The Tits Alternative

Matthew Tointon

April 2009

0 Introduction

In 1972 Jacques Tits published his paper *Free Subgroups in Linear Groups* [Tits] in the Journal of Algebra. Its key achievement was to prove a conjecture of H. Bass and J.-P. Serre, now known as the Tits Alternative for linear groups, namely that a finitely-generated linear group over an arbitrary field possesses either a solvable subgroup of finite index or a non-abelian free subgroup.

The aim of this essay is to present this result in such a way that it will be clear to a general mathematical audience. The greatest challenge in reading Tits's original paper is perhaps that the range of mathematics required to understand the theorem's proof is far greater than that required to understand its statement. Whilst this essay is not intended as a platform in which to regurgitate theory it is very much intended to overcome this challenge by presenting sufficient background detail to allow the reader, without too much effort, to enjoy a proof that is pleasing in both its variety and its ingenuity.

Large parts of the prime-characteristic proof follow basically the same lines as the characteristic-zero proof; however, certain elements of the proof, particularly where it is necessary to introduce field theory or number theory, can be made more concrete or intuitive by restricting to characteristic zero. Therefore, for the sake of clarity this exposition will present the proof over the complex numbers, although where clarity and brevity are not impaired by considering a step in the general case we will do so.

It will save some ink later to recall a customary definition:

Definition 0.1. *Let G be a group. Then G is said to be* ***virtually solvable*** *if it possesses a solvable subgroup of finite index.*

Thus the main theorem that we will prove may be stated as follows:

Theorem 1 (The Tits Alternative for Complex Linear Groups)**.** *Let G be a finitely-generated subgroup of $GL_n(\mathbb{C})$. Then either G is virtually solvable or G contains a non-abelian free subgroup.*

Remark 0.2. A group G containing a non-abelian free subgroup $F < G$ is not virtually solvable, so that this is a genuine alternative.

Indeed, suppose that such a G has a solvable subgroup $S < G$. Since non-abelian free groups are never solvable, and since subgroups of solvable groups are always solvable, a group with a free subgroup cannot be solvable, so certainly $S \neq G$. In fact, we can say more: observe that any two independent non-trivial elements of F generate a non-abelian free subgroup, so S does not contain any independent pair of elements of F. There must therefore exist some element $a \in F$ with the property that $a^n \notin S$ for all $n \in \mathbb{N}$.

Now note that for any distinct m, $n \in \mathbb{N}$, the fact that $a^{m-n} \notin S$ means that for any r, $s \in S$ we must have $a^m s \neq a^n r$, and so $a^m S \neq a^n S$ and S has infinite index. □

The strategy of the proof is essentially that found in [Tits], although the arguments will not necessarily be presented in the same order. The main reason for this is that it makes the motivation for each step somewhat clearer, although some of the ordering is forced upon us by the natural order in which the background theory is presented. Therefore, I claim no originality in the strategy of the proof, but hope that the reader will find some in its presentetion.

In the first two sections we will present some basics of algebraic-group theory, in particular highlighting certain properties of algebraic groups that were used heavily but implicitly by Tits. This will not be exciting, but it is very necessary for understanding the proof of Theorem 1. This will allow us to reduce the case in which G is not virtually solvable to the case in which the Zariski-closure of G is semisimple. In Section 3 we show that in that case G must possess elements of infinite order, and in Section 4 we examine the action of G on projective space and derive a sufficient condition for a pair of elements to generate a non-abelian free subgroup.

In Sections 5 and 6 we reduce the task to that of discovering a single diagonalisable element whose eigenvalues do not all share the same absolute value. The results of Section 6 concerning the existence of irreducible representations, or at least something similar, were certainly used by Tits, but I have not seen anything like them in the literature (probably because they are obvious if you are a representation theorist) and so their presence in the essay should make the proof easier to believe.

Then in Section 7, in one of the highlights of the proof, we show that we can change the field over which G is defined and thereby force the eigenvalues of a given element not to share the same absolute value. This entails a rather fun diversion into the world of p-adic numbers, which will allow us to use many of the strange and interesting properties exhibited by non-archimedian fields. In particular, we slightly weaken a theorem from a book of Weil that was cited by Tits, which enables us to cut out a big part of its proof without losing the key content that allowed Tits to apply it in the proof of his alternative. We also present more direct proofs of some of the preliminary results leading up to that theorem, in order to make it more self contained for this essay. Whilst this approach won't tell us anything that wasn't already known in terms of results, it should make it clearer exactly what is being used in that part of the proof and how.

All that leaves virtually no work to do, and Section 8 deals with the simple task of putting everything together and deducing the Tits Alternative.

A note on topologies. We will use different topologies at different times in this essay. I will try to remember to be explicit about which one is being used, but I am highly unlikely to be totally successful. Therefore, for the avoidance of doubt, in the event that a non-specific topology is used the reader may assume that the topology on $\mathbb{k}^n$ (where $\mathbb{k}$ is a field) comes from an absolute value on $\mathbb{k}$, and the topology on $GL_n(\mathbb{k})$ is the Zariski topology.

1 Reduction to Semisimple

In order to prove the Tits Alternative we will assume that a linear group G is not virtually solvable and deduce that it contains a non-abelian free group. The bulk of the proof, therefore, is concerned with finding this free group; this section is concerned with where we should look.

The natural thought would be to reduce to the most basic case by quotienting out any normal solvable subgroups. As we shall see, we are fortunate enough to be able to do this without sacrificing the linearity of the group. In fact, it is well known that if the group in question is a connected linear *algebraic* group then the quotient by its largest connected normal solvable subgroup is a *semisimple* algebraic group, and a great deal is known about the structure of such groups.

The aims of this section are therefore twofold. The first aim is to present some algebraic-group theory that will allow us then to understand the structure theory we have just alluded to. The second is to transform the problem from one of arbitrary linear groups to one of linear algebraic groups so that we may exploit this theory. The second aim we will achieve via the following lemma.

Lemma 1.1. *If G in Theorem 1 is not virtually solvable then we may assume its Zariski-closure to be a semisimple algebraic group.*

Rather than a lemma, in [Tits] this was simply an observation made right at the end of the proof of that paper's Theorem 1; however, the motivation for later results will be much clearer once Lemma 1.1 is established.[1]

The key references on the subject of algebraic groups are the books of Humphreys [Hump. 1], Springer [Spr.] and Borel [Borel]. They each have different strengths and weaknesses; it should be clear from the citations given below which has been most useful on each topic that we cover.

1.1 Some Algebraic Geometry

Before we begin exploring algebraic groups it will be necessary to recall some definitions from algebraic geometry. The reader familiar with that subject could quite easily skip this subsection, as its aim is simply to bring the rest of us up to speed. In this section $\Bbbk$ will denote an algebraically closed field of arbitrary characteristic.

Definition 1.1.1. ***Affine n-space*** *is the set $\Bbbk^n$, denoted $\mathbb{A}^n$.*

Definition 1.1.2. *We define the **Zariski topology** on $\mathbb{A}^n$ by declaring a set to be closed if and only if it is the set of common zeros of a collection of polynomials.*

It is straightforward to check that these closed sets satisfy the axioms for a topology, as in Section 1.2 of [Hump. 1].

The main objects of study in algebraic geometry are *varieties*, which can be thought of as subsets of affine space defined using polynomials. The actual definition of a variety is somewhat technical, and is described in full in Chapter 2 of [Hump. 1], but for the purposes of reading this essay it will be quite sufficient for the reader to think of a variety as follows.

[1] I believe a similar reduction is made early on in [Breu. 1].

Definition 1.1.3. *For the purposes of this essay we define an* ***affine variety*** *to be a* locally closed *(for the Zariski topology) subset of* $\mathbb{A}^n$*, where a* ***locally-closed*** *set is the intersection of an open set and a closed set. Locally-closed subsets of a variety are called* ***subvarieties****.*

If $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ are varieties then so is $X \times Y \subset \mathbb{A}^{m+n}$. Note that here $\mathbb{A}^{m+n}$ is given its own Zariski topology, and not the product topology.

An affine variety X is said to be *reducible* if it can be written as $X = X_1 \cup X_2$ with the X_i closed subvarieties and $X_i \neq X$, and *irreducible* otherwise. In formal topological terms:

Definition 1.1.4. *Let X be a topological space. Then X is said to be* ***irreducible*** *if it cannot be written as the union of two proper, nonempty, closed subsets.*

Often when authors work with a variety they speak of the *rational points* of that variety. We will not really make much use of this notion in this essay, but some familiarity with it serves to illuminate the notation used in many of the references, including the original paper of Tits, and so we include the following definition.

Definition 1.1.5. *Suppose $\Bbbk'$ is a subfield of $\Bbbk$, and that X is a variety defined over $\Bbbk$. The points in X whose coordinates lie in $\Bbbk'$ are called $\Bbbk'$-**rational points**, and the set of these points is denoted $X(\Bbbk')$.*

One of the most helpful aspects of the algebraic geometry behind what we define in the next subsection to be an algebraic group is the notion of the dimension of a variety X. We use the definition from [Hart.], as it is intuitively easy to grasp.

Definition 1.1.6. *The* ***dimension*** *of an affine variety is the supremum of all integers n such that there exists a chain $X_0 \subset X_1 \subset \cdots \subset X_n$ of distinct irreducible closed subsets of X.*

However, perhaps more important than the definition of dimension are its properties. Specifically, it is clear from the definition that we have the following.

Proposition 1.1.7. *Let X be an irreducible variety and let Y be a proper, closed, irreducible subset of X. Then* $\dim Y < \dim X$*.*

This, combined with the following result (Proposition 1.9 from [Hart.]), shows that the dimension of an affine variety as we have defined it is finite.

Proposition 1.1.8. *The dimension of $\mathbb{A}^n$ is n.*

We will frequently use these facts in order to consider legitimately the largest or smallest (closed) subgroup of an algebraic group with a certain property. Note that a different, but equivalent, definition of dimension is given in Chapter 3 of [Hump. 1]; Proposition 1.1.7 is proved for that definition in 3.2 of the same source.

We now have a reasonable handle on the objects of study in algebraic geometry, the varieties, but we have not yet discussed the maps between them. Those of greatest interest to us will be the *morphisms*, defined as follows.

Definition 1.1.9. *Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be affine algebraic varieties. Then a **morphism** $\varphi : X \to Y$ is a map of the form*

$$\varphi(x_1, \ldots, x_n) = (\psi_1(x), \ldots, \psi_m(x))$$

where the ψ_i are polynomials in the x_i.

Note that any morphism $\varphi : X \to Y$ is continuous for the Zariski topology, since if $Z \subset Y$ is closed, say Z is the set of zeros of a collection of polynomials $\{f_i : i \in I\}$ on Y, then $\varphi^{-1}(Z)$ is the set of zeros of the polynomials $\{f_i \circ \varphi : i \in I\}$ on X and hence also closed.

This completes the terminology that we will require. Additionally, we will often implicitly use the following technical proposition, the straightforward proof of which can be found under Proposition 1.3A of [Hump. 1].

Proposition 1.1.10. *Let X and X' be topological spaces. Then:*

(i) A subspace Y of X is irreducible (as a topological space) if and only if its closure $\overline{Y}$ is irreducible.

(ii) If $\varphi : X \to X'$ is a continuous map and X is irreducible then $\varphi(X)$ is also irreducible.

Note also that non-empty open subsets of an irreducible space are dense in that space, and hence that dense subsets of an irreducible space are connected.

1.2 Linear Algebraic Groups

Definition 1.2.1. *An **algebraic group** G is a variety with a group structure such that the maps*

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

and

$$\begin{array}{rccc} \iota & : & G & \to & G \\ & & x & \mapsto & x^{-1} \end{array}$$

are morphisms of varieties.

