It suffices to prove the Uniform Tits alternative over $\bar{\mathbb{Q}}$

Florent Martin

These are notes of a talk I gave for the lectures *Linear groups and heights* hold by Walter Gubler and Clara Löh in Regensburg during the winter term 2015-2016. The goal of the this talk is to explain in details the reduction of the Uniform Tits alternative from $\mathbb{C}$ to $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, following [3, § 3.1] and [2, § 9].

Contents

Introduction

We are interested in the following result.

Theorem (UTA: Uniform Tits alternative)**.** *For any $d \in \mathbb{N}$ there exists $N(d) \in \mathbb{N}$ such that if K is an algebraically closed field of characteristic 0, $S \subset GL_d(K)$ is a finite symmetric set with $1 \in S$, then*

- *either $\langle S \rangle$ is virtually solvable*
- *or $S^{N(d)}$ contains a generator of a free group with two generators: $F_2 \subset \langle S \rangle$.*

Let us consider the following weaker statement.

Theorem ($UTA(\bar{\mathbb{Q}})$)**.** *For any $d \in \mathbb{N}$ there exists $N(d) \in \mathbb{N}$ such that if $S \subset GL_d(\overline{\mathbb{Q}})$ is a finite symmetric set with $1 \in S$, then*

- *either $\langle S \rangle$ is virtually solvable*
- *or $S^{N(d)}$ contains a generator a a free group with two generators: $F_2 \subset \langle S \rangle$.*

The aim of this lecture is to prove

Proposition. ***2.1***

$$UTA(\bar{\mathbb{Q}}) \Rightarrow UTA.$$

There will be three main ingredients in the proof.

Proposition. ***1.8*** *Let Φ be a first order sentence. If K and K' any algebraically closed fields of characteristic* 0

$$K \models \Phi \quad \textit{if and only if} \quad K' \models \Phi.$$

Proposition. ***cf. Section 2.*** *UTA can be expressed with first order sentences.*

To prove this fact, we will need:

Proposition. *3.1 For each integer d, there exists an integer $c(d) > 0$ such that if K is a field of characteristic 0, for every subgroup $G \subseteq GL_d(K)$, G is virtually solvable if and only if there exists $P \in GL_d(K)$ such that*

$$\left(G : (G \cap (P\mathbb{T}_d(K)P^{-1}))\right) \leq c(d)$$

where $\mathbb{T}_d(K)$ is the group of invertible upper triangular $d \times d$ matrices.

1 First order logic

We refer to [5, chapter 1] for this section. The goal of this section is to explain proposition 1.8. We fix a countable set of variables $\mathcal{V} = \{a, a_1, a_2, \dots, b, b_1, b_2, \dots, z, z_1, z_2, \dots, \}$.

1.1 Definition. An atomic formula Φ is an expression of the form

$$f_1 = f_2$$

where $f_1, f_2 \in \mathbb{Z}[a, a_1, a_2, \dots, b, b_1, b_2, \dots, z, z_1, z_2, \dots]$.

1.2 Definition. The set of formulas is the smallest set $\mathcal{F}$ such that

i) $\mathcal{F}$ contains the atomic formulas.

ii) If $\Phi \in \mathcal{F}$, then $\neg\Phi \in \mathcal{F}$.

iii) If $\Phi, \Psi \in \mathcal{F}$, then $\Phi \wedge \Psi$, $\Phi \vee \Psi$, $\Phi \Rightarrow \Psi$ and $\Phi \Leftrightarrow \Psi$ are in $\mathcal{F}$.

iv) If $\Phi \in \mathcal{F}$ then for any variable $\omega \in \mathcal{V}$,

- $\exists\omega\ \Phi$ is in $\mathcal{F}$
- $\forall\omega\ \Phi$ is in $\mathcal{F}$.

We will write $f_1 \neq f_2$ in place of $\neg(f_1 = f_2)$. The notation $\forall\omega, \omega'$ (resp. $\exists\omega, \omega'$) will be used to denote $\forall\omega\ \forall\omega'$ (resp. $\exists\omega\ \exists\omega'$). We will use brackets in formula to avoid ambiguity.

1.3 Definition. If Φ is a formula and ω a variable, we say that ω is a free variable of Φ if ω occurs in Φ not in the scope of a quantifier $\exists\omega$ or $\forall\omega$. We say that ω is a bound variable if ω occurs in the scope of a quantifier $\exists\omega$ or $\forall\omega$. We say that Φ is a sentence if it has no free variables.

If Φ is a formula, we write $\Phi(\omega_1, \dots, \omega_n)$ to express the fact that the set of free variables of Φ is contained in $\{\omega_1, \dots, \omega_n\}$.

Remark. Let Φ be the formula $(x + y = 0) \wedge (\exists x\ x^2 = y)$. Then x is at the same time free and bound. We want to avoid this. However, we might replace Φ by the equivalent formula $(x_1 + y = 0) \wedge (\exists x_2\ x_2^2 = y)$ where this problem disappears. We will tacitly restrict to such formulas, where a variable is not at the same time free and bound.

