A semisimple (in fact both A and B can be taken semisimple). Moreover A has an order that exceed d_1, and $bc \notin \{0, -1, e^{\frac{2\imath\pi}{3}}, e^{\frac{4\imath\pi}{3}}\}$ after we conjugate A and B in the form (3.5) below. The general case follows from this as we will show in the next lemma.

Lemma 3.3.2. *For every $m \in \mathbb{N}$, there exists $N(m) \in \mathbb{N}$ with the following property. Let F be a finite subset of $SL_2(\overline{\mathbb{Q}})$ containing 1 and generating a non-virtually solvable subgroup such that the sum of the degrees of the geometrically irreducible components of that group is at most m. Then there exists $A, B \in F^{N(m)}$ such that A and B are semisimple, generate a non-virtually solvable group, A has an order that exceeds m, and $bc \notin \{0, -1, e^{\frac{2\imath\pi}{3}}, e^{\frac{4\imath\pi}{3}}\}$ after we conjugate A and B in the form (3.5).*

Proof. The proof of this lemma follows directly from Eskin-Mozes-Oh's " Escape from subvarieties " (see Lemma 2.5.6) applied to $\sum = F \times F$ in $SL_2 \times SL_2 \leq GL_4$ with $X = X_1 \cup X_2 \cup X_3 \cup X_4$ where

$X_1 = \{(A, B), A$ or B has order at most $d_1\}$,

$X_2 = \{(A, B), \mathrm{tr}(A)$ or $\mathrm{tr}(B)$ is $2\}$,

$X_3 = \{(A, B), A$ and B generate a virtually solvable subgroup $\}$,

X_4 the Zariski closure of $\{(gAg^{-1}, gBg^{-1}), g \in SL_2, A$ diagonal $, bc \in \{0, -1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\}\}$.

X_3 is a proper subvariety of $SL_2 \times SL_2$ because there are pairs of matrices that generate groups which are not virtually solvable. X_4 is a proper subvariety of $SL_2 \times SL_2$ too because the first matrices of pairs are semisimple. $\square$

From the properties of height that were observed in Proposition 3.2.4, $\widehat{h}(F)$ is small if and only if $e(F)$ is small. So we may as well replace $\widehat{h}(F)$ by $e(F)$ in Theorem 3.3.1. Since $e(F)$ is invariant under conjugation by any element in $GL_2(\overline{\mathbb{Q}})$, we may assume that A is diagonal, i.e.

$$A = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}, B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \tag{3.5}$$

Let $\deg(\lambda)$ be the degree of λ as an algebraic number over $\mathbb{Q}$. The following proposition is extremely important for us:

Proposition 3.3.3 (small normalised height implies small height of matrix coordinates)**.** *For every $\beta > 0$ there exists $d_0, \nu > 0$ such that, if $F = \{Id, A, B\}$ are as in (3.5) and if $e(F) \leq \nu$ and $\deg(\lambda) \geq d_0$ then*

$$\max\{h(ad), h(bc)\} \leq \beta.$$

In order to prove this statement, we need

- to give local estimates at each place v;
- to show by the equidistribution theorem that when these estimates are put together the error terms give only a negligible contribution to the height.

Let K be the number field generated by the coefficients of A and B. Let $v \in V_K$ be a place of K. We set $s_v = \log E_v(F)$ and $\delta = \lambda^{-1} - \lambda$.

Lemma 3.3.4 (Local estimates)**.** *For each $v \in V_K$ we have*

$$\max\{|a|_v, |d|_v, \sqrt{|bc|_v}\} \leq C_v e^{4s_v} \max\{1, |\delta^{-1}|_v\}$$

where C_v is a constant equal to 1 if v is a finite place and equal to a number $C_\infty > 1$ if v is infinite. Moreover there are absolute constants $\varepsilon_0 > 0$ and $C_0 > 0$ such that if v is infinite and $s_v \leq \varepsilon_0$, then

$$\max\{|ad|_v, |bc|_v\} \leq 1 + C_0(\sqrt{s_v} + \frac{\sqrt{s_v}}{|\delta|_v} + \frac{s_v}{|\delta|_v^2}).$$

Proof. In order not to overburden notation in this proof we set s_v to be some number arbitrarily close but strictly bigger than $\log E_v(F)$ and we can let it tend to $\log E_v(F)$ at the end.

If v is infinite, then $\overline{\mathbb{Q}}_v = \mathbb{C}$ and $SL_2(\mathbb{C}) = KAN$ where

- $K = SU_2(\mathbb{C})$,
- A is the group of diagonal matrices with real positive entries, $\det A = 1$,
- N is the group of unipotent complex upper triangular matrices.

As K leaves the norm invariant, there must exist a matrix $P \in AN$ such that $\max\{||PAP^{-1}||, ||PBP^{-1}||\} \leq e^{s_v}$. Since $P \in AN$ we may write $p = \begin{bmatrix} t & y \\ 0 & t^{-1} \end{bmatrix}$ with $t > 0$ and $y \in \mathbb{C}$. Then we have, setting $\delta = \lambda^{-1} - \lambda$

$$PAP^{-1} = \begin{bmatrix} \lambda & ty\delta \\ 0 & \lambda^{-1} \end{bmatrix}, PBP^{-1} = \begin{bmatrix} a + cyt^{-1} & bt^2 + dyt - ayt - cy^2 \\ t^{-2}c & -yct^{-1} + d \end{bmatrix}. \tag{3.6}$$

Claim : There is $u_0 > 0$ such that if $0 \leq u \leq u_0$ and $||B|| \leq e^u$ then

$$\max\{|a - \overline{d}|, |b + \overline{c}|\} \leq 2\sqrt{2u}, \tag{3.7}$$

$$\max\{|a|^2 + |b|^2, |d|^2 + |c|^2\} \leq 1 + 4u, \tag{3.8}$$

$$\max\{|a|, |b|, |c|, |d|\} \leq 1 + 2u. \tag{3.9}$$

To prove this recall that for the operator norm in $SL_2(\mathbb{C})$ we have

$$|a|^2 + |b|^2 = \|B^T e_1\|^2 \leq \|B\|^2 \leq e^{2u} \tag{3.10}$$

analogous $|c|^2 + |d|^2 \leq e^{2u}$ thus for $u \leq 0,5$ we have

$$\max\{|a|^2 + |b|^2, |d|^2 + |c|^2\} \leq e^{2u} \leq 1 + 4u$$

and thus

$$\max\{|a|, |b|, |c|, |d|\} \leq e^u \leq 1 + 2u.$$

So (3.8) and (3.9) are proved. From (3.10) we also have

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 \leq 2e^{2u}$$

therefore

$$|a - \overline{d}|^2 + |b + \overline{c}|^2 = |a|^2 + \ldots + |d|^2 - 2 \leq 2e^{2u} - 2 \leq 8u$$

for $u \leq 0,5$ and hence (3.7). It is reasonable to explain the meaning of (3.7). The conditions $||B|| \approx 1$ and $B \in SL_2(\mathbb{C})$ tell us that $B^*B \approx \mathrm{Id}$ and therefore

$$\begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix} = B^* \approx B^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Let now $\varepsilon > 0$ and assume that $s_v \leq \varepsilon$. From (3.6) we get

$$|\lambda|^2 + |\lambda^{-1}|^2 + |ty\delta|^2 \leq 2e^{2\varepsilon}$$

hence $|ty\delta|^2 \leq 2e^{2\varepsilon} - 2 \leq 8\varepsilon$ if ε is small enough. So $|ty\delta| \leq 2\sqrt{2\varepsilon}$. Now since $||PBP^{-1}|| \leq e^{\varepsilon}$ we have $|t^{-2}c| \leq 2$ as soon as $\varepsilon \leq \frac{1}{4}$. Hence $|yct^{-1}| \leq \frac{4\sqrt{2\varepsilon}}{|\delta|}$ and $\max\{|a|, |d|\} \leq 1 + 2\varepsilon + \frac{4\sqrt{2\varepsilon}}{|\delta|}$ Finally for some absolute constant $C > 0$ we have $|ad| \leq 1 + C(\varepsilon + \frac{\sqrt{\varepsilon}}{|\delta|} + \frac{\varepsilon}{|\delta|^2})$.