Definition 1.2.2. *A **morphism of algebraic groups** is a group homomorphism that is also a morphism of varieties.*

We can identify the set $M_n(\Bbbk)$ of $n \times n$ matrices with $\mathbb{A}^{n^2}$ in the obvious way, and write

$$GL_n(\Bbbk) = \{\, A \in M_n(\Bbbk) : \det A \neq 0 \,\}.$$

$GL_n(\Bbbk)$ may therefore be viewed as an open subset of $\mathbb{A}^{n^2}$ and hence as a variety. It is easy to see that the formulas for inversion and matrix multiplication make $GL_n(\Bbbk)$ into an algebraic group.

Definition 1.2.3. *A subgroup of $GL_n(\Bbbk)$ that is also a subvariety of $GL_n(\Bbbk)$ is called a **linear algebraic group**.*

Any closed subgroup of an algebraic group is clearly an algebraic group. Furthermore, the following results show that the closure of an arbitrary subgroup of a linear algebraic group is a subgroup with many of the same properties as the original.

Proposition 1.2.4. *Let $H < G < GL_n(\Bbbk)$ be linear groups, with H and G not necessarily closed, write $\overline{H}$ and $\overline{G}$ for their respective closures in $GL_n(\Bbbk)$, and write $\overline{H}_G$ for the closure of H in G. Then:*

(i) $\overline{H}_G$ is a subgroup of G;

(ii) If H is normal in G then so is $\overline{H}_G$;

(iii) H is soluble of derived length d if and only if $\overline{H}_G$ is;

(iv) The normaliser $N_{\overline{G}}(\overline{H})$ and centraliser $C_{\overline{G}}(\overline{H})$ of $\overline{H}$ in $\overline{G}$ are closed subgroups of $\overline{G}$;

(v) If H is normal in G then $\overline{H}$ is normal in $\overline{G}$.

Proof. (i) and (ii) are Lemma 5.9 from [Wehr.]. The reader should note that what Wehrfritz calls a *CZ-group* he defines on page 74, and that linear groups with the Zariski topology fit that definition. (iii) is Theorem 5.11 from the same source. (iv) is Corollary 8.2 from [Hump. 1].

I cannot find (v) in the literature, so we prove it here. Consider $g \in G$ as an element of $\overline{G}$. Normality of H in G implies that $H = g^{-1}Hg$, and hence $\overline{H} = \overline{gHg^{-1}} \subset g\overline{H}g^{-1}$, the last relation being due to the continuity of the map $k \mapsto g^{-1}kg$. Hence $g^{-1}\overline{H}g \subset \overline{H}$, where g was an arbitrary element of G, and so $G \subset N_{\overline{G}}(\overline{H})$. But (iv) shows that $N_{\overline{G}}(\overline{H})$ is closed, and so $\overline{G} \subset N_{\overline{G}}(\overline{H})$ and $\overline{H}$ is normal in $\overline{G}$. □

Another helpful result about closed subgroups of algebraic groups is the following result about commutators, which is Proposition 17.2 from [Hump. 1].

Lemma 1.2.5. *Let A and B be closed subgroups of an algebraic group G. Then:*

(i) If A is connected then (A, B) is closed and connected.

(ii) If A and B are normal in G then (A, B) is closed and normal in G.

In the introduction to this section we mentioned that a key reason for us to study algebraic groups was the structure theory of semisimple groups that we could exploit by considering particular quotient groups. We had therefore better note that it is legitimate to take quotients of algebraic groups by closed subgroups, and that the quotient is again a linear algebraic group.

Proposition 1.2.6. *Let G be a linear algebraic group over an algabraically-closed field and let H be a closed, normal subgroup. Then G/H is isomorphic to a linear algebraic group with the usual group structure and there is a surjective morphism of linear algebraic groups $\psi : G \to G/H$.*

This is Proposition 5.5.10 of [Spr.]. The ψ we mention here is not mentioned in the statement of the proposition in that book, but it is defined in the proof. A slight subtlety here is that the proof is over an algebraically-closed field $\Bbbk$,

and for a subfield $\Bbbk'$ of $\Bbbk$ it is not clear that $\psi(G(\Bbbk')) = (G/H)(\Bbbk')$.[2] However, in this essay we will take quotients only over algebraically closed fields, and so this will not cause us any worry. It turns out that if $\Bbbk'$ is *separably closed* then $\psi(G(\Bbbk')) = (G/H)(\Bbbk')$, as is commented after Theorem 6.8 in [Borel], but we will not make use of this.

1.3 Connected Components

The notion of irreducibility for an arbitrary variety carries over naturally to an algebraic group. The following observations make life more pleasant than it might otherwise be. The proofs are straightforward and transparently presented in Section 7.3 of [Hump. 1].

Lemma 1.3.1. *Let G be an algebraic group. Then only one irreducible component of G contains the identity e.*

This allows us to make the following definition.

Definition 1.3.2. *The unique (by Lemma 1.3.1) irreducible component of e in an algebraic group G is called the* ***identity component*** *and denoted by G°.*

Lemma 1.3.3. *Let G be an algebraic group. Then G° is a normal subgroup of finite index in G, the cosets of which are the connected and irreducible components of G. Each closed subgroup of finite index in G contains G°.*

It might seem natural to call an algebraic group G 'irreducible' if $G = G^\circ$. However, the term irreducible has a long-standing connection to representations of groups (and will indeed make an appearance in that context later in this essay), so in view of Lemma 1.3.3 we use the term *connected* instead.

Definition 1.3.4. *An algebraic group G is called* ***connected*** *if $G = G^\circ$.*

1.4 Semisimple Algebraic Groups

Lemma 1.4.1. *Let G be an algebraic group. Then G possesses a unique largest normal solvable subgroup, which is automatically closed.*

Proof. Let S be a closed, normal, solvable subgroup of maximal dimension. Since the closure of a normal solvable subgroup is normal and solvable (see Proposition 1.2.4), S is contained in no other normal solvable subgroup. Since the product of two normal subgroups is normal, S contains every other normal solvable subgroup. □

This allows us to make the following definition.

Definition 1.4.2. *The* ***radical*** *of an algebraic group G is the identity component of the largest normal solvable subgroup of G.*

The radical of G is then the the largest connected normal solvable subgroup of G, and is closed in G.

[2] Recall that $G(\Bbbk')$ denotes the $\Bbbk'$-rational points of G, that is to say the members of G all of whose matrix coefficients lie in $\Bbbk'$

Definition 1.4.3. *A **semisimple** algebraic group is a connected algebraic group with trivial radical.*

We have seen (Proposition 1.2.6) that we may consider the quotient of an algebraic group by any closed subgroup; in particular, the quotient of a connected algebraic group by its radical is clearly semisimple. With this in mind, we now recall and prove Lemma 1.1.

Lemma 1.1. *If G in Theorem 1 is not virtually solvable then we may assume its Zariski-closure to be a semisimple algebraic group.*

Proof. Write $\mathfrak{G}$ for the Zariski closure of G in $GL(V)$, and write G° for $G \cap \mathfrak{G}^\circ$. Since $\mathfrak{G}^\circ$ is of finite index in $\mathfrak{G}$, and hence G° is of finite index in G, the condition that G is not virtually solvable implies that $\mathfrak{G}^\circ$ is not solvable, and hence its radical is a proper subgroup. Writing $\mathfrak{R}$ for the radical of $\mathfrak{G}^\circ$, we therefore know that $\mathfrak{G}^\circ/\mathfrak{R}$ is non-trivial and semisimple.

Now suppose that we had proved Theorem 1 in the special case that G is not virtually solvable and has semisimple Zariski-closure. Since G° is a finite-index subgroup of a finitely-generated group it is finitely generated, and hence G°/R is finitely generated. The image of G°/R is dense in the semisimple algebraic group $\mathfrak{G}^\circ/\mathfrak{R}$, and so we could apply the special case of Theorem 1 to show that G°/R possesses a non-abelian free subgroup, and hence that G does. $\square$

2 Properties of Semisimple Groups

Now that the proof of Theorem 1 has been reduced to the study of a semisimple algebraic group it is worth noting some of the properties of such groups. One way or another, the properties that we will state here were used heavily by Tits in his proof of Theorem 1, although almost always implicitly and without statement. This is therefore a key section of this essay for a general audience hoping to understand the original paper of Tits.

These results are generally quite deep and not trivial to prove, and in fact the proofs will matter far less to us than the results themselves. Since this is meant to be an essay on the Tits Alternative and not a reference in algebraic-group theory, we will therefore state the results we need briefly and direct the reader to the literature for the proofs.

The key results we will need are as follows.

- Semisimple algebraic groups are perfect (see Definition 2.1.1 below)
- A semisimple linear algebraic group is therefore always a subgroup of a special linear group
- The set of semisimple elements of a semisimple algebraic group G contains a (Zariski-)dense open subset of G (see Definition 2.2.1 below)

2.1 Perfection of Semisimple Algebraic Groups

Definition 2.1.1. *A group G for which $G = (G, G)$ is said to be **perfect**.*

In order to show that semisimple groups are perfect we will need some structure theory. An important aspect of the structure theory of semisimple algebraic groups concerns their *simple* components, defined as follows.

Definition 2.1.2. *An algebraic group G is said to be **simple** if it is connected, it is non-abelian as a group and it has no non-trivial closed connected proper normal subgroups.*

Remarks 2.1.3.

(i) This is not equivalent to the definition of simple for an abstract group; some authors use the term ***almost simple*** to emphasise this difference. In fact, the quotient of a simple algebraic group by its centre is simple as an abstract group (29.5, [Hump. 1]).

(ii) Note that a simple algebraic group is automatically semisimple.

(iii) The non-abelian condition is necessary to prevent one-dimensional abelian groups from being simple.

The first thing to note is that any semisimple algebraic group has a simple subgroup; just take a minimal closed connected normal subgroup of positive dimension. In fact, much more than this is true. The following result, which, along with its corollary, is part of Theorem 27.5 from [Hump. 1], allows us to decompose G into the 'almost direct' product of its simple subgroups.

Proposition 2.1.4. *Let G be a semisimple algebraic group, and let $\{ G_i : i \in I \}$ be the simple subgroups of G. Then:*

(i) If $i \neq j$ then the commutator $(G_i, G_j) = e$

(ii) I is finite, say $I = \{1, \ldots, n\}$

(iii) For each i, the intersection $G_i \cap \prod_{j \neq i} G_j$ is finite

(iv) $G = \prod G_i$

(v) An arbitrary closed connected normal subgroup of G is the product of the G_i it contains

Corollary 2.1.5. *Let G be a semisimple algebraic group. Then G is perfect.*

Proof of Corollary. Proposition 2.1.4 (i) implies that $(G, G) = (G_1, G_1) \cdots (G_n, G_n)$. However, we have seen (Proposition 1.2.5) that the commutator of two closed, connected, normal subgroups of an algebraic group is also closed, connected and normal. Since G_i is not commutative, (G_i, G_i) is not trivial, and so the simplicity of G_i implies that $(G_i, G_i) = G_i$. This combined with Proposition 2.1.4 (iv) yields the desired result. □

Corollary 2.1.6. *Let $G < GL_n(\Bbbk)$ be a semisimple linear algebraic group. Then $G \subset SL_n(\Bbbk)$.*

Proof. Corollary 2.1.5 shows that G is generated by commutators. If $c = (k_1, k_2)$ is a commutator in $GL_n(\Bbbk)$ then

$$\begin{aligned} \det c &= (\det k_1)(\det k_2)(\det k_1)^{-1}(\det k_2)^{-1} \\ &= 1, \end{aligned}$$

and so G is generated by a subset of $SL_n(\Bbbk)$. □

Corollary 2.1.7. *A one-dimensional representation of a semisimple algebraic group is trivial.*

Note that Corollaries 2.1.6 and 2.1.7 apply to an arbitrary linear representation of any abstract perfect group, and not just to linear algebraic groups.

2.2 Semisimple Elements of Reductive Groups

Definition 2.2.1. *A linear endomorphism over a field $\Bbbk$ is called **semisimple** if it is diagonalisable over the algebraic closure of $\Bbbk$.*

Our desired result is the following.