1.4 Example.

$$\begin{aligned}
\Phi_0(x) &= \exists y(xy = 1)\\
\Phi_1 &= \ \forall x, y\ (x + y = y + x)\\
\Phi_2(x) &= \ \exists a\ (a^2 = x)\\
\Phi_3 &= \ \forall x\ \exists a\ (a^2 = x)\\
\Phi_4 &= \ \forall p \forall q\ \left((4p^3 + 27q^2 \neq 0) \Rightarrow \exists x_1, x_2, x_3\ (x_1^3 + px_1 + q = 0 \wedge x_2^3 + px_2 + q = 0 \wedge x_3^3 + px_3 + q = 0\right.\\
&\quad \left. \wedge x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3)\right).
\end{aligned}$$

In Φ_1, x, y are bound variables, in Φ_2, a is bound and x is free, in Φ_3, x, a are bound, in Φ_4, p, q, x_1, x_2 are bound.

1.5 Definition. Let $\Phi(\omega_1, \dots, \omega_n)$ be a formula whose free variables are contained in $\{\omega_1, \dots, \omega_n\}$. Let K be a field and let $\underline{\lambda} = (\lambda_1, \dots, \lambda_n) \in K^n$. We define

$$K \models \Phi(\underline{\lambda})$$

(to be read *the field K satisfies the formula Φ at* $(\lambda_1, \dots, \lambda_n)$) inductively on the formula Φ.

i) If Φ is the atomic formula $f_1 = f_2$ then $K \models \Phi(\underline{\lambda})$ if and only if the equality

$$f_1(\underline{\lambda}) = f_2(\underline{\lambda})$$

holds in K.

ii) If $\Phi = \neg\Psi$ then $K \models \Phi(\underline{\lambda})$ if $K \models \Psi(\underline{\lambda})$ does not hold.

iii) If Φ is equal to $\Psi_1 \wedge \Psi_2$ then $K \models \Phi(\underline{\lambda})$ if and only if $K \models \Psi_1(\underline{\lambda})$ and $K \models \Psi_2(\underline{\lambda})$. Similarly for $\vee, \Rightarrow, \Leftrightarrow$.

iv) If Φ is the formula $\exists x \Psi(\omega_1, \dots, \omega_n, x)$ then $K \models \Phi(\underline{\lambda})$ if and only if there exists an element $\alpha \in K$ such that $K \models \Psi(\underline{\lambda}, \alpha)$.

v) If Φ is the formula $\forall x \Psi(\omega_1, \dots, \omega_n, x)$ then $K \models \Phi(\underline{\lambda})$ if and only if for all elements $\alpha \in K$ it is true that $K \models \Psi(\underline{\lambda}, \alpha)$.

We write $K \not\models \varphi(\underline{\lambda})$ when $K \models \varphi(\underline{\lambda})$ does not hold.

1.6 Example. i) For any field K one has $K \models \Phi_1$. Indeed Φ_1 just says *the additive law of K is commutative* which is true in fields.

ii) Given $\alpha \in K$, $K \models \Phi_2(\alpha)$ if and only if α is a square root in K. For instance $\mathbb{Q} \not\models \Phi_2(3)$, $\mathbb{R} \models \Phi_2(3)$, $\mathbb{R} \not\models \Phi_2(-1)$, $\mathbb{C} \models \Phi_2(-1)$.

iii) One has $K \models \Phi_3$ if and only if all elements of K have a square root. For instance

(a) $K \models \Phi_3$ for

$$K = \bar{\mathbb{Q}}, \mathbb{C}, \bigcup_{n \geq 1} \mathbb{F}_{p^{2^n}} \dots$$

(b) $K \not\models \Phi_3$ for

$$K = \mathbb{Q}, \mathbb{R}, \mathbb{F}_{p^n}, \mathbb{Q}_p, \mathbb{C}(T) \dots$$

iv) The formula Φ_4 expresses the property that any degree 3 polynomial P whose discriminant is nonzero has at least three distinct roots. One deduce from this that $K \models \Phi_4$ if and only if any degree 3 polynomial in K has a root. In particular all algebraically closed fields satisfy Φ_4.

1.7 Example. The property $\mathcal{Q}$ "*for any elliptic curve $\mathcal{E}$ defined over K, the group $\mathcal{E}[7](K)$ of 7-torsion K-rational points has cardinality* 49" is a first order property. First remind that given a, b in K such that $4a^3 + 27b^2 \neq 0$, one can associate an elliptic curve $\mathcal{E}_{a,b}$ defined by the equation in x, y

$$y^2 = x^3 + ax + b.$$

There is a group law defined on $\mathcal{E}_{a,b}(K) \cup \infty$ where ∞ is the point at infinity of $\mathcal{E}_{a,b}$, and this group law is defined by polynomials with coefficients in $\mathbb{Q}(a, b)$. It follows from this that there exists a first order formula $\Phi(a, b, x, y)$ such that for $\alpha, \beta, \gamma, \delta \in K$

$$K \models \Phi(\alpha, \beta, \gamma, \delta)$$

if and only if $\mathcal{E}_{\alpha,\beta}$ is an elliptic curve, and $(\gamma, \delta) \in \mathcal{E}_{\alpha,\beta}[7](K)$. Hence the property $\mathcal{Q}$ can be expressed by the formula

$$\Psi = \forall a, b \Big(4a^3 + 27b^2 \neq 0 \Rightarrow \Big(\exists x_1, \dots, x_{48}, y_1, \dots, y_{48} \\ \Big(\bigwedge_{i=1 \dots 48} \Phi(a, b, x_i, y_i) \wedge (\forall x, y \; \Phi(a, b, x, y) \Rightarrow \bigvee_{i=1 \dots 48} x = x_i \wedge y = y_i \Big)\Big)\Big)$$

1.8 Proposition (3.2.2 [5])**.** *Let Φ be a first order sentence. Then if K and K' any algebraically closed fields of characteristic* 0

$$K \models \Phi \quad \textit{if and only if} \quad K' \models \Phi.$$

1.9 Corollary. *Let Φ be a first order sentence. If $\bar{\mathbb{Q}} \models \Phi$, then for all algebraically closed field K of characteristic* 0*, one has $K \models \Phi$.*

Let us make some remarks about this statement.