On the other hand, $|cy^2| = |t^{-2}c(ty)^2| \leq \frac{16\varepsilon}{|\delta|^2}$ and

$$|d - a||yt| \leq 2\max\{|a|, |d|\}|yt| \leq \frac{12\sqrt{2\varepsilon}}{|\delta|} + \frac{32\varepsilon}{|\delta|^2}$$

Also by (3.7) we have $|bt^2 + (d - a)yt - cy^2 + (\overline{t})^{-2}\overline{c}| \leq 2\sqrt{2\varepsilon}$ and

$$|bc + |t^{-2}c|^2| \leq 2|bt^2 + (\overline{t})^{-2}\overline{c}| \leq 4\sqrt{2\varepsilon} + \frac{24\sqrt{2\varepsilon}}{|\delta|} + \frac{96\varepsilon}{|\delta|^2},$$

and by (3.8) we have $|t^{-2}c|^2 \leq 1 + 4\varepsilon$ hence up to enlarging the absolute constant C we also have $|bc| \leq 1 + C(\sqrt{\varepsilon} + \frac{\sqrt{\varepsilon}}{|\delta|} + \frac{\varepsilon}{|\delta|^2})$.

Without the assumption that s_v is small, we can make a coarser estimate:

$|t^{-2}c|^2 \le 2e^{2s_v}, |ty\delta|^2 \le 2e^{2s_v}$, hence $|cyt^{-1}| \le \frac{4e^{4s_v}}{|\delta|}$ and

$$\max\{|a|,|d|\} \le \frac{4e^{4s_v}}{|\delta|} + 1 + 2s_v \le 4e^{4s_v}\max\{1, \frac{1}{|\delta|}\}$$

and $|ad| \le 16e^{16s_v}\max\{1, \frac{1}{|\delta|^2}\}$. Similarly, we compute $|bc| \le 20e^{16s_v}\max\{1, \frac{1}{|\delta|^2}\}$.

If v is finite and K_v is the corresponding completion, with ring of integers O_v and uniformizer π, we have $SL_2(K_v) = K_vA_vN_v$ where

- $K_v = SL_2(O_v)$,
- $A_v = \{\mathrm{diag}(\pi^n, \pi^{-n}), n \in \mathbb{Z}\}$,
- N_v is the subgroup of unipotent upper-triangular matrices with coefficients in K_v.

Hence, we also get a $P \in A_vN_v$ satisfying (3.6) with $y \in K_v$ and $t = \pi^n$ for some $n \in \mathbb{Z}$.

We first assume that v is finite. Recall that the operator norm in $SL_2(K_v)$ is given by the maximum modulus of each matrix coefficient. Hence we must have $|t^{-2}c|_v \le e^{s_v}$ and $|ty\delta|_v \le e^{s_v}$. It follows that $|cyt^{-1}|_v \le e^{2s_v}|\delta^{-1}|_v$ and hence $|a|_v \le \max\{e^{s_v}, e^{2s_v}|\delta^{-1}|_v\}$. Similarly, $|d|_v \le \max\{e^{s_v}, e^{2s_v}|\delta^{-1}|_v\}$. Hence $|ad|_v \le \max\{e^{2s_v}, e^{4s_v}|\delta^{-1}|_v^2\}$. Moreover $ad - bc = 1$, hence $|bc|_v \le \max\{1, |ad|_v\} \le \max\{e^{2s_v}, e^{4s_v}|\delta^{-1}|_v^2\}$. □

We now put together the local information obtained above to bound the heights. Let $n = [K : \mathbb{Q}]$ and V_f and V_∞ the set of finite and infinite places of K. Set ε_0, C_0 and C_∞ the constants from the previous lemma. For $A > 0$ and $x \in \overline{\mathbb{Q}}$ we set

$$h_\infty^A(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_\infty, |x|_v \ge A} n_v \log^+ |x|_v \tag{3.11}$$

where the sum is limited to those $v \in V_\infty$ for which $|x|_v \ge A$. We have:

Lemma 3.3.5 (Global estimates)**.** *For some constant C_2 satisfying $2 \le C_2 \le 2 + (2\log C_\infty + 16)/\log 2$, we have for all $\varepsilon_1 \in (0, \frac{1}{2})$ and all $\varepsilon \le \min\{\varepsilon_0, \varepsilon_1^2\}$*

$$\max\{h(ad), h(bc)\} \le C_{\varepsilon,\varepsilon_1} e(F) + 6C_0\frac{\sqrt{\varepsilon}}{\varepsilon_1} + 2h_f(\delta^{-1}) + C_2 h_\infty^{\varepsilon_1^{-1}}(\delta^{-1}) \tag{3.12}$$

where $C_{\varepsilon,\varepsilon_1} = (16 + \frac{2\log C_\infty}{\varepsilon} + \frac{2|\log \varepsilon_1|}{\varepsilon})$ *and* $\delta = \lambda + \lambda^{-1}$.

Proof. Recall that $s_v = \log E_v(F)$. If $v \in V_\infty$ and $s_v \geq \varepsilon$ then according to Lemma 3.3.4 we have $\log^+ |ad|_v \leq 2\log C_\infty + 16 s_v + 2\log^+ |\delta^{-1}|_v$ hence

$$\frac{1}{n}\sum_{v\in V_\infty, s_v\geq\varepsilon} n_v \log^+ |ad|_v$$
$$\leq \left(16 + \frac{2\log C_\infty}{\varepsilon}\right)\frac{1}{n}\sum_{v\in V_\infty, s_v\geq\varepsilon} n_v s_v + \frac{2}{n}\sum_{v\in V_\infty, s_v\geq\varepsilon} n_v \log^+ |\delta^{-1}|_v$$

Fix $\varepsilon_1 < \frac{1}{2}$. On the other hand, if $s_v \leq \varepsilon \leq \min\{\varepsilon_0, \varepsilon_1^2\}$ and $|\delta|_v \geq \varepsilon_1$ then $\log^+ |ad|_v \leq C_0(\sqrt{s_v} + \frac{\sqrt{s_v}}{|\delta|_v} + \frac{s_v}{|\delta|_v^2}) \leq 3C_0\frac{\sqrt{\varepsilon}}{\varepsilon_1}$ and, as $n_v \leq 2$,

$$\frac{1}{n}\sum_{v\in V_\infty, s_v\leq\varepsilon, |\delta|_v\geq\varepsilon_1} n_v \log^+ |ad|_v \leq 6C_0\frac{\sqrt{\varepsilon}}{\varepsilon_1}.$$

While if $s_v < \varepsilon$ and $|\delta|_v \leq \varepsilon_1 \leq \frac{1}{2}$ then $\log^+ |ad|_v \leq C_2 \log^+ |\delta^{-1}|_v$ for some absolute constant C_2 satisfying $2 \leq C_2 \leq 2 + \frac{(2\log C_1 + 16)}{\log 2}$, hence

$$\frac{1}{n}\sum_{v\in V_\infty, s_v<\varepsilon, |\delta|_v\leq\varepsilon_1} n_v \log^+ |ad|_v \leq \frac{1}{n}\sum_{v\in V_\infty, s_v\leq\varepsilon, |\delta|_v\geq\varepsilon_1} n_v C_2 \log^+ |\delta^{-1}|_v$$

