KASDI MERBAH UNIVERSITY

OUARGLA

Faculty of mathematics and matrial sciences

DEPARTEMENT OF MATHEMATICS

MASTER

Speciality: Mathematics

Option: Algebra and Geometry

By: Belmazouzi Amina

Theme

The Tits alternative and beyond

Version of :May 25,2017

jury composed of:

Mr.M. Laid YoUMBAI	M.A. University of KASDI MERBAH - Ouargla President
Mr.M. Tayab BEN MOUSSA	M.A. University of KASDI MERBAH - Ouargla Examinateur
Mr.Mohamed BOU SAID	M.A. University of KASDI MERBAH - Ouargla Examinateur
Mr.Yssine GUERBOUSSA	M.A. University of KASDI MERBAH - Ouargla Supervisor

Academic year:2016/2017

Dedication

This work is dedicated to my dear parents who bring me to life and taught me the importance of education and helping me go through all what I have been in.
My dear brothers Yacine, Mouhaad, Sohaib and my sisters Abir, Asma.
My dear aunt and all members of my family.
My best friends, Oumlkhir, Klthoum, Manal,
Hooda, Yamina, Ymna, Sakina, Oumsaad, Chahra,..., without whose caring support it would not have been possible.

Acknowledgment

First and foremost, I would like to thank Allah the Almighty.
I would like to express my full gratitude to my supervisor, Dr. Yassine Geurboussa who provided untiring help, guidance and prompt feedback in preparing the present work. He spreads no efforts in teaching us how to question opinions and express them. He was patient enough to help me organize this work.
Im, also indebted to the members of the jury for their willingness to read and examine this work.
My special thank and appreciation with deepest respect to my dear brother Yacine.
Warm thanks are due to all my friends for their encouragement and help and for Just being there in times of need.

Contents

1 Groups and free groups **3**
- 1.1 Basic facts . . . 3
- 1.2 Linear groups . . . 5
- 1.3 Free Groups . . . 6

2 Linear algebraic groups **9**
- 2.1 Affine varieties . . . 9
- 2.2 Linear Algebraic groups . . . 13
- 2.3 Semisimple linear algebraic groups . . . 15
- 2.4 Reduction for the Tits alternative. . . . 16

3 On the proof of Theorem A **17**
- 3.1 Projective transformations and Proximal elements . . . 17
  - 3.1.1 Local fields . . . 17
  - 3.1.2 Projective transformations . . . 18
  - 3.1.3 Ping-Pong tuples and free groups . . . 21
  - 3.1.4 Constructing ping-pong tuples . . . 21
- 3.2 Representation theory, and a sketch of the final step in the proof . . . 21
  - 3.2.1 Representations of abstract groups . . . 22
  - 3.2.2 Representations of algebraic groups . . . 22
  - 3.2.3 Completion of the proof . . . 23

4 The probabilistic approach and some applications of the Tits alternative **25**
- 4.1 The work of M. Larsen and A. Shalev . . . 25
  - 4.1.1 Identities and Probabilistic identities . . . 25
- 4.2 The word growth in groups . . . 31

4.3 Amenable groups 34

Introduction

The Tits alternative asserts that every finitely generated linear group contains either a normal soluble subgroup of finite index or a free non-abelian subgroup. This results was first conjectured by J-P. Serre and H. Basse. Tits established his proof in 1972 in an extraordinary paper published in Journal of Algebra. The proof of Tits combines in an ingeneous way results from algebraic geometry, number theory and group theory, and remains a land mark in the subject.

Tits' result has motivated Breuillard and Gelander to obtain the *topological Tits alternative* (see [2]) which is much stronger and has more applications. More recently there is an attempt by Shalev and Larsen (see [19]) for establishing a probabilistic Tits alternative, by using the notion of to use probabilistic identities; this approach seems quite promicing.

The paper of Breuillard and Gelander [2] is more general, and yields stronger results than that obtained by Tits. We choosed to follow the former. However, this shall make our task more difficult since we have to deal with more sophisticated tools. Following all the details is out of reach for us at this level; we could only discuss the general notions involved and try to combine them in a rough way.

The paper is organized as follows:

The first chapter contains some basic notions in abstract group theory. Its aim is to explain the terminology involved in the main theorem.

In the second chapter, we discuss some basic facts in algebraic geometry, and algebraic group theory. The main aim therein is to reduce the statement of the Tits alternative to one about algebraic groups.

In the third chapter, we discuss the core of the proof following the approach of Breuillard and Gelander. After reminding some notions on local fields, we introduce the notion of proximal elements and ping-pong tuples. This stuff gives a means for constructing free subgroups. Hence, the next aim is to prove, under appropriate conditions, that ping-pong tuples exist. This can be achieved by using representation theory of algebraic groups. In the end of the chpter we mention the topological Tits alternative and some of its consequences.

The last chapter contains three sections. The first is about the notion of probabilistic identities, and the probabilistisch analogue of the Tits alternative. In the second section we mention the importance of the Tits alternative in solving two conjectures of Milnor on the word growth of groups. The last section considers the relevance to the amenability of groups.

Chapter 1

Groups and free groups

1.1 Basic facts

Definition 1.1. *A group is a non-empty set G together with an internal operation $(a, b) \mapsto ab$ such that :*

1. *$a(bc) = (ab)c$, for all $a, b, c \in G$ (**associativity**);*
2. *there is an element $1 \in G$ such that $a1 = 1a = a$, for all $a \in G$ (**identity**);*
3. *If $a \in G$, then there is an element $a' \in G$ such that $aa' = a'a = 1$ (**inverse of** a).*

Note that the element a' which satisfies (3) is uniquely determined by a, for each $a \in G$, and we shall denote it by a^{-1}.

Examples 1.2.

❶ *For every set X, the set S_X of permutations of X,*

$$S_X = \{\sigma : X \to X, \sigma \text{ is a bejictive map}\}$$

forms a group under the usual composition of maps . Note that the isomorphism type of S_X depends only on the cardinality of X: if Y has the same cardinality as X, then S_X and S_Y are isomorphic. For $|X| = n$, the group S_X is usually denoted by S_n, and called the symmetric group of degree n.

❷ *Let R be a commutative unital ring. Then we can consider the $n \times n$ matrices with coefficients in R, and denote their set as usual by $M_n(R)$. It is straightforward to see that $M_n(R)$ is a unital ring with the usual addition and multiplication of matrices.*

An element $A \in M_n(R)$ is invertible if and only if $detA$ is invertible in R.

For instance $A \in M_n(\mathbb{Z})$ is invertible if and only if $detA = \pm 1$.

It follows that the invertible elements of $M_n(R)$ form a group which we denote by $\mathrm{GL}(n, R)$ and which we call the general linear group over R of dimension n, so

$$\mathrm{GL}(n, R) = \left\{ A \in M_n(R) \,|\, \det A \in R^\times \right\}$$

If R is a field, then

$$\mathrm{GL}(n, R) = \{ A \in M_n(R) \,|\, \det A \neq 0 \}$$

Definition 1.3.

- *Let G, H be two groups and $f : G \longrightarrow H$ be a map. We say that f is homomorphism of groups if :*
$$f(xy) = f(x)f(y)$$
for all $x, y \in G$.

  If in addition, f is bijective we say that f is an isomorphism, and that G and H are isomorphic groups (we already used this terminology in the previous example).

- *Let G be a group. A subgroup of G is non-empty subset H such that $x^{-1}y \in H$, for all $x, y \in G$.*

- *It follows that for every subset $X \subseteq G$ the intersection of subgroups containing X is a subgroup which is the smallest one that contains X. We denote this subgroup by $\langle X \rangle$.*

- *$\langle X \rangle$ is called the subgroup generated by X. We can show easily that $g \in \langle X \rangle$ if and only if there are elements $x_i \in X \cup X^{-1}$ such that $g = x_1 ... x_n$.*

- *If $\langle X \rangle = G$, we say that $\langle X \rangle$ is a generating subset of G.*

- *We say that G is finitely generated if $G = \langle X \rangle$ for some finite subset $X \subseteq G$.*

Recall that a subgroup H of G has finite index if the set $\{ xH \subseteq G \,|\, x \in G \}$ is finite.

Proposition 1.4. *Let G be a finitely generated group, and H be a subgroup of G of finite index. Then H is also finitely generated.*

For a proof for the last result see for instance [18, Theorem 1.6.11].

1.2 Linear groups

Definition 1.5. *A group G is said to be linear if there exists an injective homomorphism*

$$G \longrightarrow GL(n, K)$$

for some field K. That is G is linear if it can be embedded in the general linear group over some field K; we say here also that G linear over K.

Let K be a field. Then every subgroup of $Gl(n, K)$ is linear, and in particular the following groups are linear:

- $\mathrm{SL}(n, K) = \{A \in M_n(K) \mid \det A = 1\}$
- $\mathrm{O}(n, K) = \{A \in M_n(K) \mid A^t A = I_n\}$
- $\mathrm{Sp}(2n, K) = \{A \in M_{2n}(K) \mid A^t J A = J\}$, where

$$J = \begin{pmatrix} I_n & 0 \\ 0 & -I_n \end{pmatrix},$$

  and I_n is the identity matrix of size n.

Proposition 1.6. *Let K be an arbitrary field. Then every finite group is linear over K.*

Proof. Let G be a finite group. First we shall imbed G in S_G. For $g \in G$, define $\gamma_g : G \longrightarrow G$ by $\gamma_g(x) = gx$, for all $x \in G$. Obviously, γ_g is a bijective map, so $\gamma_g \in S_G$, now consider

$$\begin{array}{ccc} \gamma : G & \to & S_G \\ g & \mapsto & \gamma_g \end{array}$$

We claim that γ is a group morphism. Indeed, let $g_1, g_2 \in G$. Then

$$\begin{aligned} \gamma_{g_1 g_2}(x) &= (g_1 g_2)x = g_1(g_2 x) \\ &= \gamma_{g_1}(g_2 x) = \gamma_{g_1}(\gamma_{g_2}(x)) \\ &= \gamma_{g_1} \circ \gamma_{g_2}(x) \end{aligned}$$

for all $x \in G$. So $\gamma_{g_1 g_2} = \gamma_{g_1} \circ \gamma_{g_2}$. Moreover, γ is injective since if $\gamma_g = 1$, then $\gamma_g(x) = x, \forall x \in G$; so $gx = x$ and it follows that $g = 1$.
If $|G| = n$, then S_G and S_n isomorphic, therefore we have only to embed S_n in $\mathrm{GL(n, K)}$. For each $\sigma \in S_n$ consider

$$\begin{array}{ccc} \varphi_\sigma : K^n & \to & K^n \\ (x_1, ..., x_n) & \mapsto & (x_{\sigma(1)}, ..., x_{\sigma(n)}) \end{array}$$

Then φ_σ is a linear map, $\varphi_\sigma \in \mathrm{GL(n, K)}$ and $\varphi : S_n \longrightarrow \mathrm{GL(n, K)}$ is an injective group morphism. This completes the proof.