1. According to example 1.7, the property saying that the group $\mathcal{E}[7](K)$ of 7-torsion K-rational points of an elliptic curve is order 49 is a first order property. When $K = \mathbb{C}$, a classical result of complex elliptic curves says that $(\mathcal{E}(\mathbb{C}), +) \simeq (C/(\mathbb{Z} + \tau\mathbb{Z})$ for some τ with $\Im(\tau) > 0$. In this case it is easy to check that
$$\mathcal{E}(\mathbb{C})[7] = \{\frac{i}{7} + \tau\frac{i}{7} \mid 0 \leq i, j < 7,\ i, j \in \mathbb{N}\}$$
which has cardinality 49 indeed. So $\mathbb{C} \models \Psi$. Applying proposition 1.8 we deduce that for any field K of characteristic 0 which is algebraically closed, $K \models \Psi$. In other words, for any field K of characteristic zero and $\mathcal{E}$ an elliptic curve defined over K, $\left|\mathcal{E}[7](K)\right| = 49$.

2. If $\mathcal{E}$ is an elliptic curve defined over $K = \bar{\mathbb{F}_7}$ then $|\mathcal{E}[7]| = 1$ or 7, so $K \not\models \Psi$. So we can not avoid the assumption about the characteristic zero in proposition 1.8.

1.10 Remark. It is important to understand that not all properties of fields can be expressed by first order formulas.

1. The property "*K has transcendance degree at least* 1 *over* $\mathbb{Q}$" can not be expressed by a first order formula. We would like to write it as
$$\exists x\ \forall P \in \mathbb{Q}[Q]\ P(x) \neq 0.$$
But quantifying over $P \in \mathbb{Q}[Q]$ is not allowed by our definitions. We can only quantify finitely many variables in the field K whereas quantifying over $P = \sum_{i \geq 0} p_i X^i \in \mathbb{Q}[X]$ requires to quantify over the infinite set of variables $\{p_i\}_{i \in \mathbb{N}}$. Using proposition 1.8 we can prove that this is not a first order property: it holds on $\mathbb{C}$ but not on $\bar{\mathbb{Q}}$.

2. Let us consider the property *for all smooth projective curve defined over K, there exists a regular function $f : X \to \mathbb{P}^1_K$ such that f is unramified over* $\{0, 1, \infty\}$. This is not a first order property: a result of arithmetic geometry (Belyi Theorem) asserts that up to isomorphism the only field satisfying this property is $\bar{\mathbb{Q}}$.

2 The Uniform Tits Alternative is a first order property

Exercise. Prove that
$$UTA\left(\overline{\mathbb{Q}(T_1, T_2, \ldots)}\right) \Rightarrow UTA.$$

We are going to prove:

2.1 Proposition.
$$UTA\left(\overline{\mathbb{Q}}\right) \Rightarrow UTA.$$

Proof. The idea is to use corollary 1.9. The problem is that the property UTA contains two quantifiers:

- A quantifier $\forall d \in \mathbb{N}$ and
- a quantifier $\forall$ finite sets $S \subset GL_d(K)$

which are not allowed in a first order formula.

Let us fix $d \in \mathbb{N}$. According to $UTA(\overline{\mathbb{Q}})$, there exists $N(d)$ satisfying the conditions of $UTA(\bar{\mathbb{Q}})$. Let us consider the property:

Property. *$UTA(d, N(d))$. If K is an algebraically closed field of characteristic 0, $S \subset GL_d(K)$ is a finite symmetric set with $1 \in S$, then*

- *either $\langle S \rangle$ is virtually solvable*
- *or $S^{N(d)}$ contains a generator of a free group with two generators: $F_2 \subset \langle S \rangle$.*

It suffices to prove $UTA(d, N(d))$. We have removed the $\forall d \in \mathbb{N}$, but we still have the quantifier $\forall$ finite $S \subset GL_d(K)$.

So let us fix an integer k and let us consider the property:

Property. *$UTA(d, N(d), k)$. If K is an algebraically closed field of characteristic 0, $S = \{A_1, \dots, A_k\} \subset GL_d(K)$ is a finite symmetric set with $1 \in S$, and with k elements, then*

- *either $\langle S \rangle$ is virtually solvable*
- *or $S^{N(d)}$ contains a generator of a free group with two generators: $F_2 \subset \langle S \rangle$.*

By assumption, the property $UTA(d, N(d), k)$ holds for $K = \bar{\mathbb{Q}}$. So if we prove that $UTA(d, N(d), k)$ is a first order property (that is to say can be expressed by a first order formula), thanks to corollary 1.9, we will also prove $UTA(d, N(d), k)$.