When $v \in V_f$, from Lemma 3.3.4, we get

$$\sum_{v\in V_f} n_v \log^+ |ad|_v \leq \sum_{v\in V_f} 16 n_v s_v + \sum_{v\in V_f} 2n_v \log^+ |\delta^{-1}|_v.$$

But
$$\frac{2}{n}\sum_{v\in V_\infty, s_v\geq\varepsilon, |\delta|_v\geq\varepsilon_1} n_v \log^+ |\delta^{-1}|_v \leq \frac{2|\log\varepsilon_1|}{\varepsilon}\frac{1}{n}\sum_{v\in V_\infty, s_v\geq\varepsilon} n_v s_v.$$

Putting together the above estimates, we indeed obtain (3.12) for ad. The same computation works for bc. $\square$

Theorem 3.3.6 (The equidistribution of small points, Bilu [1997]). *Suppose* $(\lambda_n)_{n\geq 1}$ *is a sequence of algebraic numbers (i.e. in* $\overline{\mathbb{Q}}$*) such that* $h(\lambda_n) \to 0$ *and* $\deg(\lambda_n) \to +\infty$ *as* $n \to +\infty$*. Let* $O(\lambda_n)$ *be the Galois orbit of* λ_n *in* $\overline{\mathbb{Q}}$*. Then we* *have the following weak* convergence of probability measures on $\mathbb{C}$*

$$\frac{1}{\#O(\lambda_n)} \sum_{x \in O(\lambda_n)} \delta_x \longrightarrow^{w^*}_{n \to +\infty} d\theta \tag{3.13}$$

where $d\theta$ is the normalized Lebesgue measure on the unit circle $\{z \in \mathbb{C}, |z| = 1\}$.

We now draw two consequences of this equidistribution statement :

Lemma 3.3.7 (bounding errors terms via the equidistribution theorem I)**.** *For every $\alpha > 0$ there is $d_1, \nu_1 > 0$ and $\varepsilon_1 > 0$ with the following property. If $\lambda \in \overline{\mathbb{Q}}$ is such that $h(\lambda) \leq \nu_1$, $\deg(\lambda) \geq d_1$ then*

$$h_\infty^{\varepsilon_1^{-1}}\left(\frac{1}{1-\lambda}\right) \leq \alpha$$

where $h_\infty^{\varepsilon_1^{-1}}$ was defined in (8).

Proof. Consider the function

$$f_{\varepsilon_1}(z) = \mathrm{Id}_{|z-1|>\varepsilon_1} \log|1-z|.$$

It is locally bounded on $\mathbb{C}$. By Theorem 3.3.6, for every $\varepsilon_1 > 0$, there must exist $d_1, \eta_1 > 0$ such that, if $h(\lambda) \leq \eta_1$ and $\deg(\lambda) \geq d_1$ then

$$\left| \frac{1}{n} \sum_x f_{\varepsilon_1}(x) - \int_0^1 f_{\varepsilon_1}(e^{2\pi\imath\theta}) d\theta \right| \leq \frac{\alpha}{3}$$

On the other hand we verify that $\theta \mapsto \log|1 - e^{2\pi\imath\theta}|$ is in $L_1(0,1)$ and

$$\int_0^1 \log|1 - e^{2\pi\imath\theta}| d\theta = 0.$$

Hence we can choose $\varepsilon_1 > 0$ small enough so that

$$\left| \int_0^1 f_{\varepsilon_1}(e^{2\pi\imath\theta}) d\theta \right| \leq \frac{\alpha}{3}$$

thus now we have that

$$\left|\frac{1}{n}\sum_x f_{\varepsilon_1}(x)\right| \leq \frac{2\alpha}{3}. \tag{3.14}$$

Let $P \in \mathbb{Z}[X]$ be the minimal polynomial of λ, that is

$$P(X) = \sum_{0\leq i\leq n} a_i X^i = a_n \prod_{x\in O(\lambda)} (X - x).$$

As $P(1) \in \mathbb{Z}\backslash\{0\}$ we have $\log|P(1)| = \log|a_n| + \sum_{x\in O(\lambda)} \log|1-x| \geq 0$. So

$$\sum_{|1-x|\leq\varepsilon_1} \log\frac{1}{|1-x|} \leq \sum_{|1-x|>\varepsilon_1} \log|1-x| + \log|a_n|.$$

Recall that from (2.4) we have $h(\lambda) = \frac{1}{n}(\sum_{x\in O(\lambda)} \log^+|x| + \log|a_n|)$. Hence

$$\frac{1}{n}\sum_{|1-x|\leq\varepsilon_1} \log\frac{1}{|1-x|} \leq h(\lambda) + \frac{1}{n}\sum_{|1-x|>\varepsilon_1} \log|1-x|. \tag{3.15}$$

Combining inequality (3.14) and choosing $\eta_1 \leq \frac{\alpha}{3}$, we get

$$h_\infty^{\varepsilon_1^{-1}}\left(\frac{1}{1-\lambda}\right) \leq \alpha$$

□

Using the product formula and again applying the equidistribution theorem, we obtain a similar estimate for the finite places.

Lemma 3.3.8 (bounding errors terms via the equidistribution theorem II)**.** *For every $\alpha > 0$ there exists $\nu_0 > 0$ and $A_1 > 0$ such that for any $\lambda \in \overline{\mathbb{Q}}$ if $h(\lambda) \leq \nu_0$ and $d = \deg(\lambda) > A_1$, then*

$$h_f\left(\frac{1}{1-\lambda}\right) \leq 2\alpha. \tag{3.16}$$

Proof. We apply the product formula to $\mu = 1-\lambda$, which takes the form $h(\mu) = h(\mu^{-1})$ hence $h_f(\mu^{-1}) = h_\infty(\mu) - h_\infty(\mu^{-1}) + h_f(\mu)$. But $h_f(\mu) = h_f(1-\lambda) =$

$h_f(\lambda) \leq \eta_0$ and

$$h_\infty(\mu) - h_\infty(\mu^{-1}) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_\infty} n_v \log |\mu|_v$$
$$= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_\infty, |1-\lambda| \leq \varepsilon} n_v \log |1-\lambda|_v + \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_\infty, |1-\lambda| \geq \varepsilon} n_v \log |1-\lambda|_v \quad (3.17)$$

The first summand is estimated in Lemma 3.3.7 and the second summand is small because of Theorem 3.3.6. Hence (3.17) becomes small (for example $\leq \alpha$).

$$h_f(\mu) \leq \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_\infty} n_v \log |\mu|_v + h_f(\lambda) \leq \alpha + \eta_0 \leq 2\alpha.$$

□

Recall also the following result (which can also be deduced from the equidistribution theorem).

Theorem 3.3.9 (Zhang's theorem Zhang [1995])**.** *There exists an absolute constant $\alpha_0 > 0$ such that for any $x \in \overline{\mathbb{Q}}$, we have*

$$h(x) + h(1-x) > \alpha_0$$

unless $x \in \{0, -1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\}$.

Remark 3.3.10. *The constant α_0 is calculated explicitly by Zagier (see Zagier [1993]) and it is equal to $\frac{1}{2}\log(\frac{1}{2}(1+\sqrt{5})) = 0.2406\ldots$.*

Now we are ready to proof Proposition 3.3.3.