Proposition 2.2.2. *Let G be a semisimple algebraic group. Then the set of semisimple elements of G contains a dense open subset of G.*

This will of course imply that a dense subgroup of an algebraic group contains semisimple elements, and so certainly a group whose closure is semisimple must contain such elements.

In fact, a semisimple group is a particular example of what is called a *reductive* group.

Definition 2.2.3. *A **unipotent** element of a linear algebraic group is one whose eigenvalues are all 1. An algebraic group is called **reductive** if it is connected and its radical*[3] *contains no non-identity unipotent elements.*

Our desired result is therefore immediately implied by the following proposition, the proof of which is described in 0.15 of [Hump. 3].

Proposition 2.2.4. *Let G be a reductive algebraic group. Then the set of semisimple elements of G contains a dense open subset of G.*

[3]Recall that the radical of G is the identity component of the largest normal solvable subgroup of G, and hence trivial if G is simple

3 Elements of Infinite Order

Now that the algebraic-group theory is out of the way, we can finally do some mathematics and make some progress towards the Tits Alternative. In view of Lemma 1.1, our task from here is to show that a finitely-generated Zariski-dense subgroup of a semisimple linear algebraic group contains a non-abelian free subgroup. If we are to have any hope of achieving this then we need, at the very least, such groups to contain elements of infinite order.

The aim of this section is to prove the following.

Proposition 3.1. *Let $G < GL_n(\mathbb{C})$ be a finitely-generated group of matrices acting irreducibly on $\mathbb{C}^n$, and let F be the set of all elements of finite order in G. Suppose F is Zariski-dense in G. Then G is finite.*

Definition 3.2. *A linear group $G < GL_n(\Bbbk)$ is said to act **irreducibly** on $\Bbbk^n$ if it leaves no proper subspace of $\Bbbk^n$ invariant.*

Since non-trivial connected linear algebraic groups are clearly infinite, Proposition 3.1 implies that a dense subgroup of a semisimple algebraic group must indeed contain an element of infinite order.

Proposition 3.1 is a special case of a more general proposition proved in Section 2 of [Tits], in which essentially the same conclusion is drawn about a subgroup of the multiplicative group of an arbitrary finite-dimensional simple algebra over an arbitrary field $\Bbbk$. We reproduce that proof here, but restrict to $\mathbb{C}$ in order to make concrete the small amount of field theory that appears in the proof, and restrict to $n \times n$ matrices because this is the only algebra for which the proposition will be used in this essay.

We begin with a straightforward lemma.

Lemma 3.3. *Let $G < GL_n(\mathbb{C})$ be a group of matrices acting irreducibly on $\mathbb{C}^n$, and denote by τ the trace map*

$$\begin{array}{rccc} \tau & : & G & \to & \mathbb{C} \\ & & g & \mapsto & \operatorname{tr} g. \end{array}$$

Then there exists a basis $\{e_1, \ldots, e_{n^2}\}$ for the vector space $M_n(\mathbb{C})$ of $n \times n$ complex matrices such that

$$G \subset \left\{ \sum_{i=1}^{n^2} t_i e_i : t_i \in \tau(G) \right\}.$$

Proof. We will make use of **Burnside's Theorem** (Corollary 3.4, XVII §3, [Lang]), which states that if $\Bbbk$ is algebraically closed and if $G < GL_n(\Bbbk)$ acts irreducibly on $\Bbbk^n$ then the elements of G span the vector space $M_n(\Bbbk)$. We may therefore choose a basis of $M_n(\mathbb{C})$ conisting of elements of G, say $g_1, \ldots, g_{n^2}$.

Now define a bilinear form $\beta : M_n(\mathbb{C}) \times M_n(\mathbb{C}) \to \mathbb{C}$ by $(x, y) \mapsto \tau(xy)$, which is clearly nondegenerate. Indeed, if $y \in M_n(\mathbb{C})$ is non-zero then there must exist some non-zero $v_1 \in \mathbb{C}^n$ such that $y(v_1) \neq 0$. Extend v_1 to a basis $\{v_1, \ldots, v_n\}$ for $\mathbb{C}^n$, and let $x \in M_n(\mathbb{C})$ be any matrix such that $x(y(v_1)) = v_1$, and $x(y(v_i)) = 0$ for all other i. Then $\beta(x, y) = 1$.

Hence we may define a basis $\{e_1, \ldots, e_{n^2}\}$ for $M_n(\mathbb{C})$ *dual* to $\{g_1, \ldots, g_{n^2}\}$ with respect to β, in the sense that $\beta(e_i, g_j) = \delta_{ij}$. But then, for any $g \in G$,

$$g = \sum_{i=1}^{n^2} \beta(g, g_i) e_i = \sum_{i=1}^{n^2} \tau(g g_i) e_i.$$

□

Thus if $\tau(G)$ is finite then so must G be. Our aim will be to show that this is the case if the set $F \subset G$ of all elements of finite order is dense in G. The key observation to allow us to do this is the following.

Lemma 3.4. *Let $G < GL_n(\mathbb{C})$ be a finitely-generated group of matrices and let F be the set of all elements of finite order in G. Then $\tau(F)$ is finite.*

Proof. Write E for the set of eigenvalues of elements of F. Then $\tau(F) \subset nE = \{ \lambda_1 + \cdots + \lambda_n : \lambda_i \in E \}$, so it is sufficient to prove that E is finite.

Let $\{g_1, \ldots, g_r\}$ be a generating set for G and let $\Bbbk$ be the field generated by the coefficients of the matrices representing $g_1, \ldots, g_r$, so that $\mathbb{Q} \subset \Bbbk \subset \mathbb{C}$. Every element of G is represented by a matrix with coefficients in $\Bbbk$, so the eigenvalues of all the matrices in G are therefore roots of polynomials of degree n over $\Bbbk$, namely the characteristic polynomials of the elements of G. In particular, the members of E are roots of unity that satisfy polynomials of degree n over $\Bbbk$.

Write R_n for the set of complex roots of unity that satisfy equations of degree n over $\Bbbk$. We have just shown that $E \subset R_n$, so it is sufficient to prove that R_n is finite. Let $\xi \in R_n$. Let T be a transcendence basis of $\Bbbk$ over $\mathbb{Q}$, and write $\overline{\mathbb{Q}}$ for the algebraic closure of $\mathbb{Q}$ in $\Bbbk(\xi)$. Then we have

$$\begin{aligned} [\mathbb{Q}(\xi) : \mathbb{Q}] &\leq [\overline{\mathbb{Q}} : \mathbb{Q}] \\ &= [\overline{\mathbb{Q}}(T) : \mathbb{Q}(T)] \\ &\leq [\Bbbk(\xi) : \mathbb{Q}(T)] \\ &\leq n[\Bbbk : \mathbb{Q}(T)]. \end{aligned}$$

But ξ was arbitrary, so R_n is contained in the set of complex roots of unity of degree at most $n[\Bbbk : \mathbb{Q}(T)]$, which is of course finite. □

Note that it was necessary to introduce the transcendence basis of $\Bbbk$ so as to ensure that the final bound was finite.

We now recall and prove Proposition 3.1.

Proposition 3.1. *Let $G < GL_n(\mathbb{C})$ be a finitely-generated group of matrices acting irreducibly on $\mathbb{C}^n$, and let F be the set of all elements of finite order in G. Suppose F is Zariski-dense in G. Then G is finite.*

Proof. Lemma 3.4 showed that for any finitely-genreated G the set $\tau(F)$ is finite, and hence Zariski-closed in $\mathbb{C}$. Since τ is a polynomial function it is continuous for the Zariski topology, and so $\tau^{-1}(\tau(F))$ is closed and contains F, and hence contains G by the density of F. Thus $\tau(G) = \tau(F)$; in particular, $\tau(G)$ is finite.

Now Lemma 3.3 shows that, since G acts irreducibly on $\mathbb{C}^n$, there exists a basis $\{e_1, \ldots, e_{n^2}\}$ for $M_n(\mathbb{C})$ such that

$$G \subset \left\{ \sum_{i=1}^{n^2} t_i e_i : t_i \in \tau(G) \right\}.$$

The right-hand side of this expressions is clearly finite, and hence so must G be, as required. $\square$

4 The Search for a Free Group

In this section we seek a pair of matrices that generate a non-abelian free group, following the construction used in Section 3 of [Tits]. To say that two group elements generate a free group is to say that no non-trivial word in the elements is equal to the group identity, so we will show that the matrices we put forward have this property.

4.1 The Basic Strategy

Suppose g and h are two elements of a group G. A non-trivial word in them is of the form

$$W_{g,h} = g^{m_0}h^{n_0}\dots g^{m_k}h^{n_k},$$

with the m_i and n_i all non-zero integers, with the exception that one or both of m_0 and n_k may be zero as long as at the expression has at least one non-zero exponent. Now let G act on some set X. In order to show that a non-trivial word $W_{g,h}$ is not equal to the group identity it is sufficient to show that there is some $x \in X$ that is not fixed by $W_{g,h}$. Demonstrating this for an arbitrary word $W_{g,h}$ would therefore prove that g and h generated a free subgroup of G.

If G acts on a metric space (X, d) then there is a particularly useful strategy open to us, which we sketch here and make precise later, in Subsection 4.6. Given $g \in G$ we seek points a_g and r_g in X (where a stands for 'attracting' and r stands for 'repulsing') with the following property under the G-action on X:

(i) $\forall x \in X\backslash\{r_g\}$ $\quad g^n(x) \to a_g$ as $n \to \infty$

(ii) $\forall x \in X\backslash\{a_g\}$ $\quad g^{-n}(x) \to r_g$ as $n \to \infty$,

where the convergence is locally uniform in x. As it turns out, this is not exactly the definition that we will use, but it illustrates the concept.

The above conditions mean that, for any x other than a_g and r_g, repeated application of g will move x 'away from' r_g and 'towards' a_g. Now suppose that h has corresponding points a_h and r_h that are 'far' from a_g and r_g, and pick some $x \in X$ that is 'far' from all four of a_g, r_g, a_h and r_h. Applying a sufficiently high positive power of g to x will move x to a point $g^n(x)$ that is 'close' to a_g, which by assumption is 'far' from a_h and r_h. Applying a sufficiently high positive power of h will then send $g^n(x)$ 'close' to a_h, whilst applying a sufficiently high negative power of h will send $g^n(x)$ 'close' to r_h.

Repeated applications of high positive or negative powers of either element will similarly just move x between 'small' neighbourhoods of their respective attracting and repulsing points. But we chose x to be 'far' from all four of those points, so given that under a non-trivial word in sufficiently high powers of g and h the image of x is 'close' to one of them, that word certainly does not leave x fixed. Thus such a word cannot be equal to the identity, and so for sufficiently high $m \in \mathbb{N}$ we have that g^m and h^m generate a free group.

The rest of Section 4 will seek to formalise this strategy and to apply it to matrix groups acting on projective space and thereby present a sufficient condition for a pair of matrices to generate a free group.

4.2 Absolute Values and Locally-Compact Fields

The process we have just described for discovering a free group uses the action of the group on a metric space. Since we are interested in matrix groups, which have natural actions on vector spaces and projective spaces, we should say a brief word about metrics on such spaces.

The metrics we all know and love on $\mathbb{R}^n$ and $\mathbb{C}^n$ come from the absloute value on $\mathbb{C}$. We will need the theory we develop here for fields other than $\mathbb{R}$ or $\mathbb{C}$, so before we consider metrics on P it will help to record a generalised definition of an absolute value on a field $\Bbbk$.