Let us try to write a corresponding first order formula Φ for $UTA(d, N(d), k)$:

$$\Phi = \forall A_1, A_2, \dots, A_k \in GL_d(K) \ \Big(\{A_1, \dots, A_k\} \text{ is symetric}\Big) \Rightarrow$$
$$\Big(\Gamma := \langle A_1, \dots, A_k \rangle \text{ is virtually solvable}\Big) \bigvee \Big(\{A_1 \dots A_k\}^N \text{ contains two generators of some subgroup } F_2\Big).$$

□

Let us list three problems we face.

Problem 1. In Φ we quantify over matrices $A \in GL_d(K)$, and not over elements of the field K. But since d is fixed, this is not a problem, because A is encoded by its n^2 coefficients $(A_{i,j})_{1 \le i,j \le n}$. That $(A_{i,j})$ defines an element of $GL_d(K)$ and not simply a matrix of $M_d(K)$ can be expressed by the fact that $det(A_{i,j}) \neq 0$ which is a first order property. Note also that products and inverses of matrices are given by polynomials in the coefficients $A_{i,j}$, so we will freely quantify over matrices, multiply them and inverse them.

Problem 2. Is the property

$$VS(A_1, \dots, A_k) = \Big(\Gamma := \langle A_1, \dots, A_k \rangle \text{ is virtually solvable}\Big)$$

a first order formula? This is not obvious. This property is equivalent to:

$$\exists c \in \mathbb{N} \ \exists G \subset \Gamma := \langle A_1, \dots, A_k \rangle \ \Big| \ (G \text{ is a solvable subgroup}) \wedge ((\Gamma : G) \le c)\,.$$

The problem is that the two quantifiers $\exists c \in \mathbb{N}$ and $\exists G \subset \Gamma$ are not allowed. Thanks to proposition 3.1, we know that there exists an integer $c := c(d) \in \mathbb{N}$ (independent of K) such that for all subgroups $\Gamma \subset GL_d(K)$, Γ is virtually solvable if and only if it has a subgroup of index less than c conjugated to a subgroup of the subgroup of upper-triangular matrices that we denote by $\mathbb{T}_d$. So

$$VS(A_1, \dots, A_k) \Leftrightarrow \Big(\exists P \in GL_d(K) \ (\Gamma : (\Gamma \cap P\mathbb{T}_d(K)P^{-1})) \le c\Big).$$

The last problem is that we need to calculate in terms of a first order formula the index $(\Gamma : \Gamma \cap P\mathbb{T}_d(K)P^{-1})$.

For any integer k let us denote by $[S^k]$ the set of left classes $\gamma\cdot(\Gamma\cap P\mathbb{T}_d(K)P^{-1})$ in $\Gamma/(\Gamma\cap(P\mathbb{T}_d(K)P^{-1}))$ for some $\gamma\in S^k$. An easy induction shows that if $[S^{k+1}]=[S^{k+1}]$, for some integer k, then for any integer $j\geq k$, $[S^j]=[S^k]$. Since S generates Γ, we deduce that for all $j\geq k$

$$[S^j]=\Gamma/(\Gamma\cap(P\mathbb{T}_dP^{-1})).$$

It follows from this that

$$\Gamma/(\Gamma\cap(P\mathbb{T}_d(K)P^{-1}))\leq c\Leftrightarrow\left[\Big([S^c]=[S^{c+1}]\Big)\wedge\Big(|[S^c]|\leq c\Big)\right].$$

Let us finally remark that testing if a matrix is in $P\mathbb{T}_d(K)P^{-1}$ is a first order property: one has to check that the $d(d-1)$ lower coefficients vanish. So the property expressing that

the subgroup $\langle A_1,\ldots,A_k\rangle\subset GL_d(K)$ is virtually solvable

is equivalent to the first order formula

$$\Psi(A_1,\ldots,A_k):=\exists P\in GL_d(K)\ \Big(\bigwedge_{1\leq i_1,\ldots,i_{c+1}\leq k}\Big(\bigvee_{1\leq j_1,\ldots,j_c\leq k} P^{-1}A_{i_1}A_{i_2}\cdots A_{i_{c+1}}\cdot(A_{j_1}\cdots A_{j_c})^{-1}P\in\mathbb{T}_d(K)\Big)\wedge|[S^c]|\leq c\Big).$$

Problem 3. It remains to prove that the following property is a first order property.

Property. $\mathcal{P}(B_1\ldots B_M)$. *There exist two elements* $A,B\in\{B_1\ldots B_M\}^N$ *such that* $\langle A,B\rangle\simeq F_2$.

Exercise. For $A,B\in GL_2(K)$, let $\mathcal{G}(A,B)$ be the property that A,B generate a free group F_2. Then $\mathcal{G}$ is not a first order property. Let us sketch a proof of this fact.