□

1.3 Free Groups

Definition 1.7. *Let S be a set. A free group on S is a group F_S together with a map $i : S \longrightarrow F_S$, such that whenever G is a group and $\phi : S \longrightarrow G$ is a map, there exists a unique group homomorphism $\tilde{\phi} : F_S \longrightarrow G$ which satisfies $\tilde{\phi} \circ i = \phi$*

$$\begin{array}{ccc} S & \xrightarrow{i} & F_S \\ \phi \searrow & & \swarrow \tilde{\phi} \\ & G & \end{array}$$

Remark 1.8. *The above universal propriety guarantees that F_S is unique up to isomorphism.*

Theorem 1.9. *There exists a free group on every non-empty set S.*

Proof. Let us give a sketch of the proof:

- Consider the manoid M of the words on $S \cup S^{-1}$, where $S^{-1} = \{s^{-1} \mid s \in S\}$ is just a set which does not encounter S (one can call the elements of S^{-1} the formal inverses of the elements of S). Recall that a word on $S \cup S^{-1}$ of length n is a finite sequence $w = x_1 x_2 \dots x_n$ of elements of $S \cup S^{-1}$. We denote the unique word of length 0 by 1 and we call it the empty word. The operation on M is defined by concatenation of words, that is for two words $u = x_1 x_2 \dots x_n$ and $v = y_1 y_2 \dots y_m$ in M, the product uv is defined as
$$uv = x_1 x_2 \dots x_n y_1 \dots y_m$$
Note that 1 is the identity element for this operation, that is $u1 = 1u = u$, for all $u \in M$.

- Define an equivalence relation on M by setting : $w \sim w'$ if w can be obtained from w' by adding or deleting subwords of the form ss^{-1} or $s^{-1}s$, with $s \in S$.

- We define F_S to be the quotient of M by the relation defined above. If we have two classes $[u], [v]$ of words, then we define their product as usual by $[u][v] = [uv]$. The canonical map from S to F_S is defined by $s \mapsto [s]$.

□

Remark 1.10.

- *It is worth noting that for two subsets S and S' we have $F_S \cong F_{S'}$ if and only if S and S' have the same cardinality .*

- *In particular every positive integer n defines a unique free group F_n, which we call the Free group on n generators.*

Proposition 1.11. *Let G be a finitely generated group then there exists an epimorphism $F_d \twoheadrightarrow G$. In particular, G is isomorphic to a quotient of F_d*

Proof. Assume that $\{g_1, ..., g_d\}$ is a generating set of G and consider the free group F_d on a generators $x_1, ..., x_d$. The map $x_i \mapsto g_i$, $i = \overline{1, d}$, extends by the universal property of F_d to a group homomorphism

$$\tilde{\phi} : F_n \longrightarrow G.$$

The morphism $\tilde{\phi}$ is surjective because $g_1, ..., g_d$ generate G. It follows that $F_n/\ker\tilde{\phi} \cong G$. □

We can give the statement of the Tits alternative after the following short definition.

Definition 1.12. *Let $\mathcal{C}$ be a class of groups. A group G is said to be virtually-$\mathcal{C}$, if G contains a normal subgroup N such that:*

- *G/N is finite.*
- *N lies in the class $\mathcal{C}$.*

Examples 1.13.

❶ *For a group G, the derived series $(G^{(n)})$ is defined inductuively by $G^{(0)} = G$ and*

$$G^{(i+1)} = [G^{(i+1)}, G^{(i+1)}], \text{ for } i \geqslant 0$$

The group G is said to be soluble if $G^n = 1$, for some $n \in \mathbb{N}$.

Now, we can define the notion of virtual solubility. A group G is virtually soluble if it contains a normal subgroup N of finite index such that N is soluble.

❷ *The lower central series $(\gamma_n(G))_{n\geq 1}$ is the series of subgroups of the group G defined by*

$$\gamma_1(G) = G$$

and

$$\gamma_i + 1(G) = [\gamma_i(G), G], \text{ for } i \geqslant 1$$

The group G is nilpotent if $\gamma_n(G) = 1$ for some $n \in \mathbb{N}^*$.

The group G is said to be virtually nilpotent if it contains a normal subgroup N of finite index such that N is nilpotent.

The main theorem in this thesis is the following.

Theorem 1.14 (The Tits alternative)**.** *A finitely generated linear group G is either virtually soluble or contains a free subgroup on two generators.*

In the above theorem the group G couldn't be simultaneously virtual soluble and contains a free 2-generated subgroup; this means that the Tits alternative is really an alternative! Indeed, assume that G is virtually soluble, so it contains a normal soluble subgroup N of finite index. If moreover G contains a free non-abelian subgroup F, then FN/N is finite, hence $F/F \cap N$ is finite. This means that $F \cap N$ is a non-trivial subgroup of F. Therefore, $F \cap N$ is free non-abelian by the Nielsen-Schreier theorem, and on the

other hand $F \cap N$ is soluble since it is a subgroup of the soluble group N. Hence, we have constructed a free non-abelian group which is soluble; if this is true then it follows at least that every 2-generated group is soluble by Proposition 1.9, in particular the alternating group A_5 is soluble, a contradiction.

If G is linear over a field of characteristic 0, then we can remove the finite generation condition in the Tits alternative; in other words we have.

Theorem 1.15. *A linear group over a field of characteristic* 0 *is either virtually soluble or contains a free subgroup on two generators.*

Chapter 2

Linear algebraic groups

This chapter treats some basic notions in algebraic geometry and algebraic groups which are indisponsible in understanding the proof of the Tits alternative. It is impossible in such a situation to give full proofs for all the mentioned results; for those we refer the reader for instance to [11] and [8].

2.1 Affine varieties

Let K be an algebraically closed field, and let $\mathbb{A}^n$ denote the cartesian product K^n.
For a subset S of polynomials ring $K[X_1, ..., X_n]$ we define $V(S)$ to be the set of common zeros of the polynomials in S, that is

$$V(S) = \{(a_1, ..., a_n) \in \mathbb{A}^n \mid f(a_1, ..., a_n) = 0, \text{ for all } f \in S\}$$

if I is the ideal generated by S, then it is readily seen that $V(S) = V(I)$.

Definition 2.1. *We call algebraic subset of $\mathbb{A}^n$ every subset of the form $V(S)$, for some $S \subseteq K[X_1, ..., X_n]$.*

Examples 2.2.

❶ *$\emptyset$ and $\mathbb{A}^n$ are algebraic sets since $\emptyset = V(f)$, for any constant non zero polynomial f and $\mathbb{A}^n = V(0)$.*

❷ $\mathrm{SL}(n,K)$ *is an algebraic set* $\mathbb{A}^{n^2}$*. Indeed, we may consider the polynomial ring*

$$K\left[X_{11},X_{12},...,X_{1n},X_{21},...,X_{nn}\right]$$

so the determinant

$$\det=\sum_{\sigma\in S_n}\epsilon(\sigma)X_{1\sigma(1)}X_{2\sigma(2)}\cdots X_{n\sigma(n)}$$

is just a polynomial in the later ring. Now consider $f=det-1$*, so*

$$\mathrm{SL}(n,K)=\{A\in M_n(K)\,|\,f(A)=0\}$$

It is understood that we have identified $\mathbb{A}^{n^2}$ *with the set of* $n\times n$ *matrices* $M_n(K)$*.*

❸ $\mathrm{GL}(n,K)$ *is an algebraic set in* $\mathbb{A}^{n^2+1}$ *consider the polynomial ring* $K\left[X_{11},...,X_{nn},Y\right]$ *and the polynomial* $det(X_{11},...,X_{nn})Y-1$*, then we have the algebraic set*

$$V(f)=\{(A,y)\in M_n(K)\times K\,|\,det(A)Y=1\}$$

which can be identified to $\mathrm{GL}(n,K)$ *via*

$$\mathrm{GL}(n,K)\longrightarrow V(f)$$

$$A\longmapsto(A,(detA)^{-1})$$

Proposition 2.3.

(i) $\emptyset$ *and* $\mathbb{A}^n$ *are algebraic sets.*

(ii) *If* $\{S_i\}$ *is a family of subsets of* $K\left[X_1,...,X_n\right]$*, then* $V(\sum_i S_i)=\cap_i V(S_i)$*; in particular the intersection of family of algebraic sets is algebraic.*

(iii) *If* $S,S'\subseteq K\left[X_1,...,X_n\right]$ *then* $V(SS')=V(S)\cup V(S')$*; In particular a finite union of algebraic sets is algebraic.*

Proof.

(i) For $f=0$, $V(f)=\mathbb{A}^n$. For a constant polynomial $f=c\neq 0$, we have $V(f)=\emptyset$.

(ii) For each j, we have $S_j\subseteq\sum S_i$, so if $P\in V(\sum S_i)$, then $f(P)=0\,\forall f\in\sum S_i$; in particular if $f\in S_j$, then $f\in\sum S_i, f(p)=0$. It follows that $P\in V(S_j),\forall j$, so $P\in\cap_j V(S_j)$. We have shown that $V(\sum_i S_i)\subseteq\cap_i V(S_i)$. Conversely, let $P\in\cap_i V(S_i)$. If $f\in\sum_j S_i$, then $f=\sum f_i$, where $f_i\in S_i$. So $f(P)=\sum f_i(P)=0$. Thus $P\in V(\sum S_i)$.

(iii) Without loss of generality we may assume that S_1 and S_2 are ideals. As $S_1S_2 \subseteq S_1$, it follows that for every $P \in V(S_1)$, and $f \in S_1S_2$, $f(P) = 0$; so $V(S_1) \subseteq V(S_1S_2)$. Similarly, we have $V(S_2) \subseteq V(S_1S_2)$. Thus $V(S_1) \cup V(S_2) \subseteq V(S_1S_2)$. Conversely, let $P \in V(S_1S_2)$ and assume for a contradiction that $P \notin V(S_1)$ and $P \notin V(S_2)$. Therefore, $\exists f \in S_1$ such that $f(P) \neq 0$; and $\exists g \in S_2$ such that $g(P) \neq 0$. Now, $fg(P) = f(P)g(P) \neq 0$, but since $fg \in S_1S_2$ we should have $fg(P) = 0$. This completes the proof.

□

Corollary 2.4. *The algebraic sets in $\mathbb{A}^n$ form the closed of a topology called the Zariski topology on $\mathbb{A}^n$.*

For instance, the Zariski topology on $\mathbb{A}^1$ has as closed subsets the finite parts and $\mathbb{A}^1$. There are several definitions of affine algebraic varieties form which the following is the most convenient for us.