Definition 4.2.1. *Let $\Bbbk$ be a field. An **absolute value** on $\Bbbk$ is a function*

$$|\cdot| : \Bbbk \to \mathbb{R}_+$$

that satisfies the following conditions:

(i) $|x| = 0$ *if and only if* $x = 0$

(ii) $|xy| = |x||y|$ *for all* $x, y \in \Bbbk$

(iii) $|x + y| \leq |x| + |y|$ *for all* $x, y \in \Bbbk$

It is easy to see that setting $d(x, y) = |x - y|$ defines a metric on $\Bbbk$, which allows us to make a further definition:

Definition 4.2.2. *A field $\Bbbk$ with an absolute value $|\cdot|$ is said to be **locally compact** if it is so as a metric space, that is to say if every point $x \in K$ has a compact neighbourhood.*

In this section we will assume that $\Bbbk$ is a field of characteristic zero with an absolute value $|\cdot|$ that makes $\Bbbk$ locally compact. The properties in Definition 4.2.1 are all familiar properties of the ordinary absolute value on $\mathbb{R}$ or $\mathbb{C}$, and it is easy to see that these fields are both locally compact; for much of this section it will do the reader no harm (and may positively help his intuition) to imagine that $\Bbbk = \mathbb{R}$ and that $|\cdot|$ is the usual absolute value on $\mathbb{R}$.

4.3 Distance Functions on $\Bbbk$-spaces

Let $\Bbbk$ be a locally-compact field with an absolute value $|\cdot|$, and let V be an $(n + 1)$-dimensional vector space over $\Bbbk$. Recall the following definitions:

Definition 4.3.1. *The **projective space** $P(V)$ of V is defined by*

$$P(V) = (V \backslash \{0\}) / \sim \quad \text{where} \quad x \sim y \iff \exists \lambda \in \Bbbk : x = \lambda y$$

Thus $P(V)$ can be thought of as the set of one-dimensional subspaces of V. Henceforth, denote $P(V)$ by P.

Definition 4.3.2. *The **projective general linear group** of P is defined as*

$$PGL(P) = \frac{GL(V)}{\Bbbk . Id_V}$$

where Id_V denotes the identity transformation in $GL(V)$.

Note that $PGL(P)$ acts faithfully on P.

The spaces V and P both carry natural topologies induced by that of $\Bbbk$: the topology of V is the product topology when V is identified with $\Bbbk^{n+1}$, and the topology of P is the quotient topology under $\sim$ from Definition 4.3.1. It is well known and straightforward to check that this topology is independent of the choice of basis on V. It is also easy to see that both V and P inherit from $\Bbbk$ the property of being locally compact.

We will now give an outline of how we may define a metric on P that behaves in a way that is helpful. This is discussed fairly clearly at the beginning of Section 3 in [Tits], so our main aim here will be to try to fill in gaps where Tits was not explicit.

Let $E = \{e_0, \ldots, e_n\}$ be a basis for V, and for $v \in V$ write v_i for the i-th co-ordinate of v with respect to E. For this co-ordinate system we may define a metric on V by $d(v, w) = \max_j |v_j - w_j|$.

Now let H_i be the hyperplane defined by $\{v_i = 0\}$. For $p \in P\backslash H_i$, with $\overline{p}$, say, a representative of p in V, setting $p_j = \overline{p}_j/\overline{p}_i$ defines a natural (and obviously well-defined) n-dimensional affine co-ordinate system given on $P\backslash H_i$. For this co-ordinate system we may define a metric on $P\backslash H_i$ by $d_i(p, q) = \max_j |p_j - q_j|$. Of course, given any hyperplane H we may fix a basis of V with respect to which $H = H_i$ for some i, and hence define similarly a metric on $P\backslash H$.

The following, which is proved straightforwardly as Lemma 3.2 from [Tits], shows that there is an equivalence between any two metrics defined in this way on some compact subset of P.

Lemma 4.3.3. *Suppose H and H' are two hyperplanes, and that d and d' are distance functions coming from affine co-ordinate systems on $P\backslash H$ and $P\backslash H'$, respectively, in the way described above. If K is some compact subset of $P\backslash(H \cup H')$ then there exist $m, M \in \mathbb{R}_+\backslash\{0\}$ such that*

$$m.d|_{K\times K} \leq d'|_{K\times K} \leq M.d|_{K\times K}.$$

Ideally, the metric we use on P should also be equivalent in this sense to any metric on a compact subset coming from an affine co-ordinate system. It is with this in mind that we make the following definition, which is identical to that used in Section 3.3 of [Tits].

Definition 4.3.4. *A distance $d : P \times P \to \mathbb{R}_+$ is said to be **admissable** if it defines a metric compatible with the topology of P and if, for any compact set $K \subset P$ on which there is a metric d' coming from an affine co-ordinate system on some $P\backslash H$, there exist $m, M \in \mathbb{R}_+\backslash\{0\}$ such that*

$$m.d|_{K\times K} \leq d'|_{K\times K} \leq M.d|_{K\times K}. \qquad (\dagger)$$

In the case that $\Bbbk = \mathbb{R}$ or $\mathbb{C}$ we can consider the metric defined by considering the Euclidean norm on V and defining the distance (in P) between two 1-dimensional subspaces W_1 and W_2 of V to be the minimal distance in V between a point of norm 1 on W_1 and a point of norm 1 on W_2.

In the case that $\Bbbk$ is some other field it is not necessarily obvious that we may define an admissable distance. In fact, as we shall see in detail in Section 7, the other locally-compact fields over characteristic zero that we will ultimately need to consider have what is called the *non-archimedian property*, which means

that they satisfy a stronger version of the triangle inequality. Specifically, if $\Bbbk$ is non-archimedian then for $x, y \in \Bbbk$ we have $|x + y| \leq \max\{|x|, |y|\}$. This is clearly preserved by the metric $d(v, w) = \max_j |v_j - w_j|$ that we defined above, and so this metric on V also has the non-archimedian property.

We would therefore like to show that if $\Bbbk$ is non-archimedian then there exist admissable distances on P. We will need the following lemma, which exhibits a strange property of non-archimedian spaces.

Lemma 4.3.5. *If $\Bbbk$ is non-archimedian then we may cover P with finitely many disjoint open compact subsets K_j, each of which is contained in the complement of some hyperplane H_j.*

Proof. Let $\mathcal{B}$ be the set of all open balls $B(v, r)$ in V for which there exist hyperplanes $H_{v,r}$ such that $B(v, r) \subset P \backslash H_{v,r}$.[4] Since $\Bbbk.B(v, r)\backslash\{0\}$ is also open, the images $U_{v,r}$ of these balls in P form an open cover of P. Since P is compact, there is a finite subcover, say $\{ U_j : j = 1, \ldots, N \}$.

It is a fun exercise to show that in a non-archimedian metric space, such as V, the open balls are also closed, and so the U_j are both open and closed in P. The sets $K_j := U_j \backslash \bigcup_{i<j} U_i$ are therefore disjoint, open, compact and each contained in the complement of some hyperplane H_j. □

Lemma 4.3.6. *Let $\{ K_j : j = 1, \ldots, N \}$ be as in Lemma 4.3.5 and for each j let d_j be a metric on K_j coming from an affine co-ordinate system on $P\backslash H_j$. Set $\Delta = \sup(\bigcup_j d_j(K_j \times K_j))$ and define a distance function on the whole of P by*

$$d(p, q) = \begin{cases} d_j(p, q) & \text{if } p, q \in K_j \\ \Delta & \text{if } p \in K_j, p \in K_{j'}, j \neq j' \end{cases}$$

Then d is admissable.

Proof. It is clear that d preserves the topology on P, so it remains to show that (†) holds. Let K be compact and endowed with a metric d' coming from some affine co-ordinate system. By Lemma 4.3.3, (†) holds if $K \subset K_j$ for some j, so assume $K \cap K_j \neq \varnothing$ and $K \cap K_{j'} \neq \varnothing$.

By definition $d(K_j \times K_{j'}) = \{\Delta\}$, and by compactness d' is bounded above on K, so it is sufficient to prove that $\inf d'(K_j \times K_{j'}) > 0$. But if this were not the case then there would exist $p_n \in K_j$ and $q_n \in K_{j'}$ such that $d'(p_n, q_n) \to 0$. By compactness we could restrict to a convergent subsequence and assume that $p_n \to p$, and hence also that $q_n \to p$, but this would contradict the fact that the K_j are closed and disjoint. □

4.4 Norms of Maps

Definition 4.4.1. *Let K be a subset of P and let d be a metric on K. Then for any map $\alpha : K \to P$ we define the **norm** of α on K with respect to d by*

$$\|\alpha\|_d = \sup_{p,q \in K : p \neq q} \frac{d(\alpha(p), \alpha(q))}{d(p, q)}.$$

[4] We could of course pick just one ball centred on each v, but considering the set of all possible balls neatly makes it clear that we do not need the axiom of choice.

Despite the terminology, we do not care whether this is a norm in the usual sense of the word. The only properties that we will need are noted in the following lemma.

Lemma 4.4.2. *Let d be an admissable distance on P and let $g, h \in PGL(P)$. Then*

(i) $\|gh\|_d \leq \|g\|_d.\|h\|_d$

(ii) $\|g\|_d < \infty$

Proof. (i) is obvious for any maps $P \to P$. To prove (ii), let H be a hyperplane of P and consider a distance d_H coming from an affine co-ordinate system on $P\backslash H$. A representative $\overline{g}^{-1}$ in $GL(V)$ of g^{-1} maps any basis of $V\backslash\overline{g}H$ to a basis of $V\backslash H$, and so the function d' on $P\backslash H$ given by $d'(p,q) = d(gp, gq)$ is a metric coming from an affine co-ordinate system. Hence Lemma 4.3.3 implies that there exists $M \in \mathbb{R}_+\backslash\{0\}$ such that $d(gp, gq) \leq M.d(p,q)$ on $P\backslash H$. We may cover P with finitely many such complements of hyperplanes, and so (ii) is proved. □

4.5 Attracting Points in Projective Space

We now proceed to apply our earlier discussion of attracting and repulsing points to elements of $PGL(P)$. In light of Subsections 4.3 and 4.4 we may let d be an admissable distance on P and write $\|\cdot\|$ for the norm on P with respect to d.

Definition 4.5.1. *Let $g \in PLG(P)$, and let $\overline{g}$ be a representative of g in $GL(V)$. Let $\{\lambda_i : i = 0, \ldots, n\}$ be the eigenvalues of $\overline{g}$, repeated according to multiplicity, and write $|\lambda| = \max_i |\lambda_i|$.*

*Define the **attracting subspace** A_g of g in V by*

$$A_g = \ker \prod_{i:|\lambda_i|=|\lambda|} (\overline{g} - \lambda_i).$$

*Define the **complementary subspace** A'_g of the attracting subspace by*

$$A'_g = \ker \prod_{i:|\lambda_i|<|\lambda|} (\overline{g} - \lambda_i).$$

*Define the **attracting subspace** a_g of g in P to be the image in P of A_g, and the **complementary subspace** a'_g of the attracting subspace in P to be the image in P of A'_g.*

*If a_g is a point then call it the **attracting point** of g.*

Write

$$R_g := A_{g^{-1}}$$

$$R'_g := A'_{g^{-1}}$$

$$r_g := a_{g^{-1}}$$

$$r'_g := a'_{g^{-1}}$$

*If r_g is a point then call it the **repulsing point** of g.*

Note that these subspaces are all well defined, in that they do not depend upon the choice of $\overline{g}$. Some authors (cf [Breu. 2]) use the term *proximal elements* for elements of a linear group that possess attracting points.

The following lemma illustrates the choice of terminology (and shows that these definitions are similar to the sketch descriptions of attracting and repulsing points we gave in Subsection 4.1).

Lemma 4.5.2. *Let $g \in PGL(P)$ be diagonalisable with an attracting point a_g and let $K \subset P$ be compact with $K \cap a'_g = \varnothing$.*

Then $\|g^m|_K\| \to 0$ as $m \to \infty$, and for every neighbourhood U of a_g there exists $M \in \mathbb{N}$ such that $g^m(K) \subset U$ for all $m \geq M$.

Proof. Note that we may view $P \backslash a'_g$ as an n-dimensional linear vector space P_g over $\Bbbk$, with zero point a_g and on which g acts linearly. To see this, consider a basis for V consisting of eigenvectors of g, say $\{v_0, v_1, \ldots, v_n\}$ where v_0 is the eigenvector corresponding to a_g.