Proof of Proposition 3.3.3. Since

$$h_f\left(\frac{1}{\lambda - \lambda^{-1}}\right) \leq h_f(\lambda) + h_f\left(\frac{1}{1-\lambda^2}\right)$$

and similarly

$$h_\infty^A\left(\frac{1}{\lambda - \lambda^{-1}}\right) \leq h_\infty^A(\lambda) + h_\infty^A\left(\frac{1}{1-\lambda^2}\right),$$

it follows from the last two lemmas that we can find $\varepsilon_1 > 0$, $\nu > 0$ and $d_0 \in \mathbb{N}$ so that $2h_f(\delta^{-1}) + C_2 h_\infty^{\varepsilon_1^{-1}}(\delta^{-1}) \leq \frac{\beta}{3}$ as soon as $h(\lambda) \leq e(F) \leq \nu$ and $\deg(\lambda) \geq d_0$. Then choose ε so the $2C_1\frac{\sqrt{\varepsilon}}{\varepsilon} \leq \frac{\beta}{3}$ and finally take ν even smaller so that $C_{\varepsilon,\varepsilon_1,}\nu \leq \frac{\beta}{3}$. Now apply Lemma 3.3.5 and we are done. $\square$

And now using all results we proof Theorem 3.3.1.

Proof of Theorem 3.3.1. From the irreducibility of cyclotomic polynomials and Kronecker's theorem we have that for every $d_0 \in \mathbb{N}$ there is $\nu_0 > 0$ and $d_1 > 0$ such that if $h(\lambda) < \nu_0$ and λ is not a root of 1 of order at most d_1 then $\deg(\lambda) \geq d_0$. Let $\beta = \frac{\alpha_0}{2}$ where α_0 is given by Theorem 3.3.9. Proposition 3.3.3 yields $d_0 > 0$ and $\nu = \nu(\frac{\alpha_0}{2}) > 0$ such that $\max\{h(ad), h(bc)\} \leq \beta$ as soon as $e(\{Id, A, B\}) \leq \nu$ and $\deg(\lambda) \geq d_0$. By Lemma 3.3.2, if we have some nice $A, B \in F^{N(d_1)}$. Suppose that

$$e(F) \leq \frac{\min\{\nu, \nu_0\}}{N(d_1)}, \tag{3.18}$$

then $e(\{Id, A, B\}) \leq \min\{\nu, \nu_0\}$ and λ is not a root of 1 of order at most d_1. Hence $\deg(\lambda) \geq d_0$ and by Proposition 3.3.3, $h(ad) + h(bc) \leq 2\beta = \alpha_0$. Then according to Theorem 3.3.9, $bc \in \{0, -1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\}$ which is impossible by our choice of A, B (see Lemma 3.3.2). Thus we reached a contradiction. So the assumption (3.18) was not true. Therefore

$$e(F) \geq \frac{\min\{\nu, \nu_0\}}{N(d_1)} > 0$$

is the desired gap. This ends the proof of Theorem 3.3.1. $\square$

Here we are going to use our previous height estimates once again to show the following proposition. Observe that the minimal height $e(F)$ coincides with the infimum of $h(gFg^{-1})$ over all adelic points $g = (g_v)_v$.

Proposition 3.3.11 (Simultaneous quasi-symmetrization)**.** *There is an absolute constant $C > 0$ such that if F is a finite subset of $SL_2(\overline{\mathbb{Q}})$ generating a non-virtually solvable subgroup, then there is an element $g \in SL_2(\overline{\mathbb{Q}})$ such that $h(gFg^{-1}) \leq Ce(F) + C$.*

Proof. As we may replace F by a bounded power of it, Lemma 3.3.2 above allows us to assume that F contains a semisimple element. Let $F = \{Id, A, B_1, \dots, B_k\}$ with A semisimple. Conjugating by some $g \in SL_2(\overline{\mathbb{Q}})$ we may assume that A is in diagonal form and we write each B_i in the form (3.5) with entries a_i, b_i, c_i, d_i. Changing F into F^2 if necessary, we may assume that both b_1 and c_1 are not zero (otherwise F would be contained in the group of upper or lower triangular matrices). We may further conjugate F by the diagonal matrix $\mathrm{diag}(t, t^{-1})$, where $t \in \overline{\mathbb{Q}}$ is a root of $t^4 = c_1/b_1$ so as to ensure $b_1 = c_1$. Then

$$h(B_1) \leq h(a_1) + h(d_1) + 2h(b_1) + \log 2.$$

On the one hand, since $a_1d_1 - b_1c_1 = 1$ we have $b_1^2 = a_1d_1 - 1$ and

$$2h(b_1) = h(b_1^2) \leq h(a_1d_1) + \log 2 \leq 2e(\{A, B\}) + \log 2C_\infty.$$

On the other hand, by Lemma 3.3.4 applied to $\{A, B_i\}$ we have $\max\{|a_i|_v, |d_i|_v\} \leq C_v e^{2s_v} \max\{1, |\delta^{-1}|_v\}$ for every place v where $\delta = \lambda - \lambda^{-1}$ and $s_v = s_v(\{A, B_i\}) = \log E_v(\{A, B_i\})$. Applying Lemma 3.3.4 to $\{A, B_1B_i\}$ we get

$$\max\{|(B_1B_i)_{11}|_v, |(B_1B_i)_{22}|_v\} \leq C_v e^{2s_v} \max\{1, |\delta^{-1}|_v\}$$

with $s_v = s_v(\{A, B_1B_i\}) = \log E_v(\{A, B_1B_i\})$. We compute the matrix entry $(B_1B_i)_{11} = a_1a_i + b_1c_i$. We get

$$|c_i|_v = |((B_1B_i)_{11} - a_1a_i)b_1^{-1}|_v \leq C_v e^{2s_v} \max\{1, |\delta^{-1}|_v\} \max\{1, |b_1^{-1}|_v\}.$$

Similarly for $|b_i|_v$. Hence,

$$\begin{aligned} ||F||_v &\leq C_v \max_{i=1,\dots,k} \{|a_i|_v, |d_i|_v, |b_i|_v, |c_i|_v\} \\ &\leq C_v \max_{i=1,\dots,k} E_v(\{A, B_1, B_1B_i\})^2 \max\{1, |\delta^{-1}|_v\} \max\{1, |b_1^{-1}|_v\} \end{aligned}$$

In particular, this means that

$$h(F) \leq 2\log C_1 + 2e(F^2) + h(\delta) + h(b_1) \leq 7e(F) + 4\log 2C_\infty.$$

□

Corollary 3.3.12. *There exists a constant $C_{qs} > 0$ such that if F is as in the proposition, then there is an element $g \in SL_2(\overline{\mathbb{Q}})$ such that*

$$h(gFg^{-1}) \leq C_{qs} e(F).$$

Chapter 4

A Strong Tits Alternative for SL_2

Main result is proved in this chapter. First we find geometric conditions for "ping-pong" (see Lemma 4.1), on which geometric part of the proof of A strong Tits alternative for SL_2 4.2.1 is based. After using it and all technic for arithmetic part of the proof (developed earlier) A strong Tits alternative for SL_2 4.2.1 is proved.

4.1 Ping-pong

Here we state and prove a ping-pong criterion, which gives a sufficient condition on the finite set F for it, or a bounded power of it, to contain two free generators of a free subgroup.