Definition 2.5. *We call affine algebraic variety every closed subset of $\mathbb{A}^n$ endowed with the induced Zariski topology. If $X \subseteq \mathbb{A}^n$ is a variety, and K' is a subfield of K, then we can consider $X(K')$ the set of point of X having coordinates in K', and call $X(K')$ the set of K'-rational points of X.*

Examples **2.6.** *If $X = V(X^4 - 1) \subseteq \mathbb{C}$, or in other words $X = \{1, -1, i, -i\}$, then the $\mathbb{Q}$-rational points of X are $1$and -1.*

Definition 2.7. *A topological space $X \neq \emptyset$ is said to be irreducible if it cannot be written as $X = X_1 \cup X_2$ where X_1 and X_2 are tow proper closed subsets of X. A subset Y of X is irreducible if it is irreducible as a topological space with the induced topology.*

The irreducible subsets containing some part Y of X form an ordered set with respect to inclusion.

Lemma 2.8.

❶ *If (X_i) is totally ordered family of irreducible subsets of X, then $\cup_i X_i$ is irreducible*

❷ *If a subset $Y \subseteq X$ is irreducible, then its closure $\bar{Y}$ is irreducible.*

Proof.

❶ Assume that $\bigcup X_i$ is not irreducible, so $\bigcup X_i = Y_1 \cup Y_2$, where Y_1, Y_2 are two proper closed subsets of $\bigcup X_i$. We have $\bigcup X_i \nsubseteq Y_1$, so there exist $i \in I$ and $x_1 \in X_i$ such that $x_1 \notin Y_1$. Similarly, there exist $j \in I$ and $x_2 \in X_j$ such that $x_2 \notin Y_2$. Without loss of generality we may assume that $X_i \subseteq X_j$. Put $Z_1 = X_j \cap Y_1$ and $Z_2 = X_j \cap Y_2$. We have Z_1 and Z_2 are closed subsets of X_j such that

$$Z_1 \cup Z_2 = (X_j \cap Y_1) \cup X_j \cap Y_2 = X_j \cap (Y_1 \cup Y_2) = X_j$$

Moreover, both of them is a proper subset of X_j, since if we assume for instance that $Z_1 = X_j$, then it follows that $X_j \subseteq Y_1$ which is a contradiction. We have established that X_j is reducible which contradicts our assumption.

❷ If $\bar{Y}$ is not irreducible, then $\bar{Y} = Y_1 \cup Y_2$, where Y_1, Y_2 are two closed proper subsets of $\bar{Y}$ (so Y_1, Y_2 are also closed in X). Now, $Y = (Y_1 \cap Y) \cup (Y_2 \cap Y)$, but since Y is irreducible it follows that $Y = Y_1 \cap Y$ or $Y = Y_2 \cap Y$. This means that $Y \subseteq Y_1$ or $Y \subseteq Y_2$, from which it follows that $\bar{Y} \subseteq Y_1$ or $\bar{Y} \subseteq Y_1$ since Y_1 and Y_2 are closed. This contradicts the fact that Y_1 and Y_2 are proper subsets of $\bar{Y}$.

□

It follows from the above lemma that every topological space is a union of maximal irreducible subsets, and these maximal irreducible subsets are closed. We call them the irreducible components of X.

Corollary 2.9. *Every affine variety is a union of irreducible varieties.*

A topological space X is called noetherian if every ascending chain of open subsets of X is stationary; that is if X satisfies the ascending chain condition on the open subsets (equivalently, if every dexending chain of closed subsets is stationary).

For instance, $\mathbb{A}^n$ are always noetherian for the Zariski topology; to see this one reduces the problem to the ring $K[X_1, ..., X_n]$ which is noetherian by the Hilbert Basis Theorem.

Remark 2.10. *A noetherian space has only finitely many irreducible components. Hence, the number of irreducible components of an affine variety is always finite.*

Definition 2.11. *The dimension of an affine X variety is the maximum of the n's such that there exists a chain $X_0 \subset X_1 \subset ... \subset X_n$ of district irreducible closed subsets of X.*

Examples **2.12.** *The dimension of $\mathbb{A}^n$ is equal to n. To see this one reduce the problem to investigating the Krull dimension of the ring $K[X_1, ..., X_n]$ which is well known to be n.*

Proposition 2.13. *Let X and Y be tow irreducible affine varieties .If $Y \subset X$, then* $\dim Y < \dim X$.

Every time we have a family of mathematical object, it is natural to wonder what are the morphisms between then.

Definition 2.14. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be two affine varieties. A morphism $\varphi : X \longrightarrow Y$ is a map from X to Y such that $\exists \psi_1, ..., \psi_m \in K[X_1, ..., X_n]$ with*

$$\varphi(p) = (\psi_1(p), ..., \psi_m(p)), \forall p \in X$$

.

Note that every morphism $\varphi : X \longrightarrow Y$ of varieties is continuous (with respect to the Zariski topologies). Indeed, it suffices to show that $\varphi^{-1}(Z)$ is closed in X, for every closed subset of Y. Assume that $Z = V(S)$, for some $S = \{f_\alpha\} \subseteq K[X_1, ..., X_n]$ then $p \in \varphi^{-1}(Z)$ iff $f_\alpha(\psi_1(p), ..., \psi_m(p)) = 0, \forall \alpha$. But since for each α,

$$g_\alpha = f_\alpha(\psi_1(X_1, ..., X_n), ..., \psi_m(X_1, ..., X_n))$$

is obviously a polynomial in $K[X_1, ..., X_n]$, we have $\varphi^{-1}(Z) = V(\{g_\alpha\})$ which is closed in X. This completes the proof.

The following result is useful for the proof of Proposition 2.21.

Proposition 2.15. *Let $\varphi : X \longrightarrow Y$ be a morphism of varieties. If Z is irrducible in X, then $\varphi(Z)$ is irreducible in Y.*

We finish this section with the following result (see [11]).

Proposition 2.16. *Let $\varphi : X \longrightarrow Y$ be a morphism of irreducible varieties with $\varphi(X)$ dense in Y. Then there exists $U \neq \emptyset$ open in Y such that $U \subseteq \varphi(X)$ and*

$$\dim X = dim Y + \dim \varphi^{-1}(u), \forall u \in U$$

2.2 Linear Algebraic groups

Let $X \subseteq \mathbb{A}^n$and $Y \subseteq \mathbb{A}^m$ be two affine varieties. Then $X \times Y$ is likewise an affine variety. Indeed, we can consider $X \times Y$ as a subset of $\mathbb{A}^{n+m}$, and embed $K[X_1, ..., X_n]$ and $K[X_1, ..., X_m] \subseteq K[X_1, ..., X_{n+m}]$ so that if $X = V(S)$ and $Y = (S')$, then

$$X \times Y = V(S \cup S')$$

in other words $X \times Y$ is the set of zeros of the polynomials.

$$\begin{cases} f(X_1, ..., X_n), f \in S \\ g(X_{n+1}, ..., X_{n+m}), g \in S' \end{cases}$$

Definition 2.17. *An algebraic group G is a variety with a group structure such that*

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & xy \end{array}$$

and

$$\begin{array}{ccc} G & \to & G \\ x & \mapsto & x^{-1} \end{array}$$

are morphisms of varieties.

We may define a morphism of algebraic groups $f : G \longrightarrow G'$ to be a morphism of varieties which is also a group homomorphism.

Our basic example is the variety $\mathrm{GL}(n, K)$ endowed with the usual group structure. Since the product and the inverses of matrices are given by polynomial equations, $\mathrm{GL}(n, K)$ is an algebraic group.

Definition 2.18. *We call a linear algebraic group every closed subgroup of* $\mathrm{GL}(n, K)$.

It follows that every linear algebraic groups is an algebraic group.

Examples **2.19.** *For example* $\mathrm{SL}(n, K) = \{A \in \mathrm{GL}(n, K) \mid detA = 1\}$ *is a closed subset of* $\mathbb{A}^{n^2}$ *as we have already seen, and it is also a subgroup of* $\mathrm{GL}(n, K)$*; that is* $\mathrm{SL}(n, K)$ *is a linear algebraic group.*

Proposition 2.20. *Let* G *be a linear algebraic group, and* $H \leq G$*. The Zariski closure* $\bar{H}$ *is also a subgroup of* G*. Hence,* $\bar{H}$ *is a linear algebraic group. Moreover, if* $H \trianglelefteq G$*, then* $\bar{H} \trianglelefteq G$*.*

Proposition 2.21. *Let* G *be a linear algebraic group. Then :*

❶ *The irreducible components form a partition of* G*.*

❷ *The identity element* $1 \in G$ *lies in exactly one irreducible component which we denote* G^0*.*

❸ G^0 *is closed normal subgroup of finite index in* G

❹ *Every closed subgroup of finite index contains* G^0*; so* G^0 *is the smallest closed subgroup of finite index in* G*.*

Proof.

❶ Let X,Y be two distinct irreducible components of G. Assume for a contradiction that there exists an element $g \in X \cap Y$. Since multiplication by g^{-1} is a morphism of G onto itself, $g^{-1}X$ and $g^{-1}Y$ are irreducible and $1 \in g^{-1}X \cap g^{-1}Y$. Therefore, without loss of generality we may assume that $1 \in X \cap Y$. Now, XY is irreducible as it is the image of the irreducible subset $X \times Y$ by the multiplication in G. We have $X = X \cdot 1 \subseteq XY$ and $Y = 1 \cdot Y \subseteq XY$, so by the maximality of X,Y we get $X = XY = Y$, a contradiction, hence $X \cap Y = \emptyset$.

❷ It follows at once from the above part, that 1 lies in exactly one component.

❸ We have G^0 is an irreducible component, so $(G^0)^{-1}$ its image by the $g \mapsto g^-$ is an irreducible component. We have $1 \in G^0 \cap (G^0)^{-1}$. Thus, $G^0 = (G^0)^{-1}$. Similarly $G^0 \cdot G^0$ is irreducible and contains G^0, hence by the maximality of G^0 we have $G^0 \cdot G^0 = G^0$. This proves that G^0 is a subgroup of G.

For $x \in G$, we have $x^{-1}G^0x$ is again an irreducible component, as an isomorphic image of G^0 and $1 \in G^0 \cap g^{-1}G^0g$. Therefore $G^0 = g^{-1}G^0g$, so G^0 is normal.

Let X be any irreducible component of G. If $g \in X$, then $1 \in g^{-1}X$ and so $g^{-1}X = G^0$. It follows that $X = gG^0$; thus the components of G are exactly the cosets of G^0. Since G^0 is noetherian, there are only finitely many components of G, hence G^0 has finite index in G.