1. Prove that there exist $A,B\in GL_2(\mathbb{R})$ which generate a free group. For instance one can remark that $\pi_1(\mathbb{P}^1_{\mathbb{C}}\setminus\{0,1,\infty\})\simeq F_2$. The analytic universal covering of $\mathbb{P}^1_{\mathbb{C}}\setminus\{0,1,\infty\}$ is the Poincaré upper half-plane $\mathbb{H}$ and the latter has automorphism group $PSL_2(\mathbb{R})$. This gives a subgroup $F_2\leq PSL_2(\mathbb{R})$.
2. Deduce from this that
$$\begin{pmatrix}a_{1,1}&a_{1,2}\\a_{2,1}&a_{2,2}\end{pmatrix},B=\begin{pmatrix}b_{1,1}&b_{1,2}\\b_{2,1}&b_{2,2}\end{pmatrix}$$
generate a free group F_2 in $GL_2(K)$ with $K=\mathbb{Q}(a_{1,1},a_{1,2},a_{2,1},a_{2,2},b_{1,1},b_{1,2},b_{2,1},b_{2,2})$.
3. Deduce from this that
$$\begin{pmatrix}a_1&0\\0&a_2\end{pmatrix},B=\begin{pmatrix}b_{1,1}&b_{1,2}\\b_{2,1}&b_{2,2}\end{pmatrix}$$
generate a free group F_2 in $GL_2(K)$ with $K=\mathbb{Q}(a_1,a_2,b_{1,1},b_{1,2},b_{2,1},b_{2,2})$.
4. Deduce from this that
$$\begin{pmatrix}a&0\\0&1\end{pmatrix},B=\begin{pmatrix}b_{1,1}&b_{1,2}\\b_{2,1}&b_{2,2}\end{pmatrix}$$
generate a free group F_2 in $GL_2(K)$ with $K=\mathbb{Q}(a,b_{1,1},b_{1,2},b_{2,1},b_{2,2})$.
5. If $\mathcal{G}(A,B)$ was a first order property, the set
$$C:=\{a\in\mathbb{C}\mid\exists B\in GL_2(\mathbb{C}),\ \mathcal{P}(\begin{pmatrix}a&0\\0&1\end{pmatrix},B)\}$$
would be a dense constructible subset of $\mathbb{C}$. To do this, use quantifier elimination for algebraically closed fields, and the equivalence of first order property with constructible sets arising from it.

6. Prove that there is an integer m such that $e^{\frac{2i\pi}{m}} \in C$.

7. Obtain a contradiction by remarking that for any $B \in GL_2(\mathbb{C})$ the two matrices $\begin{pmatrix} e^{\frac{2i\pi}{m}} & 0 \\ 0 & 1 \end{pmatrix}$ and B do not generate a free group F_2.

Given a word $u \in F_2 = F_2(a,b)$, and given two matrices $A, B \in GL_d(K)$, we denote by $u(A,B)$ the matrix obtain by replacing a by A and b by B in u. For instance if $u = aba^{-1}$, $u(A,B) = ABA^{-1}$. The property that A, B generate a free group is equivalent to the infinite conjunction

$$\bigwedge_{u \in F_2 \setminus \{1\}} u(A,B) \neq 1_{GL_d}.$$

For an integer l let us set

$$\Psi_l(B_1, \ldots, B_M) := \bigvee_{1 \leq i < j \leq M} \Big(\bigwedge_{u \in F_2 \setminus \{1\},\ |u| \leq l} u(B_i, B_j) \neq 1_{GL_d} \Big).$$

The formula $\Psi_l(B_1, \ldots, B_M)$ expresses the fact that there exists a pair (B_i, B_j) such that for any nontrivial word u of F_2 of length less than l, $u(B_i, B_j) \neq 1$. It follows that $\mathcal{P}(B_1, \ldots, B_M)$ can be expressed by the infinite conjunction

$$\bigwedge_{l \in \mathbb{N}} \Psi_l(B_1, \ldots, B_M)$$

because then we can find a pair (B_i, B_j) winch satisfy $\bigwedge_{u \in F_2 \setminus \{1\},\ |u| \leq l} u(B_i, B_j) \neq 1_{GL_d}$ for infinitely many l. So for all $u \in F_2 \setminus \{1\}$ we will have that $u(B_i, B_j) \neq 1_{GL_d}$ which proves that (B_i, B_j) generate some F_2.

Remind that we had reduced $UTA(d, N(d), k)$ to the statement

$$\Phi = \forall A_1, A_2, \ldots, A_k \in GL_d(K) \ \Big(\{A_1, \ldots, A_k\} \text{ is symetric} \Big) \Rightarrow \Big(\Gamma := \langle A_1, \ldots, A_k \rangle \text{ is virtually solvable} \Big) \bigvee \Big(\{A_1 \ldots A_k\}^N \text{ contains two generators of some } F_2 \Big).$$

Setting $M = k^N$ it is equivalent to the property

$$\forall A_1, A_2, \ldots, A_k \in GL_d(K) \ \Big(\{A_1, \ldots, A_k\} \text{is symetric} \Big) \Rightarrow \Big(\Gamma := \langle A_1, \ldots, A_k \rangle \text{is virtually solvable} \Big) \bigvee \Big(\bigwedge_{l \in \mathbb{N}} \Psi_l(\{A_1 \ldots A_k\}^N) \Big).$$

Distributivity properties of $\wedge, \vee$ and $\Rightarrow$ imply that this is equivalent to the property

$$\bigwedge_{l \in \mathbb{N}} \Phi_l$$

where

$$\Phi_l := \forall A_1, A_2, \ldots, A_k \in GL_d(K) \ \Big(\{A_1, \ldots, A_k\} \text{is symetric} \Big) \Rightarrow \Big[\Big(\Gamma := \langle A_1, \ldots, A_k \rangle \text{is virtually solvable} \Big) \bigvee \Big(\Psi_l(\{A_1 \ldots A_k\}^N) \Big) \Big].$$

The latter Φ_l is now a first order formula. Since $UTA(\bar{\mathbb{Q}})$ holds, $\bar{\mathbb{Q}} \models \Phi_l$ for all integer l, so according to corollary 1.9, for any algebraically closed field K of characteristic 0 $K \models \Phi_l$ so K satisfies $UTA(d, N(d), k)$.