Working with respect to this basis, we have

$$P \backslash a'_g = \{\, [(1, x_1, \ldots, x_n)] : x_1, \ldots, x_n \in \Bbbk \,\}.$$

This allows us to define vector addition and scalar multiplication for P_g as follows:

$$[(1, x_1, \ldots, x_n)] + [(1, y_1, \ldots, y_n)] = [(1, x_1 + y_1, \ldots, x_n + y_n)] \quad \text{for all } x_i, y_i \in \Bbbk$$

$$\mu[(1, x_1, \ldots, x_n)] = [(1, \mu x_1, \ldots, \mu x_n)] \quad \text{for all } \mu \in \Bbbk.$$

It is clear that these operations make P_g a vector space with a canonical basis induced by that of V, and whose natural topology agrees with that of $P \backslash a'_g$.

Now let $\overline{g}$ be the representative of g whose eigenvalue corresponding to v_0 (and hence with strictly greatest absolute value) is 1, so that

$$\overline{g} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \lambda_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \lambda_n \end{pmatrix}$$

with $|\lambda_1|, \ldots, |\lambda_n| < 1$.

Write $\widehat{g}$ for the map on P_g induced by g, and note that we can express $\widehat{g}$ as the following matrix with respect to the induced basis for P_g:

$$\widehat{g} = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}.$$

Hence $\widehat{g}$ is a diagonal linear endomorphism of P_g with eigenvalues all of absolute value strictly less than 1. Therefore, writing d' for the metric on P_g defined by this co-ordinate system, we have that $\|\widehat{g}^m\| \to 0$ as $m \to \infty$ and so, by the equivalence of distances as discussed in Lemma 4.3.3, $\|g^m|_K\| \to 0$. Furthermore, for any compact set $K \subset P_g$ and any neighbourhood U of 0, there exists $M \in \mathbb{N}$ such that $\widehat{g}^m(K) \subset U$ for all $m \geq M$. Viewing K and U as subsets of P, with U now a neighbourhood of a_g, we have that $g^m(K) \subset U$ for all $m \geq M$ and so the lemma is proved. $\square$

4.6 A Condition for Freedom

Proposition 4.6.1 (A Condition for Freedom)**.** *Let $\mathbb{k}$ be a locally compact field, V an $(n+1)$-dimensional vector space over $\mathbb{k}$ and $P = P(V)$ the projective space of V.*

Let g and h be diagonalisable elements of $PGL(P)$, with attracting points a_g and a_h and repulsing points r_g and r_h such that

$$a_g, r_g \in P\backslash(a'_h \cup r'_h) \qquad \text{and} \qquad a_h, r_h \in P\backslash(a'_g \cup r'_g).$$

Then there exists $M \in \mathbb{N}$ such that, for all $m \geq M$, the elements g^m and h^m generate a non-abelian free group.

Proof. Fix $x \in P\backslash(\{a_g, r_g, a_h, r_h\} \cup a'_g \cup r'_g \cup a'_h \cup r'_h)$. Pick subsets $\mathcal{A}_g$, $\mathcal{R}_g$, $\mathcal{A}_h$, $\mathcal{R}_h \subset P\backslash\{x\}$ such that

(i) $\mathcal{A}_g$ is a compact neighbourhood of a_g and $\mathcal{R}_g$ is a compact neighbourhood of r_g;

(ii) $\mathcal{A}_g \cup \mathcal{R}_g \subset P\backslash(a'_h \cup r'_h)$;

(iii) both (i) and (ii) also hold with g and h interchanged,

noting that it is clear that such subsets exist.

Note that $\mathcal{A}_h \cup \mathcal{R}_h \cup \{x\}$ is compact, and so applying Lemma 4.5.2 to g with $\mathcal{A}_g$ playing the role of U, a neighbourhood of a_g, we obtain $M \in \mathbb{N}$ such that $g^m(\mathcal{A}_h \cup \mathcal{R}_h \cup \{x\}) \subset \mathcal{A}_g$. We may similarly apply Lemma 4.5.2 to g^{-1} with $\mathcal{R}_g$, to h with $\mathcal{A}_h$ or to h^{-1} with $\mathcal{R}_h$ to obtain that there exists $M \in \mathbb{N}$ such that, for all $m \geq M$:

- $g^m(\mathcal{A}_h \cup \mathcal{R}_h \cup \{x\}) \subset \mathcal{A}_g$
- $g^{-m}(\mathcal{A}_h \cup \mathcal{R}_h \cup \{x\}) \subset \mathcal{R}_g$
- $h^m(\mathcal{A}_g \cup \mathcal{R}_g \cup \{x\}) \subset \mathcal{A}_h$
- $h^{-m}(\mathcal{A}_g \cup \mathcal{R}_g \cup \{x\}) \subset \mathcal{R}_h$

Hence for all $m \geq M$, by induction on word length, an arbitrary non-trivial word w in g^m and h^m has $w(x) \in \mathcal{A}_g \cup \mathcal{R}_g \cup \mathcal{A}_h \cup \mathcal{R}_h$. Hence $w(x) \neq x$, and so w is not the identity in $PGL(P)$. Therefore g and h generate a non-abelian free group, as claimed. □

4.7 Meeting the Condition

Proposition 4.6.1 gave us a sufficient condition for a pair of matrices to generate a free group. In this subsection we make the key observation that, provided G acts irreducibly on $\mathbb{k}^n$, if a linear group G possesses a single diagonalisable element g with an attracting point and a repulsing point then we can construct a second element g' so that g and g' as a pair satisfy that condition for freedom and hence can be used to construct a non-abelian free subgroup of G. Our search for a free group in G thus reduces, in the case that G acts irreducibly, to the search for a diagonalisable element with an attracting point and a repulsing point.

Lemma 4.1. *Let $G < GL_n(\Bbbk)$ be a linear group over a locally-compact field $\Bbbk$ such that the Zariski-closure of G is Zariski-connected (and hence irreducible as a variety) in $GL_n(\Bbbk)$ and the action of G leaves no subspace of $\Bbbk^n$ invariant. Suppose G possesses a diagonalisable element g with an attracting point and a repulsing point. Then there exist $g' \in G$ and $m \in \mathbb{N}$ such that g^m and $(g')^m$ generate a non-abelian free group.*

Proof. Let $x_1, \ldots, x_n$ be a basis for $\Bbbk^n$ consisting of eigenvectors of g, with corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$, and let $x_1^*, \ldots, x_n^*$ be the basis dual to this in $(\Bbbk^n)^*$. Define linear forms $\varphi_{ij} : GL_n(\Bbbk) \to \Bbbk$ by

$$\varphi_{ij} : h \mapsto x_i^*(hx_j)$$

for each i, j. Note that for each i we have $(\dim \ker x_i^*) = (n-1)$, and so $\ker x_i^*$ is a proper subspace of $\Bbbk^n$. The irreducibility of the G-action on $\Bbbk^n$ therefore implies that for any given i, j there exists $h = h(i,j) \in G$ such that $hx_j \notin \ker x_i^*$. Hence the maps φ_{ij} are not identically zero on G. Furthermore, the φ_{ij} are also morphisms $GL_n(\Bbbk) \to \mathbb{A}^1$, so the sets on which the φ_{ij} take non-zero values are Zariski-open in $GL_n(\Bbbk)$ by continuity. Therefore, since the closure of G is irreducible as a variety and a pair of non-empty open subsets of an irreducible variety always meet, the set

$$U = \{\, h \in GL_n(\Bbbk) : \varphi_{ij}(h) \neq 0 \,\forall i, j \,\}$$

is non-empty and open in the closure of G, and so there exists $h \in G \cap U$.

Fix such an h, and observe that

$$\begin{aligned} hgh^{-1}(hx_j) &= hgx_j \\ &= \lambda_j hx_j \end{aligned}$$

for each j, so that $hx_1, \ldots, hx_n$ are eigenvectors of hgh^{-1}, with corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$. Hence hgh^{-1} is a diagonalisable element of G with an attracting point and a repulsing point.

But h was chosen so that $x_i^*(hx_j) \neq 0$ for each i, j, and hence no hx_1 is contained in the span of any $(n-1)$ of the x_i, and vice versa. In particular, the respective attracting and repulsing points of g and hgh^{-1} do not belong to each other's complementary subspaces and the hypotheses of Proposition 4.6.1 are satisfied. Hence there exists $m \in \mathbb{N}$ such that g^m and $hg^m h^{-1}$ generate a non-abelian free subgroup. □

5 Constructing Proximal Elements

We have seen in Section 4 that, provided a linear group G is Zariski-connected and acts irreducibly, if we construct a semisimple element of G with an attracting point and a repulsing point then we can produce a pair of elements generating a non-abelian free subgroup of G. In this section we will construct that element.

The ultimate aim of the section is to prove the following, which is Proposition 3.11 from [Tits].

Lemma 5.1. *Let $\mathbb{k}$ be a locally-compact field, and let G be a Zariski-connected subgroup of $GL_n(\mathbb{k})$ acting irreducibly on $\mathbb{k}^n$. Suppose that G possesses a diagonalisable element g with a repulsing point r_g. Then the set*

$$X = \{\, x \in G : a_x \text{ and } r_x \text{ are points} \,\}$$

is Zariski-dense in G.

We already know from Section 2.2 that any dense subset of a semisimple group must contain a semisimple element, so in the case that the closure of G is semisimple we will be able to deduce that the set X from Lemma 5.1 contains a diagonalisable element. Our task is therefore reduced from that of finding a semisimple element with both an attracting point *and* a repulsing point to that of finding a diagonalisable element with either an attracting point *or* a repulsing point.

As for much of the last section, let $V = \mathbb{k}^{n+1}$ and let $P = P(V)$. We will assume that $\mathbb{k}$ is of characteristic zero so as to avoid some technicalities, but everything would generalise easily. Indeed, the proof of the Converse Lemma (5.1.1) as we give it here would be slightly easier in positive characteristic.

5.1 The Converse Lemma

In this subsection we give a partial converse to Lemma 4.5.2, which will provide a sufficient condition for an element of $GL_n(\mathbb{k})$ to have an attracting point. This lemma is part (ii) of Lemma 3.8 in [Tits].

Lemma 5.1.1 (The Converse Lemma)**.** *Let $g \in PGL(P)$ and let $K \subset P$ be compact. Write K° for the interior of K, and suppose that there exists $m \in \mathbb{N}$ such that $\|g^m|_K\| < 1$ and $g^m K \subset K^\circ$. Then a_g is a point contained in K°.*

Proof. Replace g by g^m so that we may assume $m = 1$. Note that, for $r \in \mathbb{N}$, we have $g^{r+1}K \subset g^r K$, and also that $\operatorname{diam} g^r K \leq \|g|_K\| \operatorname{diam} K$, and so $\bigcap_{r\in\mathbb{N}} g^r K = \{p\}$ for some $p \in K^\circ$. Observe that $gp = p$, and so p corresponds to an eigenvector $\widehat{p}$ in V for a representative $\overline{g}$ of g in $GL(V)$. Scale $\overline{g}$ so that its eigenvalue on $\widehat{p}$ is 1.