❹ Let $H \leqslant G$ be a closed subgroup of finite index. Obviously, $H^0 \leqslant G^0 \leqslant G$. Now, $|G : H^0| = |G : H||H : H^0|$ is finite by the thrid part. Thus H^0 has finite index in G^0, and it follows that G^0 is a disjoint union of a finite number of cosets of H^0; but G^0 is irreducible, so $G^0 = H^0 \subseteq H$.

□

The subgroup G^0 is called the identity component of G.

Definition 2.22. *An algebraic group G is said to be connected if $G = G^0$.*

Proposition 2.23. *If $H, K \leq G$ are subgroups of a linear algebraic group such that K is closed and connected, then commutator $[H, K]$ is closed and connected.*

It follows for instance that if G is connected, then the terms of the derived series and the lower central series are closed and connected.

Remark 2.24.

- *If $\varphi : G_1 \longrightarrow G_2$ is a morphism of linear algebraic groups, then*

$$\dim(G_1) = \dim(Im\varphi) + \dim(Ker\varphi)$$

- $\dim G = \dim G^0$.
- $\dim(\mathrm{GL}(n, K)) = n^2$ *and* $\dim(\mathrm{SL}(n, K)) = n^2 - 1$.

2.3 Semisimple linear algebraic groups

Let G be a linear algebraic group. Then we can consider a soluble normal subgroup of G of maximal dimensions. As we have seen the closure $\bar{S}$ of S is likwise normal and soluble, so we may assume that $\bar{S} = S$, and so S is closed. Moreover, if N is any normal subgroup of G which is soluble, then NS is also soluble, so by maximality of S we have $N \subseteq S$. It follows that S contains all the normal soluble subgroups of G. we have established.

Proposition 2.25. *Let G be a linear algebraic group. Then there is a unique largest normal soluble subgroup of G, moreover this subgroup is closed.*

Definition 2.26. *The radical of an algebraic group G is the identity component of the largest normal soluble subgroup of G.*

Note that by definition, the radical of a linear algebraic group is connected.

Definition 2.27. *A linear algebraic group is said to be semi-simple if it is connected and has trivial radical.*

2.4 Reduction for the Tits alternative.

The aim of this section is to show that the Tits alternative follows from the following theorem.

Theorem A. *Let $\Gamma \leq \mathrm{GL(n,K)}$ be a connected semi-simple linear algebraic group, which has a Zariski dense finitely generated subgroup G. Then G on 2-generators free subgroup.*

Assume that Theorem A, is proved, and let G be a finitely generated subgroup of $\mathrm{GL(n,K)}$ which is not virtually soluble. Denote by T the Zariski closure of$G$, and let $G^0 = G \cap T^0$.
Since T^0 has finite index in T, it follows that

$$G/G^0 = G/G \cap T^0 \simeq GT^0/T^0 \subseteq T/T^0$$

is finite. Assume that:

- T^0 is not soluble. Otherwise, $G^0 = G \cup T^0$ is soluble, and so G is virtually soluble which contradicts our assumption.
- G^0 is finitely generated.
  This follows at once from proposition 1.

Let $\mathcal{R}$ be the soluble radical of T^0. By 1 we may assume that $T^0/\mathcal{R}$ is not trivial.

If we put $T = T^0/\mathcal{R}$, then T is a semi simple connected algebraic group. Moreover, $G^0\mathcal{R}/\mathcal{R}$ of T, and $G^0\mathcal{R}/\mathcal{R} \simeq G^0/G^0 \cup \mathcal{R}$ is finitely generated by 2. If follows that T meets the condition of theorem A, thus $G^0/G^0 \cup \mathcal{R}$ contains a 2-generated free subgroup

$$\bar{F} = F(G^0 \cup \mathcal{R})/G^0 \cup \mathcal{R}$$

Now: F is a subgroup of G^0, and $F/F \cup (G^0 \cup \mathcal{R})$ is a free group; Since extension by a free group splits, it follows that $F = F \cup (G^0 \cup \mathcal{R}).F_1$ where F_1 is a subgroup of T and so $F_1 \leqslant G^0$. Moreover $F_1 \simeq F/F \cup (G^0 \cup \mathcal{R})$ is free on 2-generators.
This proves that $G^0$and so Gcontains a free non-abelian subgroup. The later argument shows that theorem A implies the Tits alternative, The next chapter will be devoted to sketching the proof of theorem A.

Chapter 3

On the proof of Theorem A

3.1 Projective transformations and Proximal elements

In this section we follow the approach of Breuillard and Gelender [2, 1] to construct proximal elements. The role of notions presented below in the proof of the Tits Alternative will be clear later.

3.1.1 Local fields

An absolute value on a field K is a map

$$|.| : K \longrightarrow [0, +\infty[$$

which satisfies

❶ $|x| = 0 \Leftrightarrow x = 0$.

❷ $|x.y| = |x||y|$.

❸ $|x + y| \leqslant |x| + |y|$.

If instead of (3) the strongest inequality $|x + y| \leqslant \max\{|x|, |y|\}$ holds, we say that the absolute value is non-archimedian.

As an example, we have the usual absolute value $|.| : \mathbb{Q} \longrightarrow \mathbb{R}$ defined

$$|x| = \begin{cases} x \text{ if } x \geqslant 0 \\ -x \text{ otherwise .} \end{cases}$$

Let p be a prime number. For every integer $0 \neq a \in \mathbb{Z}$ we define $v_p(a)$ to be the largest power of p which divides a; and we set $v_p(0) = \infty$. For example, we have for $a = 120 = 2^3 \times 3 \times 5$, $v_2(120) = 3$, $v_3(120) = 1$, $v_5(120) = 1$ and $v_p(120) = 0$, if $p \neq 2, 3, 5$. We extend v_p to $\mathbb{Q}$ by setting

$$v_p(a/b) = v_p(a) - v_p(b).$$

The map $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ is called the p-adic valuation on $\mathbb{Q}$ and it satisfies:

(i) $v_p(ab) = v_p(a) + v_p(b)$.

(ii) $v_p(a + b) \geqslant \min\{v_p(a), v_p(b)\}$.

It follows that the map

$$\begin{array}{rccc} |.|_p : \mathbb{Q} & \to & [0, +\infty[\\ x & \mapsto & p^{-v_{p(x)}} \end{array}$$

is a (non-archimedian) absolute value on Q.

An absolute value $|.|$ on field K define a distance on K by setting:

$$d(x, y) = |x - y|$$

So K can be viewed as a metric space. If K is complete with respect to this metric we say that K is a local field.

For example, $\mathbb{Q}$ is not complete neither for the usual absolute value $|.|$, nor for the p-adic absolute values $|.|_p$, p a prime. However, we can complete $\mathbb{Q}$ with respect to each of these absolute values, and obtain $\mathbb{R}$ in the first case, and the field of p-adic numbers $\mathbb{Q}_p$, for each prime p. The fields $\mathbb{R}$ and $\mathbb{Q}_p$ are local fields.

3.1.2 Projective transformations

Let K be a local field.

❶ Assume first that K is archimedian, so $K = \mathbb{R}$ or $\mathbb{C}$ by a well-known theorem of Ostrowski. And denote by $\|.\|$ the canonical euclidean norm of K^n:

$$\|x\| = \sqrt{\sum_{i=1}^{n} |x_i|^2} \text{ Where} x = (x_1, ..., x_n)$$

One can consider the Cartan decomposition (see [3]) of SL(n, K):

$$\mathrm{SL(n,K)} = BAB$$

where $B = \mathrm{SO}_n(\mathbb{R})$ or $B = \mathrm{SU}_n(\mathbb{C})$, according to the case $K = \mathbb{R}$ or $\mathbb{C}$; and

$$A = \{ \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} \mid a_{11} \geqslant ... \geqslant a_{nn} > 0 \text{ and } \prod_{i=1}^{n} a_{ii} = 1 \}$$

Any element $g \in \mathrm{SL(n,K)}$ can be decomposed as $g = b_g a_g b'_g$, where $a_g \in A, b_g, b'_g \in B$.

❷ Assume now that K is non-archimedian and let $O_K = \{x \in K \mid |x| \leqslant 1\}$ be its valuation ring. We define a norm on K^n by setting
$\|x\| = \max_i |x_i|$, where $x = (x_1, ..., x_n)$
Then

$$\mathrm{SL(n,K)} = BAB$$

where $B = \mathrm{SL(n, O_K)}$ and

$$A = \{ \begin{pmatrix} \pi^{\delta_1} & & 0 \\ & \ddots & \\ 0 & & \pi^{\delta_n} \end{pmatrix} \mid \delta_i \in \mathbb{Z}, \delta_i \leqslant \delta_{i+1} \text{ and } \sum \delta_i = 0 \}$$

where π is uniformizing element for K.

In both cases the norm on K^n gives rise to a canonical form on the exterior product $\wedge^2 K^n$.
Now consider the projective space $\mathbb{P}^{n-1}(K)$ on K.
Recall that the elements of $\mathbb{P}^{n-1}(K)$ are equivalente classes with respect to the relation:

$$x \sim y \Leftrightarrow \exists \lambda \in K^* : x = \lambda y$$

Where $x, y \in K^n$. We denote the class of $x \in K^n$ in $\mathbb{P}^{n-1}(K)$ by $[x]$. We can define a metric on $\mathbb{P}^{n-1}(K)$ by setting

$$d([x],[y]) = \frac{\|x \wedge y\|}{\|x\|\|y\|}$$

(This metric is easily seen to be well defined).

Remarks

(a) The map d is a distance on $\mathbb{P}^{n-1}(K)$ which induces the topology defined by the local field K.

(b) d is ultra-metric if K non archimedian; that is $d([x],[y]) \leqslant \max\{d([x],[z]), d([y],[z])\}$ for all $x, y, z \in K^n$.

(c) If f is a linear form on K^n, $f : K^n \longrightarrow K$ then for every non zero vector $x \in K^n$, we have

$$d([x], [\ker f]) = \frac{\|f(x)\|}{\|f\|.\|v\|}$$

(d) The compact group K acts as an isometry group on $\mathbb{P}^{n-1}(K)$; that is

$$d(g[x], g[y]) = d([x], [y])$$

For all $g \in K$ and $x, y \in K^n$. Here $g[x]$ is defined as usual to be the class of the vector $[g.x]$.

As usual, denote by PGL(n, K) the quotient of GL(n, K) by its center. Note that the center of GL(n, K) is formed by all the diagonal matrices λI_n, with $\lambda \in K$ satisfies $\lambda^n = 1$.
There is a natural action of the projevtive special linear group PGL(n, K) on the projective space $\mathbb{P}^{n-1}(K)$: for a projective transformation $[g]$, and an element $[v] \in \mathbb{P}^{n-1}(K)$. we define $[g][v] = [gv] \in \mathbb{P}^{n-1}(K)$. obviously, this action is well defined.
For subset $S \subseteq \mathbb{P}^{n-1}(K)$, and a real number $\epsilon > 0$, we define the ϵ-neighborhood of S to be the set $\{v \in \mathbb{P}^{n-1}(K) \,|\, d(v, s) < \epsilon\}$. Note that if $S = \{w\}$, then the ϵ-neighborhood of S is just the open ϵ-ball centered at w.