Let k be a local field of characteristic zero with its standard absolute value. We set $C_k = 2$ if k is Archimedean ($\mathbb{R}$ or $\mathbb{C}$), and $C_k = 1$ if k is non Archimedean (finite extensions of the p-adic numbers $\mathbb{Q}_p$). Let $F \subset SL_2(k)$ be a finite set containing 1 such that $\Lambda_k(F^{k_1}) > C_k||F||_k$ (see Section 2.3 for notation, it is important to require a strict inequality here when k is non Archimedean). Let $k_1 \in \mathbb{N}$ be a positive integer and let $A \in F^{k_1}$ be such that $\Lambda_k(A) = \Lambda_k(F^{k_1})$. Then A is semisimple and admits two distinct eigenvectors v^+ and v^- in k_q^2 where k_q is either k or some quadratic extension of k. Since we may always replace k by k_q, there is no loss of generality in assuming that v^+ and v^- lie in k^2. Let d_k be the canonical (Fubini-Study) projective distance on $\mathbb{P}^1(k)$ namely

$$d_k(u,v) = \frac{||u \wedge v||_k}{||u||_k ||v||_k} \tag{4.1}$$

where by $\wedge$ we define usual wedge product. That is an antisymmetric variant of the tensor product. It is an associative, bilinear operation. Thus, for all $u, v \in V$ and $a, b, c, d \in k$, we have

$$(au + bv) \wedge (cu + dv) = (ad - bc) u \wedge v. \tag{4.2}$$

Lemma 4.1.1 (geometric conditions for ping-pong)**.** *Let $k_2, k_3 \in \mathbb{N}$ be two positive integers. Assume that there is $B \in F^{k_2}$ such that*

$$d_k(Bv^{\varepsilon}; v^{\varepsilon'}) \geq ||F||_k^{-k_3}, \tag{4.3}$$

$$d_k(v^{\varepsilon}; v^{\varepsilon'}) \geq ||F||_k^{-k_3} \tag{4.4}$$

for each $\varepsilon, \varepsilon' \in \{\pm\}$. Then A^l and BA^lB^{-1} generate a free subgroup of $SL_2(k)$ as soon as $l \geq (k_2+1)(k_3+1)$.

Proof. We will show that A^l and BA^lB^{-1} that satisfy (4.3) and (4.4) satisfy then the conditions of Lemma 2.1.9 and thus generate a free group.

Note that for all $u, v \in \mathbb{P}_1(k)$ we have

$$d_k(Bu, Bv) \leq ||B||^2 d_k(u,v)$$

for $B \in SL_2(k)$. Note also that when v is an eigenvector then γv for $\gamma \in k$ is an eigenvector too. Thus without loss of generality, we may assume that $||v^+||_k = ||v^-||_k = 1$. Let λ, λ^{-1} be the eigenvalues of A, where we have chosen $|\lambda|_k \geq 1$. By the assumption on A we have

$$|\lambda|_k = \Lambda_k(A) = \Lambda_k(F^{k_1}) > C_k ||F||_k \geq 1. \tag{4.5}$$

We may assume that v^+ corresponds to λ and v^- to λ^{-1}. Let $P \in GL_2(k)$ be defined by $Pe_1 = v^+$ and $Pe_2 = v^-$. Note that

$$|\det P| = ||v^+ \wedge v^-|| = \frac{||v^+ \wedge v^-||}{||v^+||||v^-||} = d_k(v^+, v^-). \tag{4.6}$$

Also $||P|| = 1$ if k is non Archimedean, and $||P||^2 \leq 2$ if k is Archimedean, so in general $||P||^2 \leq C_k$. Moreover using (4.6) and (4.4) we have

$$||P^{-1}|| = \frac{||P||}{|\det P|_k} \leq C_k^{\frac{1}{2}} ||F||^{k_3}. \tag{4.7}$$

Set $A' = P^{-1}AP, B' = P^{-1}BP$, and $F' = P^{-1}FP$. Then $A' = \mathrm{diag}(\lambda, \lambda^{-1})$. For $u, v \in \mathbb{P}_1(k)$ we have

$$d_k(Pu, Pv) = \frac{||Pu \wedge Pv||}{||Pu||||Pv||} \leq |\det P|||P^{-1}||^2 d_k(u, v) \leq \frac{C_k d_k(u, v)}{|\det P|}.$$

Hence for $i, j \in \{1, 2\}$ and taking into account (4.4) and (4.3) we get

$$d_k(B'e_i, e_j) \geq \frac{1}{C_k} d_k(v^+, v^-) d_k(BPe_i, Pe_j) \geq \frac{1}{C_k} \frac{1}{||F||^{2k_3}}. \tag{4.8}$$

By (4.7) we also have

$$||F'|| \leq ||F|| \frac{||P||^2}{|\det P|} \leq C_k ||F||^{k_3+1}.$$

Let $m \leq 2l$ be positive integers to be determined shortly below. Let

$$U_A^+ = \{x \in \mathbb{P}^1(k), d_k(x, e_1) \leq |\lambda|^{-2l}\},$$

$$U_A^- = \{x \in \mathbb{P}^1(k), d_k(x, e_2) \leq |\lambda|^{-2l}\},$$

$$U_C^+ = \{x \in \mathbb{P}^1(k), d_k(x, B'e_1) \leq |\lambda|^{-m}\},$$

$$U_C^- = \{x \in \mathbb{P}^1(k), d_k(x, B'e_2) \leq |\lambda|^{-m}\}.$$

In order to apply Lemma 2.1.9 we need to show that

- these four sets are disjoint,

- A'^l maps $(U_A^-)^c$ into U_A^+,
- A'^{-l} maps $(U_A^+)^c$ into U_A^-,
- $C' = B'A'^lB'^{-1}$ maps $(U_C^-)^c$ into U_C^+,
- C'^{-1} maps $(U_C^+)^c$ into U_C^-.

If for instance $U_A^+ \cap U_C^- \neq \emptyset$, then $d(B'e_i, e_j) \leq \frac{C_k}{|\lambda|^m}$ for some i, j, which in turn would contradict (4.8) since (4.5) gives $|\lambda|^m > C_k^2||F||^{2k_3}$ as soon as $m \geq 2k_3$. The same holds in other situations as soon as $m \geq 2(k_3+1)$.

Now since A' is diagonal, A'^l maps $(U_A^-)^c$ into U_A^+, and A'^{-l} maps $(U_A^+)^c$ into U_A^-. Finally let us check the last two conditions. If $x \in (U_C^-)^c$ then

$$d_k(x, B'e_2) > |\lambda|^{-m} \text{ and } d_k(B'^{-1}x, e_2)||B'||^2 > |\lambda|^{-m}.$$

So $B'^{-1}x \in (U_A^-)^c$ as long as $|\lambda|^{2l-m} \geq ||B'||^2$. Then $A'^lB'^{-1}x \in U_A^+$ and

$$d_k(C'x, B'e_1) \leq \frac{||B'||^2}{|\lambda|^{2l}} \leq |\lambda|^{-m}.$$

And similarly if $x \in (U_C^+)^c$.

So the above works as soon as

$$m \geq 2(k_3+1) \tag{4.9}$$

because we need that $|\lambda|^m > C_k^2||F||^{2(k_3+1)}$,

$$2l - m \geq 2k_2(k_3+1) \tag{4.10}$$

because we need that $|\lambda|^{2l-m} > C_k^{2k_2}||F||^{2k_2k_3+2k_2} \geq ||F'||^{2k_2} \geq ||B'||^2$.

Adding the inequalities (4.9) and (4.10) we have that $l \geq (k_2+1)(k_3+1)$. □

Remark 4.1.2. *A similar ping-pong lemma holds with the ping-pong players A^l and BA^lB (instead of BA^lB^{-1}) if we assume similar lower bounds on $d_k(B^\delta v^\varepsilon, v^{\varepsilon'})$ for $\delta \in \{0, \pm 1, \pm 2\}$ and $\varepsilon, \varepsilon' \in \{\pm\}$. This allows us to find the ping-pong players in some F^n, that is without having to take inverses of elements of F.*

4.2 A Strong Tits Alternative

First let us state Theorem 1.0.1 for SL_2 that will be proved here.

Theorem 4.2.1 (strong uniform Tits Alternative)**.** *There exists an absolute constant $N \in \mathbb{N}$ such that if K is any field and F a finite symmetric subset of $SL_2(K)$ containing 1 then either F^N contains two elements which generate a nonabelian free group, or the group generated by F is virtually solvable (i.e. contains a finite index solvable subgroup).*

We first assume that F has coefficients in $\overline{\mathbb{Q}}$.