We first claim that the multiplicity of 1 as an eigenvalue of $\overline{g}$ is 1. Indeed, suppose this is not the case; then there exists a two-dimensional subspace V' of V that is invariant under $\overline{g}$ and such that $\overline{g}|_{V'}$ has eigenvalues all equal to 1. Now $\overline{g}|_{V'}$ cannot be the identity, since then $\|g|_K\| \geq 1$, so we may assume $\overline{g}|_{V'}$ is of the form

$$\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix},$$

with respect to a basis for which $\widehat{p}$ corrseponds to the vector $(1,0)$. Hence

$$\overline{g}^r|_{V'} = \begin{pmatrix} 1 & r\mu \\ 0 & 1 \end{pmatrix}.$$

[*This would already be a contradiction in characteristic p: consider the case* $r = p$.] Openness of K° implies that, for sufficiently large (in absolute value) $r \in \mathbb{N}$, the point in P corrseponding to

$$\begin{pmatrix} 1 \\ -\mu^{-1}r^{-1} \end{pmatrix}$$

is in K, and hence the vector corresponding to

$$\begin{pmatrix} 1 & r\mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ -\mu^{-1}r^{-1} \end{pmatrix} = \begin{pmatrix} 0 \\ -\mu^{-1}r^{-1} \end{pmatrix} \sim \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

is in $g^r(K)$. Hence, writing $\widehat{p}'$ for the vector $(0,1)$ in V', and p' for the point in P corresponding to $\widehat{p}'$, both p and p' belong to $g^r(K)$ for sufficiently large r (in absolute value), contradicting the fact that $\operatorname{diam} g^r K \to 0$ as $r \to \infty$.

Thus the egienvalue 1 has multiplicity 1 in $\overline{g}$. Now let λ be another eigenvalue of $\overline{g}$, with corresponding eigenvector $\widehat{q}$, and restrict to the subspace W of V with basis $\widehat{p}$ and $\widehat{q}$. Again, for sufficiently small ε, the point corresponding to $(1,\varepsilon)$ in W belongs to K.

But

$$\overline{g}^r \begin{pmatrix} 1 \\ \varepsilon \end{pmatrix} = \begin{pmatrix} 1 \\ \lambda^r\varepsilon \end{pmatrix},$$

and so $\lambda^r\varepsilon \to 0$ as $r \to \infty$ by the fact that $\bigcap_{r\in\mathbb{N}} g^r K = \{p\}$. Hence $|\lambda| < 1$.

Since λ was arbitrary, this shows that 1 is a multiplicity-1 eigenvalue of $\overline{g}$ of strictly greater absolute value than all the other eigenvalues, and hence that p is an attracting point of g. □

5.2 A Bound on Norms of Powers

The Converse Lemma (5.1.1) gave us a two-part sufficient condition for an element $g \in PGL(P)$ to have an attracting point. The first part of this condition was that some power of g should have norm less than 1 on some compact subset $K \subset P$. In this subsection we will show that, provided K is chosen sensibly, we can at least guarantee that the norms of powers of g are bounded.

Lemma 5.2.1. *Let $g \in PGL(P)$ be diagonalisable and let K be a compact subset of $P\backslash a'_g$. Then the set $\{\, \|g^m|_K\| : m \in \mathbb{N} \,\}$ is bounded.*

Proof. Let $\overline{g} \in GL(V)$ be a representative of g. Let $E = \{e_0, \ldots, e_n\}$ be a basis of eigenvectors numbered such that A_g is spanned by $e_0, \ldots, e_r$ and A'_g is spanned by $e_{r+1}, \ldots, e_n$. Write $\lambda_0, \ldots, \lambda n$ for the corresponding eigenvalues.

If the conclusion of the lemma is false then there exist $m_i \in \mathbb{N}$ and $p_i, q_i \in K$ such that

$$\frac{d(g^{m_i}p_i, g^{m_i}q_i)}{d(p_i, q_i)} \to \infty \qquad (\dagger)$$

as $i \to \infty$. By compactness of K we may replace (p_i) with a subsequence and hence assume that $p_i \to p$, some $p \in K$. Since d is bounded on P, in order for $(\dagger)$ to hold we must also have that $q_i \to p$.

Let v be a point in V corresponding to p, and write v_i for the i-th co-ordinate of v when expressed with respect to the basis E. Since $p \in K \subset P\backslash A'_g$, it must be the case that $v_i \neq 0$ for some $i \leq r$. Without loss of generality we may assume that $v_0 = 0$ and scale $\overline{g}$ so that $\lambda_0 = 1$.

Now let $\widehat{H}$ be the subspace of V spanned by $e_1, \ldots, e_n$, and let H be the corresponding subspace of P. By considering only sufficiently large $i \in \mathbb{N}$ we may assume that each p_i and each q_i lies in $P\backslash H$. Just as we did in the proof of Lemma 4.5.2, we may view $P\backslash H$ as a vector space with the point corresponding to e_0 as its zero point.

As before, $P\backslash H$ is invariant under g, and the action of g on $P\backslash H$ is of the form

$$\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}$$

with respect to the natural basis. This and any power of it clearly has norm at most 1 on $P\backslash H$ with respect to this co-ordinate system, and so by the equivalence of distances discussed earlier this contradicts (†). Hence the conclusion of the lemma is true. □

5.3 Keeping Control of K

The second part of the condition from the Converse Lemma (5.1.1) for an element $g \in PGL(P)$ to have an attracting point demanded that some power of g should map some compact subset $K \subset P$ to its own interior. In this subesction we will prove a lemma that will provide at least some control over the image of certain K for infinitely many powers of g. Before we can do so, we will need a simple technical lemma.

Lemma 5.3.1. *Let $\xi_1, \ldots, \xi_r \in \Bbbk$ with $|\xi_i| = 1$ for each i. Then there exists an increasing sequence c_m of integers such that $\xi_i^{c_m} \to 1$ for each i.*

Proof. By compactness of the set $\{ x \in \Bbbk : |x| = 1 \}$, the sequence $(\xi_1^l, \ldots, \xi_r^l)_{l \in \mathbb{N}}$ in $\Bbbk^r$ has a convergent subsequence, and so there exist $(l_j)_{j \in \mathbb{N}}$ such that $\xi_i^{l_j} \to \lambda_i$, say, for each i. Hence $\xi_i^{l_{j+1} - l_j} \to 1$ as $j \to \infty$.

If the sequence $l_{j+1} - l_j$ is bounded then the ξ_i are all of finite order, and setting the c_m to be successive multiples of the product of their orders will do. Otherwise, take for (c_m) an increasing subsequence of $(l_{j+1} - l_j)$. □

Lemma 5.3.2. *For $h \in PGL(P)$ write $\overline{\pi}_h \in End(V)$ for the projection of V onto A_h with kernel A_h, and let π_h be the corresponding map on P.*

Let $g \in PGL(P)$ be diagonalisable with a representative $\overline{g} \in GL(V)$. Then there exists an infinite set $N \subset \mathbb{N}$ such that:

(i) For any compact subset $K \subset P\backslash a'_g$ and for any neighbourhood U of $\pi(K)$, we have $g^m K \subset U$ for all but finitely many $m \in N$.

(ii) If $g' \in PGL(P)$ has a representative in $GL(V)$ with the same eigenvalues as $\overline{g}$, then (i) remains true with g' in place of g for the same set N.

Proof. Write $\pi := \pi_g$ and $\overline{\pi} := \overline{\pi}_g$. Let $e_0, \ldots, e_n$ be a basis of V consisting of eigenvectors of $\overline{g}$, with corresponding eigenvalues $\lambda_0, \ldots, \lambda_n$, numbered so that A_g is spanned by $e_0, \ldots, e_r$. Scale $\overline{g}$ so that $\lambda_0 = 1$.

Since $|\lambda_0| = \cdots = |\lambda_r| = 1$, Lemma 5.3.1 shows that we may pick $N \subset \mathbb{N}$ such that, for each $i \leq r$, we have $\lambda_i^m \to 1$ as $m \to \infty$ through N. Since $|\lambda_i| < 1$ for $i > r$, in that case we have $\lambda_i^m \to 0$ as $m \to \infty$ through N.

Therefore,

$$\overline{g}^m \to \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} = \overline{\pi}$$

as $m \to \infty$ through N, and so if $p \in P \backslash a'_g$ then $g^m p \to \pi(p)$ as $m \to \infty$ through N.

Now suppose that $K \subset P \backslash a'_g$ is compact and U is a neighbourhood of $\pi(K)$, as in the statement of (i). For $p \in K$ we have just shown that $g^m p \in K$ for all but finitely many $m \in N$. Furthermore, Lemma 5.2.1 shows that $\{ \|g^m|_K\| : m \in N \}$ is bounded, and so there exists a neighbourhood K_p of p such that $g^m K_p \subset U$ for the same $m \in N$.

Since K is compact, it is covered by finitely many K_p, and so $g^m K \subset U$ for all but finitely many $m \in N$ and (i) is proved. To prove (ii), simply note that the set N depended only on the eigenvalues of $\overline{g}$. □

5.4 The Proof of Lemma 5.1

We are at last ready to prove Lemma 5.1. The argument will be slightly clearer if we state the following as a lemma first.

Lemma 5.4.1. *Let V_1 and V_2 be subspaces of V. Then the set $C = \{ g \in GL(V) : gV_1 \subset V_2 \}$ is Zariski-closed in $GL(V)$.*

Proof. Pick a basis $v_1, \ldots, v_r$ for V_2, and extend it to a basis $v_1, \ldots, v_n$ for V. Write for $x \in V$, write x_j for the j co-ordinate of x with respect to this basis. Now pick a basis $w_1, \ldots, w_s$ for V_1.

Then $C = \{ g \in GL(V) : (\forall i)(\forall j > r)((gw_i)_j = 0) \}$, which is clearly closed. □

Corollary 5.4.2. *A linear group G acts irreducibly on V if and only if its Zariski-closure does.*

We now recall and prove Lemma 5.1. The proof is essentially reproduced from [Tits], although in places we provide more detailed justification of individual steps.

Lemma 5.1. *Let G be a Zariski-connected subgroup of $GL_n(\mathbb{k})$, where $\mathbb{k}$ is a locally-compact field, such that the action of G on $\mathbb{k}^n$ is irreducible. Suppose that G possesses a diagonalisable element g with a repulsing point r_g. Then the set*

$$X = \{ x \in G : a_x \text{ and } r_x \text{ are points} \}$$

is Zariski-dense in G.

Proof. Note that, for any $v \in V$, the subspace of V spanned by Gv is invariant under G and so is the whole of V. Hence the set

$$H = \{\, x \in G : xA_g \nsubseteq R'_g \,\} \cap \{\, x \in G : A_g \nsubseteq xR'_g \,\}$$

is non-empty. H is also Zariski-open by Lemma 5.4.1, and so the connectedness of G implies that H is open and dense in G.

Let $h \in H$ and set

$$B = hA'_g \oplus (hA_g \cap R'_g)$$
$$B' = A'_g \oplus (A_g \cap hR'_g).$$

Note that $A_g \nsubseteq hR'_g$ by the definition of H, and so $A_g \nsubseteq B'$ and $B' \neq V$. Similarly $B \neq V$, and so by the same argument as for H the set

$$U = \{\, x \in G : xR_g \nsubseteq B \,\} \cap \{\, x \in G : hR_g \nsubseteq xB' \,\}$$

is non-empty and hence open and dense in G.

Let $u \in U$.

Now define:

$$\pi = \text{ the projection of } V \text{ onto } A_g \text{ with kernel } A'_g$$

$$\pi' = \text{ the projection of } V \text{ onto } hA_g \text{ with kernel } hA'_g$$

Now $hA'_g \subset B$ by definition of B and $uR_g \nsubseteq B$ by definition of U, so certainly

$$uR_g \nsubseteq hA'_g.$$

Furthermore, the definition of U implies that $uR_g \nsubseteq B = hA'_g \oplus (hA_g \cap R'_g)$. Noting that $V = hA'_g \oplus hA_g$, this must mean that $uR_g \cap (hA'_g + (hA_g \backslash R'_g)) \neq \varnothing$, and hence that

$$\pi'(uR_g) \nsubseteq R'_g.$$

Similarly,

$$u^{-1}hR_g \nsubseteq A'_g$$
$$\pi(u^{-1}hR_g) \nsubseteq hR'_g.$$

Considering g, h, u, π, π' now acting on P, and recalling that a_g, a'_g, r_g, r'_g are the respective images of A_g, A'_g, R_g, R'_g in P, we may therefore pick:

- Y a compact neighbourhood of r_g such that
  - (i) $uY \cap ha'_g = \varnothing$
  - (ii) $\pi'(uY) \cap r'_g = \varnothing$
- Y' a compact neighbourhood of $u^{-1}hr_g$ such that
  - (i) $Y' \cap a'_g = \varnothing$
  - (ii) $\pi(Y') \cap hr'_g = \varnothing$
- Z a compact neighbourhood of $\pi'(uY)$ such that $Z \cap r'_g = \varnothing$
- Z' a compact neighbourhood of $\pi(Y')$ such that $Z' \cap hr'_g = \varnothing$

Now Lemma 4.4.2 implies that u, h, h^{-1} have finite norm, and Lemma 5.2.1 shows that $\{ \|g^m|_K\| : m \in \mathbb{N} \}$ is bounded for every compact $K \subset P \backslash a'_g$. Thus, in particular, there exists $r \in \mathbb{R}$ such that

$$\|hg^m h^{-1} u|_Y\| < r \quad \text{and} \quad \|g^m|_{Y'}\| < r \qquad (\dagger)$$

for each $m \in \mathbb{N}$.