Definition 3.1. *Let $\epsilon > 0$. A projective transformation $[g]$ is said to be ϵ-contracting if the following hold:*

- *There exists a projective point $v_g \in \mathbb{P}^{n-1}(K)$ called an atractting point of $[g]$.*
- *There exists a hyperplane $H_g \subseteq \mathbb{P}^{n-1}(K)$, called a replusive hyperplane of $[g]$ such that:*
  $[g]$ maps the complement of the ϵ-neighborhood of H_g into the ϵ-ball centered at v_g.

For an element $g \in$ GL(n, K), the diagonal matrix a_g which arises in the decomposition of g as an element of BAB is uniquely determined. We denote by $a_1(g), ..., a_n(g)$ the diagonal enties of a_g, listed in a decraesing order.

Proposition 3.2. *Let $\epsilon < 1/4$. If $|\frac{a_2(g)}{a_1(g)}| \leqslant \epsilon^2$, then $[g]$ is ϵ-contracting then $|\frac{a_2(g)}{a_1(g)}| \leqslant \frac{\epsilon^2}{\pi}$ if K is non-archimedian with uniformizing π; and $|\frac{a_2(g)}{a_1(g)}| \leqslant 4\epsilon^2$ if K is archimedian.*

Proof. See [1, Prop 3.3] □

Definition 3.3. *A projective transformation $[g]$ is called (r, ϵ)-proximal $(r > 2\epsilon > 0)$ if it is ϵ-contracting some repulsive hyperplane H_g such that*

$$d(v_g, H_g) \geqslant r$$

.

3.1.3 Ping-Pong tuples and free groups

An m-tuple $(a_1, ..., a_n)$ of element of PGL(n, K) is called a ping-pong m-tuple if :

- For every i, a_i and a_i^{-1} are (r, ϵ)-proximal elements for some $r > 2\epsilon > 0$.
- If v_i^+ and H_i^+, v_i^- and H_i^- are the attracting points and the repulsive hyperplanes of a_i and a_i^{-1} respctively, then $d(v_i^{\pm}, H_j^{\pm}) > r$, whenever $i \neq j$. The main result here is the following.

Proposition 3.4. *Every ping-pong m-tuple $(a_1, ..., a_n)$ in* PGL(n, K) *generates a free group of rank m; that is $\langle a_1, ..., a_m \rangle$ is a free subgroup of* PGL(n, K)*, of rank m*

3.1.4 Constructing ping-pong tuples

Let F be a finite subset of $\mathrm{PGL}(n, K)$, r a positive real number, and $m \in \mathbb{N}$. we may that F is (m, r)-separating if for every $2m$ point $v_1, ..., v_{2m}$ in $\mathbb{P}^{n-1}(K)$ and $2m$ hyperplanes $H_1, ..., H_{2m} \subseteq \mathbb{P}^{n-1}(K)$, there exists an element $\gamma \in F$ such that: $d(\gamma v_i, H_j)) > r$ and $d(\gamma^{-1} v_i, H_j > r$ for all $i \neq j)$.
A proof of the following key result can be found in[2, 1, Section 3] .

Proposition 3.5. *Let F be an (m, r)-separating set in* PGL(n, K)*. Then $\exists C > 1$ such that for every ϵ with $0 < \epsilon < 1/C$ we have*

- *For every ϵ-contracting transformation $[g] \in$ PGL(n, K), there exists $[f] \in F$ such that $[f^g]$ and its inverse are (C, ϵ)-contracting.*
- *If $a_1, ..., a_n \in \mathrm{PGL}(n, K)$, and γ is a projective transformation such that γ and γ^{-1} are ϵ-contracting, there exist $h_1, ..., h_n, g_1, ..., g_m \in F$ so that*

$$(g_1 \gamma a_1 h_1, g_2 \gamma a_2 h_2, ..., g_m \gamma a_m h_m)$$

is a ping-pong m-tuple.

3.2 Representation theory, and a sketch of the final step in the proof

The book of G. Malle and D. Testerman [11] contains a good chapter on the representation theory of linear algebraic groups, which we shall refer to it frequently. We shall also refer the reader frequently to the paper by Breuillard and Gelander [2] which contains the main core of the proof.

3.2.1 Representations of abstract groups

Let G be a group, and V be K-vector space of finite dimension. A linear representation of G over V is a group morphism $\rho : G \to GL(V)$. The dimension of the representation ρ is, by definition, the dimension of V.

It is convenient to denote $\rho(g)(v)$ by $g.v$, for $g \in G$ and $v \in V$. A subspace W of V is invariant if $g.w \in W$, for all $g \in G$ and all $w \in W$. If V contains no invariant subspace other than V and $\{0\}$, we say that ρ is an irreducible representation. We say that ρ is semisimple if V can be expressed as a direct sum $V = \bigoplus_i V_i$, where each subspace is invariant and the restriction

$$\rho_{V_i} : G \to GL(V_i)$$

is irreductible.

For every $\rho : G \to GL(V)$. We can associate a map called the character of ρ, defined by

$$\mathcal{X} : G \to K$$

$$g \mapsto \mathrm{Tr}(\rho(g))$$

where $\mathrm{Tr}(\rho(g))$ is the trace of the matrix associated to the linear map $\rho(g)$ with respect to any basis of V.

3.2.2 Representations of algebraic groups

Let G be an algebraic group of over a field K, and V be a finite dimensional vector space over K.

A representation $\rho : G \to GL(V)$ is said to be *rational* if ρ is a rational map; that is to say ρ is a morphism of algebraic groups.

The rational representations of an algebraic group G of degree 1 are called *the characters* of G; hence, a character χ of G is a morphism of algebraic groups $\chi : G \to K^\times$. The characters of G are denoted by $\mathbb{X}(G)$, and they form a group under the addition:

$$(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g)$$

.

A torus in the algebraic group G is a subgroup which is isomorphic to $K^\times \times \cdots \times K^\times$ for some n, where $K^\times$ is the miltiplicative group of the field on which G is defined. It is worth mentioning that all the maximal tori in G are conjugate; and the dimension of one of these maximal tori is know as *the rank* of G and denoted by $\mathrm{rk}(G)$.

To each maximal torus T one can assign a root system Φ (with basis $\Delta \subseteq \Phi^+$) see [11]).The group $N_G(T)/T$ is called the Weyl group of G. For any rational representation $\rho : G \to \mathrm{GL}(V)$ of G, we have

$$V = \bigoplus_{\chi} V_\chi$$

where χ runs over the characters of the maximal torus T, and $V = \{v \in V \,|\, \rho(t)v = \chi(t)v, \forall t \in T\}$

Definition 3.6. *Under the above notation, every charcter χ of T such that $V_\chi \neq 0$ is called a weight of V with respect to the torus T and $V - \chi$ is called a weight espace of V.*

3.2.3 Completion of the proof

Throughout, assume that L is a field which is finitely generated over its prime subfield ($\mathbb{Q}$ or $\mathbb{F}_p$ according to the characteristic of L). Let G be an algebraic group over L, such that the connected component G^0 is semisimple. Assume also that we have a finitely generated subring R of L. Fix a rational representation $\rho' : G \to \mathrm{GL}(d, L)$; so the set $G(R)$ of R-rational points of G is mapped into $\mathrm{GL}(d, R)$ by ρ'. The main theorem in this section is the following.

Theorem 3.7. *(See [2, Theorem 4.3])*
Let $\Omega_0 \subset G^0(R)$ be a Zariski-dense subset of G^0 with $\Omega_0 = \Omega_0^{-1}$. Suppose $\{g_1, \cdots g_n\}$ is a finite subset of $G(L)$ whose image in G/G^0 covers the whole G/G^0, and let

$$\Omega = g_1\Omega_0 g_1^{-1} \cup \cdots \cup g_m\Omega_0 g_m^{-1}$$

Then we can find a number $r > 0$, a local field K, an embedding $L \hookrightarrow K$ and a (strongly) irreducible projective representation $\rho : G(L) \to \mathrm{PGL}(d, K)$ defined over L with the following property. If $\epsilon \in [0, \frac{r}{2}]$ and $a_1, \ldots a_n \in G(L)$ are n arbitrary points, then there exist n elements $x_1, \ldots x_n$ with

$$x_i \in \Omega^{4m+2} a_i \Omega$$

such that the $\rho(x_i)^{\pm 1}$'s are (r, ϵ)-proximal transformations on $\mathbb{P}(L^d)$, and the $\rho(x_i)$'s form a ping-pong n-tuple.

As an immediate consequence, by Proposition 3.4, the elements $\rho(x_i)$, for $i = 1, \ldots n$, generate a subgroup isomorphic to the free group F_n.

We can now deduce Theorem A. Let G be a finitely generated linear group, and let Γ be its Zariski closure. By the assumptions of Theorem A, we may assume that Γ is a connected semisimple algebraic group (so in particular $\Gamma = \Gamma^0$).

Let $H \leqslant G$ be a subgroup of finite index, let $g_1, \ldots, g_n$ be arbitrary elements of G, and $\Omega_0 = \pi(\bigcap_{i=1}^m g_i H g_i^{-1})$, where $\pi : G \to \Gamma$ and K is the base field of G. It follows

that Ω_0 is a dense subset of $\Gamma = \Gamma^0$ which satisfies obviously $\Omega_0^{-1} = \Omega_0$. By the last theorem, the elements $\pi(g_1), \ldots, \pi(g_n)$ form a ping-pong n-tuple, so they generate a free group.

Remark 3.8. *The above argument yields in fact a stronger result. Firstly, the assumption in Theorem A that* Γ *is connected can be dropped; and secondly, for every* $H \leqslant G$ *of finite index, any choice of* $g_1, \ldots, g_n \in G$ *yields an* n*-tuple* $(a_1, ..., a_n)$ *that generate a free group and such that* $a_i = g_i \mod H$ *for all* i*.*

The appraoch that we followed yields results which are more strong than the Tits alternative.

Theorem 3.9 (see Theorem 1.3 in [2])**.** *Let* K *be a local field and* Γ *a subgroup of* $\mathrm{GL}(n, K)$*. Then* Γ *contains either an open solvable subgroup or a dense free subgroup (with respect to the topology induced by that of the absolute value on* K*).*

The later was called by Breuillard and Gelander **the topological Tits alternative**.

A version of the Tits alternative that is slightly modified from the one that we have already mentioned can be stated as follows (this version can be also found in Tits' paper [16]).