We will show that if F generates a non virtually solvable subgroup of $SL_2(K)$ for some number field K then for at least one place $v \in V_K$ the conditions of the ping-pong Lemma 4.1.1 are satisfied, with k_1, k_2, and k_3 bounded and independent of K. This will be done by finding an appropriate prime and a place above it where F will satisfy the requirements of Lemma 4.1.1.

Let F be a finite subset of $SL_2(\overline{\mathbb{Q}})$ which generates a non virtually solvable subgroup and contains 1. According to Lemma 3.3.2, as one may change F into a bounded power of itself if necessary, we may assume that F contains two semisimple elements which generate a non virtually solvable subgroup. Now, from Corollary 3.3.12, after possibly conjugating F inside $SL_2(\overline{\mathbb{Q}})$ we may assume that $h(F) \leq C_{qs}e(F)$ where $C_{qs} > 0$ is the universal constant given by Corollary 3.3.12.

The last important ingredient in the proof of Theorem 4.2.1 is the product formula on the projective line $\mathbb{P}^1(\overline{\mathbb{Q}})$ (see [Bombieri and Gubler, 2006, 2.8.21]), that is for all $(u; v) \in \mathbb{P}^1(\overline{\mathbb{Q}})^2$

$$\prod_{v \in V_K} d_v(u,v)^{\frac{n_v}{[K:\mathbb{Q}]}} = \frac{1}{H(u)H(v)}. \tag{4.11}$$

Recall that

$$\log H(u) = h(u) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log ||(u_1,u_2)||_v$$

represent $u \in \mathbb{P}^1(K)$ if $(u_1,u_2) \in K^2$. This formula is straightforward from the usual product formula and the definition of the standard distance (see (4.1)) because

$$\log \prod_{v\in V_K} d_v(u,v)^{\frac{n_v}{[K:\mathbb{Q}]}}$$
$$= \frac{1}{[K:\mathbb{Q}]} \sum_{v\in V_K} n_v(\log \|u\wedge v\| - \log\|u\| - \log\|v\|) = -\log H(u) - \log H(v)$$
$$= \log \frac{1}{H(u)H(v)}. \quad (4.12)$$

Lemma 4.2.2. *Let $f(x) \in \overline{\mathbb{Q}}[x]$ and α be its root. Then*

$$h(\alpha) \le h(f) + \log \deg f.$$

Proof. Consider the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ then for α we have $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$.

$$\max\{1, |\alpha|_v^n\} \le \begin{cases} n|f|_v \max\{1, |\alpha|_v^{n-1}\}, \text{ if } v \text{ is archimedean;} \\ |f|_v \max\{1, |\alpha|_v^{n-1}\}, \text{ if } v \text{ is non-archimedean.} \end{cases}$$

Then we have

$$\max\{1, |\alpha|_v\} \le \begin{cases} n|f|_v \max\{1, |\alpha|_v\}, \text{ if } v \text{ is archimedean;} \\ |f|_v \max\{1, |\alpha|_v\}, \text{ if } v \text{ is non-archimedean.} \end{cases}$$

So $h(\alpha) \le h(f) + \log n$. □

Lemma 4.2.3 (Height of F controls heights of eigenobjects)**.** *Let $A \in SL_2(\overline{\mathbb{Q}})$ and $v \in \mathbb{P}^1(\overline{\mathbb{Q}})$ an eigendirection of A, then $h(v) \le h(A) + 2\log 2$.*

Proof.
$$(A - \lambda \mathrm{Id})v = \begin{bmatrix} a_{11}-\lambda & a_{12} \\ a_{21} & a_{22}-\lambda \end{bmatrix} v = 0$$

We take $v^T = (a_{12}, a_{11} - \lambda)$ and denote $\mu = \frac{a_{11}-\lambda}{a_{12}}$. Tacking into account that λ is an eigenvalue of A have

$$f(\mu) = a_{12}^2\mu^2 + a_{12}(a_{22} - a_{11})\mu - a_{12}a_{21} = 0.$$

By Lemma 4.2.2 we have $h(\mu) \leq h(f) + \log 2$.

Consider $f(x) = a_{12}x^2 + (a_{22} - a_{11})x - a_{21}$. We have

$$|f|_v \leq \begin{cases} \max\{1, \|A\|_v\}, \text{ if } v \text{ is non-archimedean;} \\ \max\{1, \sqrt{2}\|A\|_v\}, \text{ if } v \text{ is archimedean.} \end{cases}$$

Therefore we have $h(f) \leq h(A) + \frac{1}{2}\log 2$ We can take $v^T = (1, \mu)$ and thus

$$\|f\|_v \leq \begin{cases} \max\{1, \|\mu\|_v\}, \text{ if } v \text{ is non-archimedean;} \\ \sqrt{1 + |\mu|_v^2}, \text{ if } v \text{ is archimedean.} \end{cases}$$

Therefore we have $h(v) \leq h(\mu) + \frac{1}{2}\log 2$. Collecting together all inequalities we have $h(v) \leq h(A) + 2\log 2$ □

Let us introduce some notation. Suppose $A \in SL_2(\overline{\mathbb{Q}})$ is semisimple with eigendirections v_A^+ and v_A^- in $\mathbb{P}^1(\overline{\mathbb{Q}})$ and suppose $B \in SL_2(\overline{\mathbb{Q}})$. Then, assuming A and B have coefficients in a number field K, we set for each place $v \in V_K$:

$$\delta_v^{+,-}(B, A) = \log \frac{1}{d_v(Bv_A^+, v_A^-)}$$

where d_v is the standard distance on $\mathbb{P}^1(K_v)$ and K_v is the completion of K at v. Note that as $d_v \leq 1$ we have $\delta_v^{+,-}(B, A) \geq 0$. If $d_v(Bv_A^+, v_A^-) = 0$ we set $\delta_v^{+,-}(B, A) = 0$. We define similarly $\delta_v^{+,+}(B, A), \delta_v^{-,+}(B, A)$, and $\delta_v^{-,-}(B, A)$ in the obvious manner and we set

$$\delta_v(B, A) = \delta_v^{+,-}(B, A) + \delta_v^{+,+}(B, A) + \delta_v^{-,+}(B, A) + \delta_v^{-,-}(B, A).$$

For a finite subset F of $SL_2(\overline{\mathbb{Q}})$, we also define

$$\delta_v(F) = \sum \delta_v(\mathrm{Id}, A) + \delta_v(B, A)$$

where the sum runs over all pairs (A, B) of elements of F with A semisimple and B in "nice position". with respect to A; namely such that $Bv_A^+ \notin \{v_A^+, v_A^-\}$ and $Bv_A^- \notin \{v_A^+, v_A^-\}$. If this set of pairs is empty we set δ to be 0. However, in our case, it will be non empty if not for F itself then for a bounded power of it (see Lemma 4.2.5 below). We also define the corresponding global quantity:

$$\delta^{+,-}(B,A) = \frac{1}{[K:\overline{\mathbb{Q}}]} \sum_{v \in V_K} n_v \delta_v^{+,-}(B,A),$$

$$\delta(B,A) = \frac{1}{[K:\overline{\mathbb{Q}}]} \sum_{v \in V_K} n_v \delta_v(B,A),$$

and

$$\delta(F) = \frac{1}{[K:\overline{\mathbb{Q}}]} \sum_{v \in V_K} n_v \delta_v(F).$$