Recall from Lemma 5.3.2 that there exists an infinite set $N \subset \mathbb{N}$ with the property that, for any compact subset $K \subset P \backslash a'_g$ and for any neighbourhood D of $\pi(K)$, we have $g^m K \subset D$ for all but finitely many $m \in N$. Recall also that the closure of the group $g^{\mathbb{Z}}$ has finitely many Zariski-connected components, and so we may replace N with an infinite subset such that g^N is contained in one of those components.

Note that if $\overline{g}$ is a representative of g then some representative of hgh^{-1} will have the same eigenvalues as $\overline{g}$, and and also that if g^N is connected then so must $hg^N h^{-1}$ be. Note also that $a'_{hgh^{-1}} = ha'_g$. Recalling that N depends only on the eigenvalues of a representative of g, and not on K and D, the same N will therefore have the same properties for hgh^{-1} as it does for g, with π' in place of π and ha'_g in the place of a'_g.

Thus we have, for all but finitely many $m \in N$:

$$g^m Y' \subset Z' \quad \text{and} \quad hg^m h^{-1} uY \subset Z, \qquad (1)$$

with Y' playing the role of K and Z' playing the role of D in the first expression, and with uY playing the role of K and Z that of D in the second expression.

Now recall from Lemma 4.5.2 that since g has a repulsing point and since Z does not meet r'_g, we have that $\|g^{-m}|_Z\| \to 0$ as $m \to \infty$. Furthermore, by the same lemma, since Y is a neighbourhood of r_g we have that $g^{-m} Z \subset Y^\circ$ for sufficiently large m, where Y° denotes the interior of Y. Hence for all but finitely many $m \in \mathbb{N}$, and so certainly for all but finitely many $m \in N$, we have:

$$\|g^{-m}|_Z\| < r^{-1} \quad \text{and} \quad g^{-m} Z \subset Y^\circ. \qquad (2)$$

Similarly, for all but finitely many $m \in N$ we have:

$$\|hg^{-m} h^{-1}|_{Z'}\| < r^{-1} \|u^{-1}\|^{-1} \quad \text{and} \quad hg^{-m} h^{-1} Z' \subset (Y')^\circ. \qquad (3)$$

Now let N' be the subset of N for which (1), (2) and (3) hold simultaneously, noting that $N \backslash N$ is finite since each holds for all but finitely many $m \in N$. For all $\in N'$, we have:

$$\begin{array}{ll}
g^{-m} hg^m h^{-1} uY \subset Y^\circ & \text{(by (1) and (2))} \\
u^{-1} hg^{-m} h^{-1} g^m Y' \subset (Y')^\circ & \text{(by (1) and (3))} \\
\|g^{-m} hg^m h^{-1} u|_Y\| < 1 & \text{(by (†), (1) and (2))} \\
\|u^{-1} hg^{-m} h^{-1} g^m|_{Y'}\| < 1 & \text{(by (†), (1) and (3))}
\end{array}$$

Thus, by the Converse Lemma (5.1.1), and returning to considering g, h, u as members of $GL(V)$, we have

$$g^{-m} hg^m h^{-1} u \in X$$

for each $m \in N'$.

At this point Tits did something rather cunning. Recall that $N \backslash N'$ is finite, and so $g^N \backslash g^{N'}$ is finite. Since finite sets are closed for the Zariski topology, and since g^N was connected, the set $g^{N'}$ is dense in g^N, and so the Zariski-closure $\overline{X}$ of X in G contains $g^{-m}hg^m h^{-1}u$ for *all* $m \in N$.

Now recall that u was an arbitrary element of U, and that N was chosen for g independently of the choice of u. Thus $g^{-m}hg^m h^{-1}u \in X$ for each $m \in N$ for every $u \in U$. Hence

$$\overline{X} \supset g^{-m}hg^m h^{-1}\overline{U}$$

for each $m \in N$. But U was dense in G, and so for every $m \in N$ we have

$$\overline{X} \supset g^{-m}hg^m h^{-1}G = G,$$

and X is dense in G as claimed. □

6 Representations

We have seen in Section 3 that if G is a connected linear group acting irreducibly on $\Bbbk^n$ then we can find an element g of infinite order in any dense subgroup. We have also seen in Sections 4 and 5 that if G acts irreducibly on $\Bbbk^n$ and g has an attracting point then we may construct a pair of elements generating a free group. These are extremely useful results, but they leave two big questions: how can we be sure that G acts irreducibly, and how can we construct an element with an attracting point?

The following representation theory results answer the first question and set us well on the way to answering the second.

Proposition 6.1. *Let G be a perfect algebraic group with a non-trivial rational representation $\rho : G \to GL_n(\Bbbk)$. Then G possesses a non-trivial irreducible rational representation.*

In particular, since any semisimple linear algebraic group G is perfect and a rational representation of itself, an arbitrary semisimple linear algebraic group has a non-trivial irreducible representation.

Lemma 6.2. *Let $\rho : G \to GL_n(\Bbbk)$ be a rational representation of an algebraic group over an arbitrary field $\Bbbk$ endowed with an absolute value, let $\rho(g) \in \rho(G)$ be diagonal, and let d be the number of eigenvalues of G with maximum absolute value. Suppose $d < n$. Then there exists an absolutely irreducible representation ρ' of G in which $\rho'(g)$ is diagonal and $d = 1$.*

Here, a *rational representation* is just the algebraic-group analogue of a linear representation of an abstract group.

Definition 6.3. *Let G be an algebraic group. A **rational representation** of G is a morphism of algebraic groups $\rho : G \to GL_n(\Bbbk)$. ρ is said to have **degree** n. ρ is said to be **irreducible** if the action of $\rho(G)$ on $\Bbbk^n$ leaves no proper subspace of $\Bbbk^n$ invariant. Writing $\mathbb{K}$ for the algebraic closure of $\Bbbk$, the representation ρ is said to be **absolutely irreducible** if the action of $\rho(G)$ on $\mathbb{K}^n$ is irreducible.*

These results, particularly the parts concerning the existence of irreducible representations, are rather glossed over in [Tits], and I have not seen anything along these lines in the literature, although the central argument that we employ is very simple. For the sake of non-specialists we will give detailed proofs in this section.

Throughout this section we will assume all representations to be of finite degree, and $\Bbbk$ will be an arbitrary field of arbitrary characteristic.

6.1 Quotients and Exterior Powers

Both of the main results from Section 6 assume that a group G has a representation with certain properties, and assert that it must possess an irreducible representation with similar properties. There are two key tools that we will use to construct new representations from the existing ones, so we introduce them in this subsection for use in the subsequent ones.

The first is the ***quotient representation***. Let $\rho : G \to V$ be a representation over an arbitrary field, and suppose that V has a $\rho(G)$-invariant subspace

W. As abstract vector spaces, we can consider the quotient $V/W = V/\underset{W}{\sim}$, where $\underset{W}{\sim}$ is the equivalence relation defined by $u \underset{W}{\sim} v$ if $u - v \in W$. The equivalence classes $v + W$ form a vector space of dimension $\dim V - \dim W$ in the obvious way.

Proposition 6.1.1. *Let $\rho : G \to V$ be a rational representation of a linear algebraic group, and let W be a $\rho(G)$-invariant subspace of V. Then defining $\rho_{V/W} : G \to V/W$ by*

$$\rho_{V/W}(g)(v + W) := \rho(g)(v) + W$$

defines a rational representation of G in V/W.

Proof. Write $n := \dim V$ and $m := \dim W$. The proposition is essentially obvious, but there is a helpful concrete way to see it that will illuminate some of the arguments later in this section. Observe that we may choose a basis $v_1, \ldots, v_n$ for V with respect to which the matrices representing elements of $\rho(G)$ are simultaneously of the form

$$\left(\begin{array}{c|c} M & * \\ \hline 0 & A \end{array}\right),$$

where M is am $m \times m$ invertible matrix acting on the subspace W and A is an $(n-m) \times (n-m)$ invertible matrix. Observe further that

$$\{v_{m+1} + W, \ldots, v_n + W\}$$

is a basis for V/W that highlights an obvious isomorphism from $\langle v_{m+1}, \ldots, v_n \rangle$ to V/W.

With respect to these bases, we may therefore define a morphism (of varieties) $\varphi : \rho(G) \to GL(V/W)$ by

$$\varphi : \left(\begin{array}{c|c} * & * \\ \hline 0 & A \end{array}\right) \mapsto A.$$

It is clear that

$$\left(\begin{array}{c|c} * & * \\ \hline 0 & A \end{array}\right)\left(\begin{array}{c|c} * & * \\ \hline 0 & B \end{array}\right) = \left(\begin{array}{c|c} * & * \\ \hline 0 & AB \end{array}\right),$$

and so φ is a morphism of algebraic groups. Thus $\varphi \circ \rho$ is a rational representation of G. Since $\varphi \circ \rho$ is clearly equal to $\rho_{V/W}$, the proposition is proved. □

Remark 6.1.2. Note that the matrix coefficients of elements of $\rho_{V/W}(G)$ are all coefficients of elements of $\rho(G)$. Therefore, if $\rho(G)$ is defined over a subfield $\Bbbk'$ of $\Bbbk$ then $\rho_{V/W}(G)$ is also defined over $\Bbbk'$.

The second tool we will need for constructing new representations from existing ones is the ***exterior power***. We take the definition from [FulHar].

Definition 6.1.3. *Let V be a finite-dimensional vector space with basis $v_1, \ldots, v_n$. Then the d-**th tensor power** $V^{\otimes d}$ of V is the vector space with basis*

$$\{\, v_{i_1} \otimes \cdots \otimes v_{i_d} : i_1, \ldots, i_d \in \{1, \ldots, n\} \,\}.$$

*The d-**th exterior power** $\bigwedge^d V$ of V is the quotient of $V^{\otimes d}$ by the subspace generated by the vectors $v_{i_1} \otimes \cdots \otimes v_{i_d}$ with two of the i_j equal.*

If $\pi : V^{\otimes d} \to \bigwedge^d V$ is the projection corresponding to this quotient, write $v_{i_1} \wedge \cdots \wedge v_{i_d}$ for $\pi(v_{i_1} \otimes \cdots \otimes v_{i_d})$.

Then the set

$$\{ v_{i_1} \wedge \cdots \wedge v_{i_d} : 1 \leq i_1 < \cdots < i_d \leq n \}$$

is a basis for $\bigwedge^d V$.

Definition 6.1.4. *The d-**th exterior power** $\bigwedge^d \rho$ of a representation $\rho : G \to GL(V)$ is defined by*

$$\bigwedge^d \rho(g)(v_{i_1} \wedge \cdots \wedge v_{i_d}) = \rho(g)v_{i_1} \wedge \cdots \wedge \rho(g)v_{i_d}.$$

6.2 Representations of Perfect Groups

Recall that we defined a *perfect group* G to be one that is generated entirely by commutators, so that $G = (G, G)$, and that semisimple algebraic groups are perfect. In this subsection, we will recall and prove Proposition 6.1, which concerns representations of such groups.