Theorem 3.10. *Let* L *be a field and* G *be a finitely generated subgroup of* $\mathrm{GL}(n, L)$*. Then* G *contains either a Zariski open soluble subgroup or a Zariski dense free subgroup of finite rank.*

The last theorem can be deduced from the topological Tits alternative as follows:

Consider $G \leqslant \mathrm{GL}(n, L)$ as in the last theorem, and let $\mathcal{R}$ be the subring of L generated by all the entries of the matrice in G. A theorem Noether (the Noether normalization theorem) implies that $\mathcal{R}$ can be embeded in the valuation ring $\mathcal{O}$ of some local field K, hence G can be embeded in the linear group $\mathrm{GL}(n, \mathcal{O})$.
The topology induced on G from the Zariski topology of $\mathrm{GL}(n, L)$ coincides with that induced from the Zariski topology of $\mathrm{GL}(n, K)$, and the later is weaker than the topology induced by the local field K (since the polynomail functions on K are continuous with respect to the later topology). If the image of G in $\mathrm{GL}(n, K)$ contains an open solvable subgroup, then so the closure of G. Hence, G is virtually solvable, and its Zariski connected conponent is solvable and Zariski open. Otherwise the image of G in $\mathrm{GL}(n, K)$ does not contains an open soluble subgroup, hence by the topological Tits alternative, it contains a dense free subgroup (which can be chosen to be of finite rank). This free subgroup is Zariski dense.

The topological Tits alternative has applications to Lie groups, to the theory of profinite groups, amenability.... For these, we refer the reader to [2]. (It remains to prove Theorem 3.7).

Chapter 4

The probabilistic approach and some applications of the Tits alternative

4.1 The work of M. Larsen and A. Shalev

4.1.1 Identities and Probabilistic identities

Let $w(x_1...x_n)$ be an element of F_n and let G be a group, we can define a map from G^n into G by sending each $(g_1, ..., g_n) \in G^n$ to the element $w(g_1...g_n) \in G$ obtained by replacing each indeterminate x_i by g_i. We call the later map the evaluation of the word w on G, and $w(g_1...g_n)$ the value of the word w on $(g_1...g_n)$.

For example, we have

1. For $w_1 = x_1^{-1}x_2^{-1}x_1x_2 \in F_2$, the associated evaluation map is given by

$$\begin{array}{ccc} G^2 & \to & G \\ (g_1, g_2) & \mapsto & [g_1, g_2] \end{array}$$

2. Consider, $w_2 \in F_3$ defined by

$$w_2 = x_2^{-1}x_1^{-1}x_2x_1x_3^{-1}x_1^{-1}x_2^{-1}x_1x_2x_3.$$

More concisely, $w_2 = [x_1, x_2, x_3]$; hence the associated evaluation is

$$\begin{array}{ccc} G^3 & \to & G \\ (g_1, g_2, g_3) & \mapsto & [g_1, g_2, g_3] \end{array}$$

3. For $w_3 = x^5 \in F_n$, we have

$$\begin{array}{ccc} G & \to & G \\ g & \mapsto & g^5 \end{array}$$

Definition 4.1. *We say that w is an identity for G if the map on G induced by w is trivial; that is to say $w(g_1...g_n) = 1 \ \forall g_1, ..., g_n \in G$.*

Examples 4.2.

1. *The word $w_1 = x_1^{-1}x_2^{-1}x_1x_2$ is identity of a group G if and only if $[g_1, g_2] = 1$, for all $g_1, g_2 \in G$. This holds if and only if G is abelien.*
2. *The group G satisfies the identity if and only if G is nilpotent of class ≤ 2.*

The previous definition can be relaxed to be more useful. For a ward $w \in F_n$, define

$$P_G(w) = \frac{|\{(g_1, ..., g_n) \,|\, w(g_1...g_n) = 1\}|}{|G|^n}$$

Obviously, we have

$$\frac{1}{|G|^n} \leq P_G(w) \leq 1.$$

We can interpret $P_G(w)$ as the probability for an n-tuple of elements of G to satisfies the identity w.

We can extend the later definition to the infinite groups which are residually finite.

Let $\mathcal{C}$ be a class of groups.

Definition 4.3. *A group G is said to be residually-$\mathcal{C}$ if*

$$\bigcap \{N \lhd G \,|\quad G/N \text{ is a } \mathcal{C}\text{-group}\} = \{1\}$$

that is to say that the intersection of all normal subgroups $N \lhd G$ such that G/N has the property $\mathcal{C}$, is trivial.

❶ We obtain the class of residually finite groups by taking $\mathcal{C}$ to be the class of finite groups. Therefore, a group G is residually finite if

$$\bigcap \{N \lhd G \,|\quad G/N \text{ is finite } \} = \{1\}$$

❷ If we take $\mathcal{C}$ to be the class of finite p-groups then G is said to be residually finite p-groups.

Proposition 4.4. *Let G be a group and $\mathcal{C}$ be a class of groups. Then G is residually-$\mathcal{C}$ if, and only if, for every $1 \neq g \in G$, there exists a epimorphism $\phi : G \longrightarrow H$, where H is a $\mathcal{C}$-group such that $\phi(g) \neq 1$.*

Proof. Assume that G is residually-$\mathcal{C}$, and let $g \in G$ with $g \neq 1$. As $\bigcap\{N \mid \quad G/N \text{ is a } \mathcal{C}\text{-group}\} = 1$, there exists $N \lhd G$ such that G/N is a $\mathcal{C}$-group, and $g \notin N$. Now, if we consider the canonical projection $\phi : G \to G/N$, then $\phi(g) \neq 1$.

In the reverse direction, assume for a contradiction that

$$\bigcap\{N \mid \quad G/N \text{ is a } \mathcal{C}\text{-group}\} \neq 1$$

and let $g \neq 1$ be an element in the later set. By assumption, there exists an epimorphism $\phi : G \longrightarrow H$, where H is a $\mathcal{C}$-group such that $\phi(g) \neq 1$. Now, $G/\ker\Phi \cong H$, so $\ker\Phi$ is an elemnt of the set $\{N \mid \quad G/N \text{ is a } \mathcal{C}\text{-group}\}$, so $g \in \ker\phi$, a contradiction. □

Let $w(x_1, ..., x_n) \in F_n$, and let G be a residually finite group. For each finite quotient G/N of N, we can define the probability $P_{G/N}(w)$ that the identity $w = 1$ holds in the finite group G/N.

Definition 4.5. *With the above notation, we say that w is a probabilistic identity for the residually finite group G if there exists $\epsilon > 0$, such that $P_{G/N}(w) \geqslant \epsilon$, for all $N \lhd G$ of finite index.*

Note that w is a probabilistic identity for G if and only if $\inf P_{G/N}(w)$ is positive, where the inf is taken over all the subgroups $N \lhd G$ of finite index.

The group G is said to satisfy a probabilistic identity if there exists a non-trivial word $w \in F_n$ (for some n) such that w is a probabilistic identity for G.

It seems convenient here to explain the relvance of the above definitions to the notion of Haar measures:

For a finite group G, the function

$$\mu : P(G) \to [0, +\infty[$$

which sends each $X \subseteq G$ into $\mu(X) = \dfrac{|X|}{|G|}$ is a (Haar) measure on G.

This measure extends to the cartesian product G^n; and $P_G(w)$ the probability that G satisfies the identity $w = 1$ is just

$$\mu\{(g_1, ..., g_n) \in G^n \mid \mu(g_1, ..., g_n) = 1\}.$$

More generally, a Haar measure on a compact topological group G, is a measure μ on G defined on the σ-algebra generated by all the closed subsets of G, such that :

1. $\mu(G)$ is finite.

2. $\mu(G)$ is finite, and μ is left invariant, that is to say that $\mu(gX) = \mu(X)$, for every mesurable subset of X.

By the finiteness of μ, we can always assume that μ is normalized, so that $\mu(G) = 1$. It is a well known result that such a measure exists on every (locally compact) topological group.

For every group G, we can define a topology by taking the normal subgroups of finite index of G to be a basis for the neighborhoods of the identity 1. This topology is called the profinite topology on G, and it makes G into a topological group.

The finite quotients $(G/N)_{N \lhd_f G}$ of G form an inverse system of finite groups, where the transition homomorphisms are defined whenever $N, M \lhd_f G$, and $N \subseteq M$ (so the indexing set of the system is the set of all the $N \lhd_f G$ ordered by reverse inclusion) and they are given by the natural projections

$$G/N \longrightarrow G/M$$

$$xN \longmapsto xM$$

If we view each of the quoteints G/N as a discrete topological group, then the inverse limit $\varprojlim(G/N)$ is naturally a topological group which is compact (this follows from the fact that $\varprojlim G/N$ is a closed subgroup of $\prod_{N \lhd_f G}(G/N)$, and $\prod_{N \lhd_f G}(G/N)$ is compact by Tychonov's theorem. Without details, we call the group $\varprojlim(G/N)$ the profinite completion of the group G, and we denote it by $\hat{G}$.

A residually finite group G can be embedded naturally in its profinite completion $\hat{G}$ via the map

$$i : G \longrightarrow \hat{G}$$

$$x \longmapsto (xN)_{N \lhd_f G}$$

Note that the map i is continuous when considering G as a topological group with respect to the profinite topology; it is injective exactly because G is residually finite, and its image is a dense subgroup of $\hat{G}$.

We say that G is a *profinite group* if the map i is a homeomorphism. Equivalently, a profinite group is a compact topological group in which the normal subgroups of finite index form a basis for the neighborhoods of the identity element of G.

Let us examine Haar measures on profinite groups more closely. Since a profinite group Γ is compact, each open subgroup H of Γ has finite index. Indeed, the set of left cosets $\Gamma/H = \{gH \mid g \in \Gamma\}$ form a partition of Γ which cannot be refined, so necessarily Γ/H is finite; this prove the claim.

Secondly, we have

$$\mu(H) = \frac{1}{|\Gamma : H|}$$

where μ denotes a normalized Haar measure on Γ. Indeed, if $g_1H, ..., g_nH$ are the left cosets in Γ modulo H, then

$$\mu(\coprod(g_iH)) = \mu(\Gamma) = 1.$$

On the other hand,

$$\mu(\coprod g_iH) = \sum_{i=1} \mu(g_iH) = n\mu(H)$$

so $\mu(H) = \dfrac{1}{n} = \dfrac{1}{|\Gamma : H|}$ as claimed.

It is worthnoting that a there is a unique (normalized) Haar measure on Γ, and under under suitable conditions, one has

$$\mu(X) = \inf \frac{|XN/N|}{|\Gamma/N|}$$

where the inf is takend over all the open normal subgroups of Γ; and X denotes a measurable subset of Γ.