3 A Uniform bound for virtually solvable groups

We want to prove the following result which was used in the previous section.

3.1 Proposition. *For each integer d, there exists an integer $c(d) > 0$ such that if K is a field of characteristic 0, for every subgroup $G \subseteq GL_d(K)$, G is virtually solvable if and only if there exists $P \in GL_d(K)$ such that*

$$\big(G : (G \cap (P\mathbb{T}_d(K)P^{-1}))\big) \leq c(d).$$

Remark. Proposition 3.1 does not hold in positive characteristic. Indeed, any finite subgroup is virtually solvable, so this would means that we could find an integer c such that for any integer n $SL_2(\mathbb{F}_{pn})$ contains a solvable subgroup G of index less than c. The same should hold for $PSL_2(\mathbb{F}_{pn})$ which is simple for $\mathbb{F}_{pn} \neq \mathbb{F}_2, \mathbb{F}_3$. This contradicts the fact that $|PSL_2(\mathbb{F}_{p^n})| \xrightarrow[n\to\infty]{} +\infty$ and that $PSL_2(\mathbb{F}_{p^n})$ is a simple group which is not commutative.

We will admit the following results.

3.2 Theorem (Jordan-Schur Theorem, see 36.13 [4])**.** *For each integer n there exists a $\beta(n) \in \mathbb{N}$ such that if K is a field of characteristic 0, and G a finite subgroup of $GL_n(K)$, then there exists a normal abelian subgroup $A \lhd G$ such that $(G : A) \leq \beta(n)$.*

3.3 Definition. The map

$$\begin{array}{ccc} GL_d(K) & \to & K^{d^2} \\ A & \mapsto & (A_{i,j})_{1\leq i,j\leq n} \end{array} \tag{1}$$

identifies $GL_d(K)$ with the Zariski open subset of K^{d^2} defined by $\det(A_{i,j}) \neq 0$. This allows us to consider $GL_d(K)$ as an algebraic variety.

1. A subgroup $\mathbb{G} \subset GL_d(K)$ is called an algebraic group if it is a Zariski-closed subset of $GL_d(K)$.
2. If $G \subset GL_d(K)$ is a subgroup, we set

$$\mathbb{G} := \bigcap_{\substack{\mathbb{H} \subset G \\ \mathbb{H} \text{ is an algebraic group}}} \mathbb{H}.$$

One can check that $\mathbb{G}$ is an algebraic group, and that it is the smallest algebraic group containing G.

3.4 Example.
- The group of upper triangular matrices $\mathbb{T}_d(K)$.
- The group of diagonal matrices $\mathbb{D}_d(K)$.
- The group of unipotent matrices $\mathbb{U}_d(K) = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix} \right\}$.
- If $\mathbb{G} \subset GL_d(K)$ is an algebraic group, any conjugate $P\mathbb{G}P^{-1}$ is an algebraic group.

3.5 Lemma (1.2 [1])**.** *Let $\mathbb{G} \subset GL_d(K)$ be an algebraic group and let $\mathbb{G}_0$ be the Zariski connected component of $\mathbb{G}$ containing $1 \in GL_d(K)$. Then $\mathbb{G}^0$ is an algebraic group, $\mathbb{G}^0 \lhd \mathbb{G}$ and $(\mathbb{G} : \mathbb{G}^0) < \infty$.*

3.6 Lemma. *If $H \subset G$ is a subgroup then*

$$(\mathbb{G} : \mathbb{H}) \leq (G : H).$$

Proof. Let $g_1, \ldots, g_n$ be a set of representatives of G/H. Then $\cup_i g_i\mathbb{H}$ is exactly the group generated by $\mathbb{H}$ and the g_i's. Hence, it is Zariski closed and contains G. It follows that $\mathbb{G} = \cup_i g_i\mathbb{H}$. ☐

Remark. Let $H \subset G$ be a subgroup of finite index, then in general ($(\mathbb{G} : \mathbb{H}) < (G : H)$. For instance if $g = \mu_{p_\infty} \mu_{p'}$, and $H = \mu_{p_\infty}$.

3.7 Lemma (Corollary I.2.4 of [1])**.** *If $G \subset GL_d(K)$ is a solvable group, then so is $\mathbb{G}$.*

3.8 Theorem (Lie-Kolchin theorem III.10.5 of [1])**.** *Let $\mathbb{G} \subset GL_d(K)$ be an algebraic group which is Zariski-connected and solvable. Then there exists $P \in GL_d(K)$ such that*

$$\mathbb{G} \subset P \mathbb{T}_d(K) P^{-1}. \tag{2}$$

Let us start the proof of proposition 3.1, by induction on d. For $d = 1$, $GL_1(K)$ is abelian, so G is solvable. Hence we can take $c(1) = 1$.

We fix an integer $d > 1$ and we assume that the above properties hold for all $d' < d$. We start by an important lemma.