Proposition 4.2.4 (Height of F controls adelic distance between eigenobjects)**.** *With the above notation, for every $B \in SL_2(\overline{\mathbb{Q}})$ in nice position with respect to a semisimple $A \in SL_2(\overline{\mathbb{Q}})$ (or for $B = \mathrm{Id}$), we have*

$$\delta(B,A) \leq 8h(A) + 4h(B) + 16log2$$

In particular for any finite subset F in $SL_2(\overline{\mathbb{Q}})$

$$\delta(F) \leq 12|F|^2(2h(F) + 3log2).$$

Proof. From the product formula (4.11) above we have

$$\begin{aligned} \delta^{+,-}(B,A) = \frac{1}{[K:\overline{\mathbb{Q}}]} \sum_{v \in V_K} n_v \delta_v^{+,-}(B,A) &= \frac{1}{[K:\overline{\mathbb{Q}}]} \sum_{v \in V_K} n_v \log \frac{1}{d_v(Bv_A^+, v_A^-)} \\ &= \frac{1}{[K:\overline{\mathbb{Q}}]} \sum_{v \in V_K} n_v \log d_v(Bv_A^+, v_A^-) = h(Bv_A^+) + h(v_A^-). \end{aligned}$$

On the other hand, we easily compute

$$\begin{aligned} h(Bv_A^+) = \frac{1}{[K:\overline{\mathbb{Q}}]} &\sum_{v \in V_K} n_v \log \|Bv_A^+\|_v \\ &\leq \frac{1}{[K:\overline{\mathbb{Q}}]} \sum_{v \in V_K} n_v (\log \|B\|_v + \log \|v_A^+\|_v) \leq h(B) + h(v_A^+). \end{aligned}$$

From Lemma 4.2.3, we get

$$\delta^{+,-}(B,A) \leq h(B) + 2h(v_A^+) \leq h(B) + 2h(A) + 4\log 2.$$

Note that analogous estimation holds for every $\delta^{\pm,\pm}(B,A)$. Now taking into account that

$$\delta(B,A) = \delta^{+,-}(B,A) + \delta^{+,+}(B,A) + \delta^{-,+}(B,A) + \delta^{-,-}(B,A).$$

we obtain desired bounds. Also we have

$$\begin{aligned}\delta_v(F) = \sum \delta_v(\mathrm{Id},A) + \delta_v(B,A) \\ \leq \sum 4h(\mathrm{Id}) + 8h(A) + 16\log 2 + 4h(B) + 8h(A) + 16\log 2 \\ \leq 12|F|^2(2h(F) + 3log2).\end{aligned}$$

□

Lemma 4.2.5. *There is an integer $n_0 \geq 2$ such that if F is a finite subset of $SL_2(\mathbb{C})$ containing 1 and generating a non virtually solvable group, then for any semisimple $A \in F$ there exists $B \in F^{n_0}$ which is in nice position with respect to A.*

Proof. This is another occurrence of the escape trick described in Lemma 2.5.6. The subvarieties

$$X_A = \{B \in GL_2, Bv_A^+ \in \{v_A^\pm\} \text{ or } Bv_A^- \in \{v_A^\pm\}\}$$

are conjugate to each other in GL_2. The group generated by F clearly can not be contained in any $X_A(\mathbb{C})$ otherwise it would be virtually solvable. Thus by Lemma 2.5.6 there is N such that for each semisimple A in F, F^N is not contained in $X_A(\mathbb{C})$. □

Note that since we assume that F generates a non virtually solvable group, then according to Theorem 1.2, $h(F) \geq e(F) \geq \varepsilon$ for some fixed ε. Therefore, there exists a constant $D_{qs} > 0$ such that

$$\delta(F) \leq D_{qs}|F|^2 h(F).$$

We have for all $n \in \mathbb{N}$

$$\delta(F^n) \leq D_{qs}|F^n|^2 h(F^n) \leq D_{qs}|F|^{2n} n h(F)$$

We may write with obvious notation

$$\delta = \sum_{p \in \{\infty\} \cup \mathcal{P}} \delta_p = \delta_\infty + \delta_f$$

We fix $n = n_0$ as in Lemma 4.2.5 and let $D'_{qs} = D_{qs} n_0$ so that $\delta(F^{n_0}) \leq D'_{qs}|F|^{2n_0} h(F)$ and $h(F) \leq C_{qs} e(F)$. For each $p \in \{\infty\} \cup \mathcal{P}$ we set $e_p = e_p(F)$, $h_p = h_p(F)$ and $\delta_p = \delta_p(F^{n_0})$.

Claim : There exists a constant $C'' > 0$ such that for any set F in $SL_2(\overline{\mathbb{Q}})$ containing 1 and generating a non virtually solvable subgroup, there exist $p \in \{\infty\} \cup \mathcal{P}$ and a place $v|p$ such that, $\max\{\delta_v, h_v\} \leq C''|F|^{2n_0} e_v$ and $e_v > \frac{e_p}{2}$. Moreover if $p = \infty$, we may assume that $e_\infty \geq \frac{1}{2}e$.

We now prove this claim. Suppose first that $e_\infty \geq \frac{1}{2}e$, then

$$\delta_\infty + h_\infty \leq C_{qs}(D'_{qs}|F|^{2n_0} + 1)e_\infty.$$

We also have

$$e_\infty = \frac{1}{[K:\mathbb{Q}]}\left(\sum_{v \in V_\infty^+} n_v e_v + \sum_{v \in V_\infty^-} n_v e_v\right) \leq \frac{1}{[K:\mathbb{Q}]}\sum_{v \in V_\infty^+} n_v e_v + \frac{e_\infty}{2}$$

where $V_\infty^+ = \{v \in V_\infty, e_v \geq \frac{e_\infty}{2}\}$. Therefore

$$e_\infty \leq \frac{2}{[K:\mathbb{Q}]}\sum_{v \in V_\infty^+} n_v e_v$$

Hence

$$\sum_{v\in V_\infty^+} n_v(\delta_v+h_v) \leq 4C_{qs}(D'_{qs}|F|^{2n_0}+1)\sum_{v\in V_\infty^+} n_v e_v.$$

So for at least one $v \in V_\infty^+$ we have

$$\max\{\delta_v, h_v\} \leq \delta_v + h_v \leq 4C_{qs}(D'_{qs}|F|^{2n_0}+1)e_v.$$

Now suppose $e_\infty = \frac{e}{2}$, then

$$e_f = \frac{e}{2} > 0 \text{ and } \sum_{p\in\mathcal{P}} \delta_p + h_p \leq 2C_{qs}(D'_{qs}|F|^{2n_0}+1)\sum_{p\in\mathcal{P}} e_p$$

hence there must be one $p \in \mathcal{P}$ for which

$$e_p > 0 \text{ and } \delta_p + h_p \leq 2C_{qs}(D'_{qs}|F|^{2n_0}+1)e_p.$$

As this is an average over the places $v|p$ as before there must be some place $v|p$ for which

$$e_v \geq \frac{e_p}{2} \text{ and } \max\{\delta_v, h_v\} \leq \delta_v + h_v \leq 4C_{qs}(D'_{qs}|F|^{2n_0}+1)e_v.$$

So we have justified the claim.

End of the proof of Theorems 4.2.1. Let us recall what we have so far. We started with a set F in $SL_2(\overline{\mathbb{Q}})$ containing 1 and generating a non virtually solvable subgroup. We found the constant $n_0 \geq 2$ as in Lemma 4.2.5. We also found a constant C'' such that for some prime p and a place $v|p$ one has $\max\{\delta_v(F^{n_0}), h_v(F)\} \leq C''|F|^{2n_0}e_v(F)$ and $e_v(F) \geq \frac{1}{4}e_p(F) > 0$ (with $e_\infty \geq \frac{e}{2}$ in case $p = \infty$). Set $D''_F := C''|F|^{2n_0}$.