The Haar measure on a profinite group Γ can be extended naturally to the cartesian product Γ^n, so for a word $w \in F_n$, we can speak in general about the probability that an identity w holds in Γ. More precisely, since the product in Γ is continuous map, the map

$$\Gamma^n \longrightarrow \Gamma$$

$$(g_1, ..., g_n) \longmapsto w(g_1, ..., g_n)$$

is always continuous. It follows that the fibers

$$B_x = \{(g_1, ..., g_n) \in \Gamma^n \,|\, w(g_1, ..., g_n) = x\}$$

are closed subsets in Γ^n, and consequently the B_x's are measurable. The set

$$B = \{(g_1, ..., g_n) \in G^n \,|\, w(g_1, ..., g_n) = 1\}$$

is the fiber of w on $x = 1$; so taking the measure $\mu(B)$ makes sense.

Definition 4.6. *We say that G satisfies the probabilistic identity $w = 1$, if $\mu(B) > 0$.*

For instance, if w is an identity for G then $B = G^n$; thus $\mu(B) = 1$. This proves that every identity in the profinite group G is a probabilistic identity in G.

The important thing here is that an identity w holds in a residually finite group G with a positive probability if and only if it holds with a positive probability with respect to the Haar measure in the profinite completion $\hat{G}$. To prove the last claim one needs deeper investigation of the Haar measures on a profinite groups; at this point, we refer the reader to [5, Chapter 16] .

The first main result that we wish to discuss here is the following.

Theorem 4.7 (see[9]). *Let G be a finitely generated linear group. Then G satisfies a probabilistic identity if and only if G is virtually soluble.*

Since a virtually soluble group satisfies an identity, it follows that every finitely generated linear group which satisfies a probabilistic identity, satisfies an identity.
It is natural to ask wether the some result holds for all the residually finite groups.

Open Problem. *Is every residually finite group which satisfies a probabilistic identity, satisfies an identity?*

A profinite group Γ is said to be randomly free if for every positive integer n, the set

$$\{(g_1, ..., g_n) \in \Gamma^n \mid \langle g_1, ..., g_n \rangle \simeq F_n\}$$

has measure 1.

We have implicitely assumed above that the sets of the form

$$X = \{(g_1, ..., g_n) \in G^n \mid \langle g_1, ..., g_n \rangle \simeq F_n\}$$

are measurable. To justify this assumption, note first that the subgroup $\langle g_1, ..., g_n \rangle$ is not free if and only if there exists $1 \neq w \in F_n$ such that $w(g_1, ..., g_n) =$. Thus if we set

$$X_w = \{(g_1, ..., g_n) \in G^n \mid w(g_1, ..., g_n) = 1\}$$

then

$$X = G^n - \cup_{w \neq 1} X_w$$

but we have already seen that every set X_w is measurable, and since the group F_n is countable it follows that $\cup X_w \mid w \in F_n, w \neq 1$ is likewise measurable, so X is measurable.

The last definition extends naturally to the class of residually finite groups.

Definition 4.8. *A residually finite group G is said to be randomly free if its profinite completion is randomly free.*

The second main result of this section is the following

Theorem 4.9 (see [9]). *A finitely generated linear group is either virtually soluble or randomly free.*

Proof. The proof depends heavily on Theorem 4.7. Let G be finitely generated linear group and assume that G is not virtually soluble. Hence by theorem 4.7, G satisfies no probabilistic identity. Let $\hat{G}$ be the profinite completion of G. For every $w \in F_n$, consider

$$X_w = \{(g_1, ..., g_n) \in \hat{G}^n \mid w(g_1, ..., g_n) = 1\}.$$

Since G satisfies no probabilistic identity, it follows that $\mu(X_w) = 0$, whenever $w \neq 1$. If we set

$$X = \{(g_1, ..., g_n) \in \hat{G}^n \mid \langle g_1, ..., g_n \rangle \simeq F_n\}$$

then , we have $X = \hat{G}^n - \cup_{w \neq} X_w$. Since the Haar measure is σ-additive, and the family $(X_w)_{w \in F_n}$ is countrable, we have

$$\mu(X) = \mu(\hat{G}^n) - \sum_{w \neq 1} \mu(X_w).$$

Hence $\mu(X) = \mu(\hat{G}^n) = 1$. □

Similar to the proof of the Tits alternative, the proof of Theorem 4.7 uses algebraic group theory. The use of the language of "affine schemes" makes an attempt to survey this proof here superfluous; we refer the reader directly to the paper [9].

We finish this section by mentioning the relvance to coset identities. A word $w \in F_n, w \neq 1$, is a coset identity of a group G if G contains a subgroup H of finite index, and there are $g_1, ..., g_n \in G$ such that

$$w(g_1 h, ..., g_2 h) = 1 \text{ for all } h_1, ..., h_n \in H$$

Proposition 4.10. *A residually finite group G which satisfies a coset identity, satisfies a probabilistic identity.*

The last proposition together with theorem 4.7 implies at once the following.

Theorem 4.11 (03)**.** *Every finitely generated linear group which satisfies a coset identity is virtually soluble.*

4.2 The word growth in groups

Let G be a finitely generated group, and X be a finite generating set of G. Then every element $g \in G$ can be written as finite product

$$g = x_1 x_2 \cdots x_n \quad \text{where } x_i \in X \cup X^{-1}$$

The above representation is not unique, so we can consider the set of all such representations, and define $l(g)$ the length of g to be the length of shortest word in that set. For each integer $n \geqslant 1$ we define $a_n(G)$ to be the number of the elements of the set

$$\{g \in G \,|\, l(g) \leqslant n\}$$

We can consider G as metric space with respect to the distance $d(g, h) = l(gh^{-1})$ for $g, h \in G$. Hence $a_n(G)$ may be interpreted as the size of the ball centred at 1 that has radius n in that metric space. It is worth mentioning that all the balls with the same radius have the same size, so $a_n(G)$ is in fact the size of any ball of radius n in G.
The function $n \to a_n(G)$ is termed the growth function of G (with respect to the generating set X).

Examples **4.12.**

❶ *For $G = \mathbb{Z}$, with respect to the generating set $\{1, -1\}$; the element of a given length n are exactly $\{n, -n\}$. It follows that*

$$a_n(G) = 1 + 2 + ... + 2 = 2n + 1$$

❶ *For every finite group G; $a_n(G)$ is constant for n large enough (in fact $a_n(G) = |G|$, for n greater than the maximal length of an element of G).*

Proposition 4.13. *Let F_d be a free group on d-generators on consider the natural generating set $X = \{x_1^{\pm 1}, ..., x_d^{\pm 1}\}$ of F_d. Then for every integer $n \geqslant 1$,*

$$b_n(F_d) = 2d(2d-1)^{n-1}$$

where $b_n(F_d)$ denotes the number of elements of F_d of length n.

Proof. Each element of F_d can be uniquely expresed as a reduced word, and the length of such an element is equal to the length of its corresponding reduced word. For $n = 1$ the reduced words of length 1 are the elements of X; so $b_1(F_d) = 2d$. Assume that the claim is proved for the reduced words of length n. Every word $w = y_1, ..., y_n$ of length n defines exactly $2d - 1$ reduced words of length $n + 1$, since these can be obtained by adding to w any letter $x \in X - \{y_n^{-1}\}$. Thus $b_{n+1}(F_d) = b_n(F_d)(2d - 1) = 2d(2d - 1)^n$ as desired. □

Corollary 4.14 (1)**.** *The growth function of F_d is given by*

$$a_n(F_d) = 1 + 2d \sum_{i=1}^{n} (2d-1)^{i-1}$$

Note that if we have an epimorphism $G \xrightarrow{\varphi} H$, and a generating set X of G; then $\varphi(X)$ is generating set of H. If $h \in H$ has a length $\leqslant n$ with respect to $\varphi(X)$, then any element $g \in G$ such that $\varphi(g) = h$, has length at most n with respect to X. Using this observation and the fact that every d-generated group G is an epimorphic image of F_d, one obtains the following.

Corollary 4.15 (2)**.** *Let G be a d-generated group, generated say by $g_1, ..., g_d$. Then the growth function of G with respect $X = \{g_1^{\pm 1}, ..., g_d^{\pm 1}\}$ satisfies*

$$a_n(G) \leqslant 1 + 2d \sum_{i=1}^{n} (2d-1)^{i-1}$$

Naturally, we may ask about how the growth function depends on the choice of the generating set.

Definition 4.16. *Two functions $f, g : \mathbb{N} \to \mathbb{R}$ are said to be equivalent if there exists a constant $c > 0$ such that*

$$f(n) \leqslant Ag(An) \text{ and } g(n) \leqslant Af(An)$$

We claim that two growth functions of the same group are equivalent. Indeed, consider a group G which is generated by two distinct finite subsets X and Y. We can express each element of X as product of elements of Y, and conversly each element of Y can be expressed as product of elements of X. If we take A to be the maximal length of all preceding expressions, then for each $g \in G$, $l_X(g) \leqslant A \cdot l_Y(g)$ and $l_Y(g) \leqslant A \cdot l_X(g)$, where $l_X(g), l_Y(g)$ denote the length of g with respect to X and Y respectively. This proves the claim. Hence, we can speak about the growth type of given finitely generated group G:

* We say that g has expenential growth if $\exists a, b > 1$ such that $a^n \leqslant a_n(G) \leqslant b^n$.
* We say that G has polynomial growth if there exists integer k, c such that

$$a_n(G) \leqslant kn^c$$

.

* We say that G has intermediate growth if its growth is niether polynomail nor exponential.

Remark 4.17.

1. *The above definition makes sense, since a function which is equivalent to a function of polynomial (resp, exponential) growth has likewise polynomial (resp, exponential) growth.*
2. *The growth of a group can be at most exponential. This follows from Corollary 4.15, and the fact that free groups have exponential growth. To see that F_d has exponential growth, observe first that $a_n(F_d) \geqslant a_n(F_2)$ and*

$$a_n(F_2) = 1 + 4\sum_{i=1}^{n} 3^{i-1} \geqslant 4^n$$

The interest in growth of groups was first motivated by Riemannian geometry: J. Milnor observed that some geometric problem can be reduced to the study of the growth function of the associated fondamental group. In this context Milnor made two famous conjectures:

Conjecture 1. *A finitely generated group has polynomial growth if and only if it is virtually nilpotent.*

Conjecture 2. *The growth of finitely generated groups is either polynomial or exponential.*

The second conjecture turned out to be false in general when Grigorchuk constructed groups of intermediate growth in 1980. Nevertheless, Conjecture 1 is true for linear groups.

Theorem 4.18. *A linear group has either polynomial or exponential growth.*

By the Tits alternative, we may assume that our group G is either virtually soluble, or contains a non-abelian free group. In the later case G should be of exponential growth as we have seen in Remark 1.17.(2). Otherwise, a Theorem of wolf (see [12]), we know that a soluble group has either exponential or polynomial growth.