3.9 Lemma. *We can find a constant $c'(d)$ such that for any G as above, if G stabilizes a non trivial subspace $\{0\} \subsetneq V \subsetneq K^d$, then there exists $P \in GL_d(K)$ such that*

$$(G : (G \cap P \mathbb{T}_n(K) P^{-1})) \leq c'(d).$$

Proof. Up to conjugation in GL_d, we can assume that $V = \langle e_1, \dots e_{d_1} \rangle$ where $(e_i)_{1 \leq i \leq d}$ is the standard basis of K^d and $d_1 := \dim(V)$. So $1 \leq d_1 < d$. Let us set $d_2 := d - d_1$. So

$$G \subset \left\{ \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array} \right) \middle| A \in GL_{d_1}(K),\ B \in M_{d_1, d_2}(K),\ C \in GL_{d_2}(K) \right\}.$$

We now consider the group homomorphism

$$\begin{array}{cccc} \varphi_1 : & G & \to & GL_{d_1} \\ & \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array} \right) & \mapsto & A \end{array}$$

and denote by $F_1 \subset GL_{d_1}$ its image. By induction hypothesis, there exists $P_1 \in GL_{d_1}(K)$ such that

$$\big(PF_1 : (F_1 \cap P_1 \mathbb{T}_{d_1}(K) P_1^{-1}) \big) \leq c(d_1). \tag{3}$$

Similarly, we set

$$\begin{array}{cccc} \varphi_2 : & G & \to & GL_{d_2} \\ & \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array} \right) & \mapsto & C \end{array}$$

with image $F_2 \subset GL_{d_2}$. By induction hypothesis, there exists $P_2 \in GL_{d_2}(K)$ such that

$$\big(F_2 : (F_2 \cap P_2 \mathbb{T}_{d_2}(K) P_2^{-1}) \big) \leq c(d_2). \tag{4}$$

We set

$$P := \left(\begin{array}{c|c} P_1 & 0 \\ \hline 0 & P_2 \end{array} \right).$$

We obtain that

$$\big(G : (G \cap P \mathbb{T}_d(K) P^{-1} \big) \leq c(d_1) c(d_2).$$

So

$$c'(d) := \sup_{1 \leq d_1 < d} c(d_1) c(d - d_1)$$

works. ∎

Thanks to this lemma, we can assume that G acts irreducibly on K^d. Since G is virtually solvable, there exists a solvable subgroup $S \subset G$ of finite index. Thanks to lemma 3.6, $(\mathbb{G} : \mathbb{S}) < +\infty$. It follows that $\mathbb{S}$ is Zariski closed and open, hence $\mathbb{G}^0 \subseteq \mathbb{S}$. Thanks to lemma 3.7, $\mathbb{S}$ is solvable, hence $\mathbb{G}^0$ is also solvable. Thanks to theorem 3.8, there exists a $P \in GL_d(K)$ such that $\mathbb{G}^0 \subseteq P\mathbb{T}_d(K)P^{-1}$. In particular,

$$(G : G \cap P\mathbb{T}_d(K)P^{-1}) \leq (\mathbb{G} : \mathbb{G} \cap P\mathbb{T}_d(K)P^{-1}) \leq (\mathbb{G} : \mathbb{G}^0)$$

so we are reduced to bound $(\mathbb{G} : \mathbb{G}^0)$. Since G acts irreducibly, $\mathbb{G}$ also acts irreducibly on K^d. Up to conjugation by P, we can assume that $\mathbb{G}^0 \subset \mathbb{T}_d(K)$. If we intersect the natural exact sequence of groups

$$1 \to \mathbb{U}_d(K) \to \mathbb{T}_d(K) \xrightarrow{\Psi} \mathbb{D}_d(K) \to 1 \tag{5}$$

with $\mathbb{G}^0$, we obtain an exact sequence

$$1 \to \mathbb{U} \to \mathbb{G}^0 \to \mathbb{D} \to 1 \tag{6}$$

where $\mathbb{U} := \mathbb{U}_d(K) \cap \mathbb{G}^0$ and $\mathbb{D} := \Psi(\mathbb{G}^0)$.

Claim. $\mathbb{U} \lhd \mathbb{G}$.

Proof of the claim. We already know that $\mathbb{U} \lhd \mathbb{G}^0 \lhd \mathbb{G}$. Let $u \in \mathbb{U}$ and $g \in \mathbb{G}$. Then $gug^{-1} \in \mathbb{G}^0$ because $\mathbb{G}^0 \lhd \mathbb{G}$. On the other hand, $\mathbb{U}$ is exactly the set of elements $h \in \mathbb{G}^0$ whose characteristic polynomial is $\chi_h(X) = (X-1)^d$. Since the characteristic polynomial is invariant under conjugation, it follows that $gug^{-1} \in \mathbb{U}$. □

Claim. $\mathbb{U} = \{1\}$.

Proof of the claim. Let us set

$$V := \{v \in K^d \mid u(v) = v,\ \forall u \in \mathbb{U}\}.$$

Then V is a vector subspace of K^d, which contains $K \cdot e_1$. If $\mathbb{U} \neq \{1\}$, we have that $V \subsetneq K^d$. Then we claim that $\mathbb{G}$ stabilizes V. Indeed if $g \in \mathbb{G}$, $v \in V$, then for all $u \in \mathbb{U}$ we have

$$u(g(v)) = gg^{-1}ug(v) = gu'(v) = g(v)$$

where $u' := g^{-1}ug \in \mathbb{U}$ because $\mathbb{U} \lhd \mathbb{G}$. So $g(v) \in V$.