Suppose first that $v \in V_f$. Recall that we had $\Lambda_v(F^2) \geq E_v(F)^2$ by Lemma 3.1.9. Let $A_0 \in F^2$ be such that $\Lambda_v(A_0) = \Lambda_v(F^2)$. Then

$$\Lambda_v(A_0) \geq E_v(F)^2 \geq ||F||_v^{\frac{2}{D''_F}} > 1$$

and hence if $k_1 \in \mathbb{N}$ is the first even integer strictly larger that D''_F, we have $\Lambda_v(A) > ||F||_v$ if $A = A_0^{\frac{k_1}{2}} \in F^{k_1}$. Moreover we have $\delta_v(F^{n_0}) \leq D''_F e_v(F)$

therefore for every $B \in F^{n_0}$ which is in nice position with respect to A_0 (and there are such B's according to Lemma 4.2.5) we have

$$\delta_v(\mathrm{Id}, A_0) + \delta_v(B, A_0) \leq D''_F e_v(F).$$

Fix one such B. We have

$$d_v(Bv_A^{\varepsilon}, v_A^{\varepsilon'}) \geq E_v(F)^{-D''_F} \geq ||F||_v^{-D''_F}$$

and also

$$d_v(v_A^{\varepsilon}; v_A^{\varepsilon'}) \geq E_v(F)^{-D''_F} \geq ||F||_v^{-D''_F}$$

for all $\varepsilon, \varepsilon' \in \{\pm\}$. Therefore we are in a position to apply the ping-pong lemma 4.1.1 to the pair A and B with k_1 as above $(\leq D''_F + 2), k_2 = n_0$ and $k_3 = D''_F$. This ends the proof in the case when $v \in V_f$.

Suppose now that $v \in V_\infty$. We have $E_v(F) \geq \exp(\frac{\varepsilon}{2}) \geq \exp(\frac{\varepsilon}{2})$ where ε is the constant from Theorem 3.3.1 Now Lemma 3.1.16 shows that there is a constant $n_1 = n_1(\varepsilon) \in \mathbb{N}$ such that $E_v(F^{n_1}) \geq \frac{2}{c^2}$ where c is the constant in Lemma 3.1.9 Then by Lemma 3.1.9

$$\Lambda_v(F^{2n_1}) \geq c^2 E_v(F^{n_1})^2 \geq 2E_v(F^{n_1}) \geq 2E_v(F) \geq 2||F||^{\frac{1}{D''_F}}.$$

Observe that after possibly changing n_0 we may assume that it is larger than $2n_1$. Pick $A_0 \in F^{2n_1}$ such that $\Lambda_v(A_0) = \Lambda_v(F^{2n_1})$. Finally if k'_1 is the smallest integer strictly larger than D''_F, we set $A = A_0^{k'_1} \in F^{k_1}$ where $k_1 = 2n_1 k'_1$. We have $\Lambda_v(A) > 2||F||_v$. Moreover $\delta_v(F^{n_0}) \leq D''_F e_v(F)$ therefore for every $B \in F^{n_0}$ which is in nice position with respect to A_0 (and there are such B's according to Lemma 4.2.5) we have

$$\delta_v(\mathrm{Id}, A_0) + \delta_v(B, A_0) \leq D''_F e_v(F).$$

Fix one such B. We have

$$d_v(Bv_A^{\varepsilon}; v_A^{\varepsilon'}) \geq E_v(F)^{-D''_F} \geq ||F||_v^{-D''_F}$$

and also

$$d_v(v_A^{\varepsilon}, v_A^{\varepsilon'}) \geq E_v(F)^{-D_F''} \geq ||F||_v^{-D_F''}$$

for all $\varepsilon, \varepsilon' \in \{\pm\}$. Therefore we are in a position to apply the ping-pong lemma 4.1.1 to the pair A and B with k_1 as above ($\leq 2n_1(D_F''+1)$), $k_2 = n_0$ and $k_3 = D_F''$.

There are several ways to see that Theorem 4.2.1 for $SL_2(\overline{\mathbb{Q}})$ imply the same theorem for $SL_2(\mathbb{C})$. One can use the remark made in the introduction that both results are equivalent to a countable union of assertions expressible in first order logic. By elimination of quantifiers for algebraically closed fields, we know that two algebraically closed fields of the same characteristic satisfy the same statements of first order logic (see [Fried and Jarden, 2005, chp. 9]). Hence the validity of Theorems 4.2.1 over $\overline{\mathbb{Q}}$ is equivalent to its validity over $\mathbb{C}$.

References

Gilbert Baumslag, Benjamin Fine, Charles F.III Miller, and Douglas Troeger. Virtual properties of cyclically pinched one-relator groups. **Int. J. Algebra Comput.**, 19(2):213–227, 2009. doi: 10.1142/S0218196709005032. 4

Yuri Bilu. Limit distribution of small points on algebraic tori. **Duke Math. J.**, 89(3):465–476, 1997. doi: 10.1215/S0012-7094-97-08921-3. 33

Yuri F. Bilu, Yann Bugeaud, and Maurice Mignotte. **The Problem of Catalan.** Springer . 9

Enrico Bombieri and Walter Gubler. **Heights in Diophantine geometry.** New Mathematical Monographs 4. Cambridge: Cambridge University Press. xvi, 652 p., 2006. doi: 10.2277/0511138091. 12, 44

Emmanuel Breuillard. **A strong Tits alternative.** preprint, http://www.math.u-psud.fr/ breuilla/NewUT7.pdf , 2008a. 1, 20, 21, 24, 28

Emmanuel Breuillard. **A height gap theorem for finite subsets of GL(n,Q) and non amenable subgroups.** preprint, 2008b. 1, 26

Emmanuel Breuillard. **Heights on SL(2) and free subgroup.** to appear in Bob Zimmer's Festschrift, Chicago Univ. Press, 2011. 1, 15

Alex Eskin, Shahar Mozes, and Hee Oh. On uniform exponential growth for linear groups. **Invent. Math.**, 160(1):1–30, 2005. doi: 10.1007/s00222-004-0378-z. 5, 12

Michael D. Fried and Moshe Jarden. **Field arithmetic. 2nd revised and enlarged ed.** Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge 11. Berlin: Springer. xxii, 780 p., 2005. 52

N. Gill. **Growth in groups III: escape.** http://www.maths.bris.ac.uk/ manpg/escape.pdf. 13

Rostislav I. Grigorchuk. On growth in group theory. Proc. Int. Congr. Math., Kyoto/Japan 1990, Vol. I, 325-338 (1991)., 1991. 4

Rotislav Grigorchuk and Pierre de la Harpe. Limit behaviour of exponential growth rates for finitely generated groups. Ghys, Étienne (ed.) et al., Essays on geometry and related topics. Mémoires dédiés à André Haefliger. Vol. 2. Genève: L'Enseignement Mathématique. Monogr. Enseign. Math. 38, 351-370 (2001)., 2001. 1

Serge Lang. **Fundamentals of Diophantine geometry.** New York etc.: Springer-Verlag. XVIII, 370 p. DM 132.00; $ 51.30 , 1983. 8

A. Schinzel. **Polynomials with special regard to reducibility.** Encyclopedia of Mathematics and Its Applications. 77. Cambridge: Cambridge University Press. ix, 558 p. , 2000. 13

Jacques Tits. Free subgroups in linear groups. **J. Algebra**, 20:250–270, 1972. doi: 10.1016/0021-8693(72)90058-0. 6

Michel Waldschmidt. **Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables.** Grundlehren der Mathematischen Wissenschaften. 326. Berlin: Springer. xxiii, 633 p. DM 169.00; öS 1234.00; sFr. 153.00, 2000. 12

D. Zagier. Algebraic numbers close to both 0 and 1. **Math. Comp.**, 61(203): 485–491, 1993. ISSN 0025-5718. doi: 10.2307/2152970. URL `http://dx.doi.org/10.2307/2152970`. 36

Shouwu Zhang. Small points and adelic metrics. **J. Algebr. Geom.**, 4(2): 281–300, 1995. 36