The first conjecture is a Theorem now after the extraordinary work of Gromov on it.

Theorem 4.19 (Gromov's theorem)**.** *A finitely generated group G has polynomial word growth if and only if it is virtually nilpotent.*

The important thing to mention here is that the reduction of the problem to linear groups crucial, so the Tits alternative is of great importance for the proof. Details and more related subjects can be found in [12]. We also refer the reader to the bibliography therein for the results and the historical facts mentioned in this section freely.

4.3 Amenable groups

Let G be a group. A finitely additive measure on G is a map

$$\mu : \varphi(G) \to [0, +\infty[$$

which satisfies the following properties:

1. If $A, B \subseteq G$ are disjoint subsets then
$$\mu(A \cup B) = \mu(A) + \mu(B)$$
2. We have $\mu(gA) = \mu(A)$, for all $g \in G$ and $A \subseteq G$.
3. $\mu(G) > 0$.

A finitely additive measure need not be necessarily a measure in the customary sense: First we require that a finitely additive measure is defined on all the subsets, not only on the measurable ones; and secondly it need not be necessarily σ-additive.

Definition 4.20. *A group G is amenable if we can define a finitely additive measure on it.*

For instance, every finite group G is amenable. Indeed, set for every $X \subseteq G$,

$$\mu(X) = \frac{|X|}{|G|}$$

then μ is finitely additive measure.

Proposition 4.21. *The free group F_2 is not amenable.*

Proof. Assume that $F_2 = \langle a, b\rangle$, and that μ is a finitely additive measure on F_2. Let A^+, A^-, B^+ and B^- be the subsets of reduced words starting by a, a^{-1}, b and b^{-1} respectively. An element in A which is different from x, couldn't have x^{-1} as a second letter, so it lies either in xA^+, xB^+ or xB^-. This means that $A^+ - \{x\} = xA^+ \coprod xB^+ \coprod xB^-$ (a disjoint union). Using the fact that μ is invariant under transformation, it follows that $\mu(A^+) = \mu\{x\} + \mu(A^+) + \mu(B^+) + \mu(B^-)$ so $\mu\{x\} + \mu(B^+) + \mu(B^-) = 0$. But all in the last equation are non-negative. Thus, in particular $\mu(B^+) = \mu(B^-) = 0$. Now, the same argument applied on B^+ geilds $\mu(A^+) = \mu(A^-) = 0$. Finally, as $F_2 = A^+ \cup A^- \cup B^+ \cup B^-$, it follows that $\mu(F_2) = 0$, a contradiction. □

An old conjecture of J. Von Neuman asserts the following.

Conjecture 4.22. *A group G is non amenable if and only if it contains a subgroup isomorphic to F_2.*

First, note that subgroups and quotionts of an amenable groups are amenable. Indeed, let G be an amenable group with measure μ, $H \leqslant G$ and $N \lhd G$. Let T be left transversal for H in G (i.e, for each $x \in G, \exists t \in T$ such that $xH = tH$; and for $s, t \in T$, we have $sH \neq tH$ whenever $s \neq t$). We define a measure μ on H by setting $\mu_H(A) = \mu(T \cdot A)$, for all $A \subseteq H$. We have $\mu_H(H) = \mu(T.H) = \mu(G) > 0$; and for $A, B \subseteq H$, disjoints we have $T(A \coprod B) = (TA) \coprod (TB)$, hence

$$\mu_H(A \coprod B) = \mu(TA \coprod TB)$$

$$= \mu(TA) + \mu(TB) = \mu_H(A) + \mu_H(B)$$

This proves that μ_H is a finitely additive measure on H.

Now, we shall define a measure μ' on G/N by taking

$$\mu'(A) = \mu(\bigcup_i x_i N)$$

where $A = \{x_i N\}_i \subseteq G/N$. We leave the details of checking that μ' is finitely additive to the reader.

Therefore, if G is an amenable group, then G couldn't contains a copy of F_2; otherwise F_2 would be amenable which contradicts the last proposition. We have established the following.

Corollary 4.23. *A group which contains a copy of F_2 is not amenable.*

This corollary proves one direction in Von Neuman's conjecture. The reverse implication, *viz.,* a non-amenable group contains a copy of F_2 is much more subtle. We know after the work of Ol'shanski that "Tarski Monsters" are non-amenable, though they are

torson groups, so they do not contain a copy of F_2. This refutes the conjecture of Von Neuman in general.

Other counter-examples are provided by the free Burnside groups $B(d, n)$, for n large enough. The last result is due to S.I. Adyan (1982).

More recently, Ol'shanski and Mark Sapir(2003) gave counter-examples to the conjecture which are finitely presented.

By the Tits alternative we can prove that Von Neuman's conjecture holds for linear groups. More precisely we have

Theorem 4.24.

❶ *If G is finitely generated linear group which is non-amenable, then G contains a copy of F_2.*

❷ *If G is a linear group over a field of characteristic zero, and G is non-amenable; then G contains F_2 as subgroup.*

Clearly, to prove the last theorem, we have only to show that if our group G is non-amenable, then it couldn't be virtually soluble. Equivalently we need to prove the following.

Theorem 4.25. *A linear group is amenable if and only if it is virtually soluble.*

Proposition 4.26. *Every virtually soluble group is amenable.*

Proof. A soluble group can be obtained by successive extensions involving only abelian groups. Thus to prove the claim, it is enough to prove the following:

(1) Every abelian group is amenable.

(2) An extension of an amenable group by an amenable groups is likwise amenable.

(3) A finite group is amenable.

The last statement is already shown in the begining of the section. We shall prove (2) and refer the reader to the litterature for (1). See for instance [12].

So let G be a group and $N \lhd G$ such that G/N and N are amenable. Let ν,η be finitely additive measures on N and G/N respectively, and let$A \subseteq G$. For each $xN \in G/N$, define

$$f(xN) = \nu(N \cap (xA))$$

We claim that f is a well defined function on G/N. So let $y \in xN = Nx$, hence $y = nx$, for some $n \in N$.

We have

$$\nu(n(N \cap xA)) = \nu(nN \cap nxA) = \nu(N \cap yA)$$

So $\nu(N \cap xA) = \nu(N \cap yA)$, as desired. Define $\mu(A) = \int f d\eta$, where

$$\int f d\mu = inf\{\sum_{i=1}^{k} \eta(A_i)a_i\}$$

and the inf is taken over all the subdivisions $\{a_0, ..., a_n\}$ of $f(G/N)$, and $A_i = \{\bar{x} \in G/N \mid \quad a_{i-1} \leqslant f(\bar{x}) < a_i\}$.
Now, μ is the desired measure on G.

□

Conclusion

The importance of the Tits alternative suggests that an analogue of it for other classes of groups (other than the linear ones) should be of great interest. The work of Breuillard and Gelander suggests that the ideas in the proof of the Tits alternative could be taken further to prove more strong results. Also, the probabilistic approach looks quite promicing in understanding the behaviour of groups (finite of infinite). The lack of time prevented us from speaking about the relevance to the Banach-Tarski Paradox, and to Kazhdan's property (T), so the subject is very rich. Those topics might be our main axe of researech in the following years.

Bibliography

[1] E. Breuillard and T. Gelander, A topological Tits Alternative, *J. Algebra* **261** (2007), 448-467.

[2] E. Breuillard and T. Gelander, On dense free subgroups of Lie groups, *J. Algebra*

[3] F. Bruhat and J. Tits, Groupes réductifs sur un corps local, I. Données radicielles valuées, Publ. Math. *IHES* **41** (1972), 5-251.

[4] J. Dixon, M. du Sautoy, A. Mann, D. Segal, Analytic pro-p Groups, second ed., Cambridge Univ. Press, 1999.

[5] M.D. Fried and M. Jarden, Filed arithmetic, Springer-Verlag, (1986).

[6] The GAP Group, GAP Groups, Algorithms, and Programming, www.gap-system.org.

[7] D. Gorenstein, Finite groups, Chelsea, New York, 1980.

[8] R. Hartshorn, Algebraic Geomtry, GTM , Springer-Verlag, 1976.

[9] M. Larsen and A. Shalev, A probabilistic Tits alternative,

[10] D. Gorenstein, Finite groups, Chelsea, New York, 1980.

[11] G. Malle and D. Testerman, Linear Algebraic Groups and Finite Groups of Lie Type, Cambridge University Press, 2011.

[12] A. Mann, How groups grow, Cambridge University Press, 2015.

[13] B. Huppert, Endliche Gruppen. I. *Die Grundlehren der Mathematischen Wissenschaften*, Band 134. Springer-Verlag, Berlin, 1967.

[14] B. Huppert and N. Blackburn, Finite Groups II, Springer-Verlag, Berlin, 1982.

[15] I.M. Isaacs, Finite group theory, AMS, Providence, RI, 2008.

[16] J. Tits , Free subgroups in linear Groups, Journal of algebra 20,250-270, 1972.

[17] V.D. Mazurov and E. I. Khukhro, The Kourovka Notebook. Unsolved Problems in Group Theory. 18th Edition, Russian Academy of Sciences, Siberian Division, Institute of Mathematics, Novosibirsk, 2014.

[18] D. J. S. Robinson, A Course in the Theory of Groups, 2nd ed. New York: Springer-Verlag, 1995.

[19] D. Segal and A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math.* Soc.(2) **55** (1997), 320-334.

[20] J.- P. Serre, Corps locaux, Hermann, Paris, 1968.

Abstract

In this note, we discuss the Tits alternative which asserts that every finitely generated linear group contains either a normal soluble subgroup of finite index or a free non-abelian subgroup.

Key words: Group , free group, Tits alternative, finitely generated group, linear group, Representation of group, identities, probabilistic identities, amenable .

Résumé

Dans cette note, nous discutons de l'alternative Tits qui affirme que tout groupe linéaire fini généré contient soit un sous-groupe résoluble normal d'indice fini, soit un sous-groupe libre non abélien.

Mots clés: Groupe, Groupe libre, Alternative Tits, Groupe fini généré, Groupe linéaire, Représentation du groupe, Identités, identités probabilistes, Groupe acceptable.

ملخص

ناقشنا في هذه المذكرة متباينة Tits والتي أكد فيها بأن كل زمرة منتهية التوليد إما أن تحتوي على زمرة جزئية قابلة للحل منتهية الدليل أو زمرة جزئية غير تبديلية .

الكلمات المفتاحية : زمرة , زمرة جزئية , زمرة حرة, متباينة Tits, زمرة منتهية التوليد,زمرة خطية, تمثيل الزمر, المتطابقات, احتمالي المتطابقات, الزمرة القابلة للتغيير.