But this contradicts our assumption that $\mathbb{G}$ acts irreducibly on K^d. □

Since we know that $\mathbb{G}^0 \lhd \mathbb{G}$, it follows that $\mathbb{G} \subset N_{GL_d(K)}(\mathbb{G}^0)$. Hence we get

$$\begin{aligned} \left(N_{GL_d(K)}(\mathbb{G}^0) : Z_{GL_d(K)}(\mathbb{G}^0)\right) &\geq \left(\mathbb{G} \cap N_{GL_d(K)}(\mathbb{G}^0) : \mathbb{G} \cap Z_{GL_d(K)}(\mathbb{G}^0)\right) \\ &= \left(N_{\mathbb{G}}(\mathbb{G}^0) : Z_{\mathbb{G}}(\mathbb{G}^0)\right) \\ &= \left(\mathbb{G} : Z_{\mathbb{G}}(\mathbb{G}^0)\right). \end{aligned}$$

Now a matrix computation leads that for any algebraic subgroup $\mathbb{D} \subset \mathbb{D}_d(K)$ one has

$$\left(N_{GL_d(K)}(\mathbb{D}) : Z_{GL_d(K)}(\mathbb{D})\right) \leq d!.$$

Hence, we can replace if necessary $\mathbb{G}$ by $Z_{\mathbb{G}}(\mathbb{G}^0)$, that is to say, we can assume that

$$\mathbb{G}^0 \subset Z(\mathbb{G}). \tag{7}$$

Let us now distinguish three cases.

- $\mathbb{G}^0 \not\subseteq K^* \operatorname{Id}_d$ Then we can find an element $g_0 \in \mathbb{G}^0$ which is not an homothety. Let us write

$$g_0 = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_d \end{pmatrix}$$

and let us set

$$V := \{v \in K^d \mid g_0 v = a_1 v\}.$$

Then for any $g \in \mathbb{G}^0$ and for any $v \in V$,

$$g_0(gv) = gg_0(v) = g(a_1 v) = a_1(gv)$$

so $gv \in V$. So V is fixed by $\mathbb{G}^0$. On the other hand $e_1 \in V$, and since we assumed that g_0 is not a homothety, $V \neq K^d$. But this contradicts the irreducibility of the action $\mathbb{G} \curvearrowright K^d$.

- If $\mathbb{G}^0 = \{1\}$. Then $\mathbb{G} \simeq \mathbb{G}/\mathbb{G}^0$ which is finite. So $\mathbb{G}$ is finite. Thanks to theorem 3.2 there exists an abelian subgroup $A \subset \mathbb{G}$ such that $(\mathbb{G} : A) \leq \beta(d)$. In particular A is solvable.

- The remaining case would be that $\{1\} \subsetneq \mathbb{G}^0 \subset K^* \operatorname{Id}_d$. Since $\mathbb{G}^0$ is Zariski connected, the only possibility is that $\mathbb{G}^0 = K^* \operatorname{Id}_d$. We have an exact sequence of groups

$$1 \to \mathbb{G}^0 \to \mathbb{G} \to \mathbb{G}/\mathbb{G}^0 \to 1. \tag{8}$$

whose right part is a finite group. If we intersect this short exact sequence with $SL_d(K)$ we obtain

$$1 \to SL_d(K) \cap \mathbb{G}^0 \to \mathbb{G} \cap SL_d(K) \to (\mathbb{G} \cap SL_d(K))/(SL_d(K) \cap \mathbb{G}^0) \to 1. \tag{9}$$

The right hand side is still finite, and the left hand side is

$$SL_d(K) \cap K^* \operatorname{Id}_d(K) = \mu_d \operatorname{Id}_d$$

is also finite. So $\mathbb{G} \cap SL_d(K)$ is finite. We claim that

$$(\mathbb{G} \cap SL_d(K)) \cdot \mathbb{G}^0 = \mathbb{G}.$$

Indeed, if $g \in \mathbb{G}$, then there exists $\lambda \in K^*$ such that $\det(\lambda \operatorname{Id}) = \det(g)$, hence $g\lambda^{-1} = h \in SL_d(K)$. So $g = \lambda \cdot h$ with $\lambda \operatorname{Id}_d \in \mathbb{G}^0$ and $h \in \mathbb{H}$.

To conclude we apply theorem 3.2 to $\mathbb{G} \cap SL_d(K)$ which is finite. It contains an abelian subgroup $A \subset (\mathbb{G} \cap SL_d(K))$ with $((\mathbb{G} \cap SL_d(K)) : A) \leq \beta(d)$. So we get that

$$\begin{aligned}(\mathbb{G} : \mathbb{G}^0 A) &= (\mathbb{G}^0 \mathbb{H} : \mathbb{G}^0 A) \\ &\leq (\mathbb{H} : A) \\ &\leq \beta(d).\end{aligned}$$

Since $\mathbb{G}^0$ and A are abelian, and $\mathbb{G}^0 \subset Z(\mathbb{G})$, it follows that $\mathbb{G}^0 A$ is abelian, hence solvable.

References

[1] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[2] Emmanuel Breuillard. Heights on SL_2 and free subgroups. In *Geometry, rigidity, and group actions*, Chicago Lectures in Math., pages 455–493. Univ. Chicago Press, Chicago, IL, 2011.

[3] Emmanuel Breuillard. Diophantine geometry and uniform growth of finite and infinite groups. In *Proceedings of the International Congress of Mathematicians*. ICM Seoul, 2014.

[4] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[5] David Marker. Introduction to model theory. In *Model theory, algebra, and geometry*, volume 39 of *Math. Sci. Res. Inst. Publ.*, pages 15–35. Cambridge Univ. Press, Cambridge, 2000.