Proposition 6.1. *Let $\rho : G \to GL_n(\Bbbk)$ be a non-trivial rational representation of a perfect linear algebraic group G. Then G possesses a non-trivial irreducible rational representation.*

Proof. Without loss of generality, assume that ρ is a non-trivial representation of G of minimum degree. Consider a minimal invariant non-trivial subspace W of $\Bbbk^n$ under $\rho(G)$, and note that $\rho(G)|_W$ is irreducible.

Suppose $W \neq \Bbbk^n$. Then $\rho(G)|_W$ is of strictly lower degree than ρ, and hence trivial by minimality of ρ. W is therefore one-dimensional, and so we may simultaneously put all the elements $\rho(g)$ of $\rho(G)$ into the form

$$\left(\begin{array}{c|c} 1 & * \\ \hline 0 & \rho_{\Bbbk^n/W}(g) \end{array}\right),$$

where $\rho_{\Bbbk^n/W}(g)$ is an $(n-1) \times (n-1)$ invertible matrix corresponding to the image of G in the quotient representation by W.

However, $\rho_{\Bbbk^n/W}$ is a representation of G of rank $n-1$, and hence trivial by minimality of ρ. We have therefore, in fact, simultaneously written all the elements of $\rho(G)$ in the form

$$\left(\begin{array}{c|c} 1 & * \\ \hline 0 & I_{n-1} \end{array}\right),$$

where I_{n-1} is the $(n-1) \times (n-1)$ identity matrix. But then $\rho(G)$ is isomorphic to a subgroup of the group of unitary upper-triangular matrices, which is well known and easily verified[5] to be solvable. This contradicts the fact that $(\rho(G), \rho(G)) = \rho(G)$.

Hence it must be the case that $W = \Bbbk^n$, and so ρ is an irreducible representation of G. □

[5]The conclusion is obvious if one writes out a general commutator explicitly. Successive commutators have more and more diagonals of zeros above the main diagonal, until eventually one runs out of space for non-zero entries and is left with the identity.

6.3 Reducing the Attracting Eigenspace

In this section we begin with a representation $\rho : G \to GL_n(\Bbbk)$ and a diagonal element $\rho(g)$. Writing $d = d_\rho(g)$ for the number of eigenvalues of $\rho(g)$ with maximum absolute value, we assume that $d < n$ and seek an irreducible representation in which g is still diagonal but so that $d = 1$.

Tits dispatched this with a single rather cryptic comment in [Tits], stating that 'upon extending the field [in order to preserve irreducibility of ρ] and replacing ρ by a suitable composition factor of its d-th tensor power, we may assume that $d = 1$'. It is not totally obvious to a non-specialist (such as the author of this essay) precisely what Tits meant for his readers to do, so a brief exposition is warranted. It is also not clear whether the approach we take here is exactly that intended by Tits, although it is certainly in the same spirit. We take a quotient of the exterior power, where he said to take a composition factor of the tensor power, and then construct an irreducible representation without the need to extend the field.

The following lemma shows that, provided we can find some representation ρ of G for which $d_\rho(g) = 1$, we can construct an irreducible one with the same property.

Lemma 6.3.1. *Let G be a linear algebraic group over an arbitrary field $\Bbbk$ endowed with an absolute value, and let $g \in G$. Suppose there exists a rational representation $\rho : G \to \Bbbk^n$ for which $\rho(g)$ is diagonalisable and has a unique (multiplicity-1) eigenvalue λ with maximum absolute value. Then there exists an absolutely irreducible rational representation $\rho' : G \to \Bbbk^m$ for which $\rho'(g)$ is diagonalisable and has λ as its unique eigenvalue with maximum absolute value.*

Proof. Write $\mathbb{K}$ for the algebraic closure of $\Bbbk$ and let ρ act on $\mathbb{K}^n$. Abbreviate $V := \mathbb{K}^n$. Without loss of generality we may assume that ρ is of minimum degree over $\mathbb{K}$ with $\rho(G)$ defined over $\Bbbk$, the element $\rho(g)$ diagonalisable over $\Bbbk$ and λ the unique maximum eigenvalue of $\rho(g)$. Let $v_1, \ldots, v_n$ be a basis of V consisting of eigenvectors of $\rho(g)$, with corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$ and $\lambda_1 = \lambda$, noting that $\rho(g)$ was diagonalisable over $\Bbbk$ and hence that we may still assume that $\rho(G)$ is defined over $\Bbbk$.

Let W be a maximal $\rho(G)$-invariant subspace of V such that $W \neq V$. We will show that $W = \{0\}$ and hence that V is irreducible. Observe that the minimal polynomial of $\rho(g)|_W$ divides the minimal polynomial of $\rho(g)$, and so $\rho(g)|_W$ is diagonalisable and W is spanned by eigenvectors of $\rho(g)$. By minimality of ρ we must therefore have $v_1 \notin W$, so without loss of generality we may assume that W is spanned by $v_{r+1}, \ldots, v_n$, with $r \geq 1$.

Therefore, $v_1 + W, \ldots, v_r + W$ is a basis for V/W, and so the image of $\rho(g)$ is diagonalisable in V/W with eigenvalues $\lambda_1, \ldots, \lambda_r$, and in particular with unique maximum eigenvalue $\lambda_1 = \lambda$. In view of Remark 6.1.2 the representation $\rho_{V/W}(G)$ is defined over $\Bbbk$, and so by minimality of the degree of ρ we have $r = n$ and $W = \{0\}$, as required. □

This shows that we need not care about irreducibility when constructing the representation required by the main lemma of this section. With this in mind, we now recall and prove that lemma.

Lemma 6.2. *Let $\rho : G \to GL_n(\Bbbk)$ be a rational representation of an algebraic*

group over an arbitrary field $\Bbbk$ endowed with an absolute value, let $\rho(g) \in \rho(G)$ be diagonal, and let d be the number of eigenvalues of G with maximum absolute value. Suppose $d < n$. Then there exists an absolutely irreducible representation ρ' of G in which $\rho'(g)$ is diagonal and $d = 1$.

Proof. Abbreviate $V := \Bbbk^n$. Let $v_1, \ldots, v_n$ be a basis for V consisting of eigenvectors of g, with corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$ numbered so that the maximum absolute value is attained by $\lambda_1, \ldots, \lambda_d$.

Recall that $\bigwedge^d V$ has basis

$$\{ v_{i_1} \wedge \cdots \wedge v_{i_d} : 1 \leq i_1 < \ldots < i_d \leq n \}.$$

Note that each member $v_{i_1} \wedge \cdots \wedge v_{i_d}$ of this basis is an eigenvector for $\bigwedge^d \rho(g)$ with eigenvalue $\lambda_{i_1} \cdots \lambda_{i_d}$. The absolute value of this eigenvalue is clearly maximised if and only if $i_j = j$ for each $j = 1, \ldots, d$, and so in $\bigwedge^d V$ we have $d = 1$.

Hence, by Lemma 6.3.1, there exists an absolutely irreducible representation for which $d = 1$, as required. □

6.4 A Stronger Result – but only in Characteristic 0

Both of the key results proved in Section 6 used the same inductive technique to prove the existence of an irreducible representation with a particular property, given an arbitrary representation with that property. This involved taking a representation of minimal rank with the given property; considering the quotient by an arbitrary subspace; showing that the quotient had the same property as the original representation; and then using the minimality of the original to deduce that the invariant subspace must have been either trivial or the whole space, and hence that the original representation was irreducible.

In fact, much more is true in the case of semisimple algebraic groups over characteristic zero. In Section 14.3 of [Hump. 1], Humphreys concludes that any rational representation of a semisimple algebraic group over characteristic zero is completely reducible, which immediately implies both Proposition 6.1 and a version of Lemma 6.3.1 in that case. However, the proof of this statement is not straightforward, whilst the arguments given here are simple and illuminating and quite sufficient for our needs.

Furthermore, I do not know whether complete reducibility holds in arbitrary characteristic. Whist the characteristic-zero complete-reducibility result would be sufficient to prove the complex version of the Tits Alternative that we have stated in this essay, to rely on it without knowing how to generalise it would somehow have been 'cheating'. Anyway, we have what we need.

The reader interested in pursuing the proof in [Hump. 1] of complete reducibility over characteristic zero should note that it uses, without proof, Weyl's theorem on the complete reducibility of representations of semisimple Lie algebras. Weyl's theorem is proved in 6.3 of [Hump. 2].[6]

[6] Why sell one book when you could sell two?

7 Choosing Absolute Values

In light of Lemma 6.2, we have succeeded in reducing our problem to that of constructing a diagonalisable element of a semisimple algebraic group G whose eigenvalues do not all share the same absolute value. In order to achieve this, Tits made the wonderfully cunning observation that for a given matrix he could play with the field of definition and change the absolute values of the eigenvalues of that matrix.

We have seen (Lemma 2.1.6) that matrices in a semisimple algebraic group have determinant 1, so if we could produce at least one eigenvalue whose absolute value was not 1 then this would be sufficient to show that the eigenvalues do not all have the same absolute value, and we would be done.

The following proposition will allow us to do just that.

Proposition 7.1. *Let $\Bbbk \subset \mathbb{C}$ be a finite field extension of $\mathbb{Q}$ and let $\lambda \in \Bbbk^\times$ be an element of infinite order. Then there exists an extension of $\Bbbk$ to a locally-compact field $\Bbbk'$ endowed with an absolute value $|\cdot|$ for which $|\lambda| \neq 1$.*

The proposition remains true if $\Bbbk$ is a finite extension of its prime subfield with arbitrary characteristic and the proof is essentially the same. However, for the sake of clarity this section will restrict its development of absolute values to characteristic zero, and this will of course be sufficient to prove Theorem 1 in the form we have stated it, over the complex numbers.

The key to the proof of Proposition 7.1 lies in a theorem from [Weil], which was cited in [Tits]. We will state a slightly weakened version of this theorem, which will reduce the amount of theory on which it relies without sacrificing what we need in order to prove Proposition 7.1. We will also restrict to characteristic zero, as this will enable us to give more direct proofs of some of the preliminary results from [Weil], which it is hoped will make the whole argument far easier to follow. For the reader interested in the general proof, we will endeavour to make it clear which of Weil's general arguments correspond to our specific ones.

7.1 p-adic Absolute Values

Recall the definition of an absolute value on a field $\Bbbk$ that was stated in Section 4.2.

Definition 4.2.1. *Let $\Bbbk$ be a field. An **absolute value** on $\Bbbk$ is a function*

$$|\cdot| : \Bbbk \to \mathbb{R}_+$$

that satisfies the following conditions:

(i) $|x| = 0$ *if and only if* $x = 0$

(ii) $|xy| = |x||y|$ *for all* $x, y \in \Bbbk$

(iii) $|x + y| \leq |x| + |y|$ *for all* $x, y \in \Bbbk$

These are all well-known properties of the standard absolute value on $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$; what is not immediately clear is whether there are any other functions on those fields that would satisfy the same properties.

A moment's thought leads to the conclusion that any field can be given an absolute value by setting $|0| = 0$ and $|x| = 1$ otherwise, the so-called *trivial absolute value*, but this is not particularly interesting. Given an existing absolute value $|\cdot|$ and some $\alpha \in \mathbb{R}$ with $0 < \alpha < 1$[7] we can also define a new absolute value $|\cdot|'$ by setting

$$|x|' = |x|^\alpha \qquad \forall x \in \Bbbk,$$

but it is easy to check that any two absolute values related in this way necessarily define the same topology on $\Bbbk$ and so this construction does not give us anything new and interesting to work with.

However, it turns out that there is a whole family of absolute values on $\mathbb{Q}$ that are genuinely different to the standard one, called the *p-adic* absolute values. [Gouv.] provides a very clear and entertaining introduction to their properties, although is more bedtime reading than weighty reference. In this subsection we will present what we need in order for the proof of Proposition 7.1 to make sense.

We begin with a definition.

Definition 7.1.1. *Let $p \in \mathbb{Z}$ be prime. Define the **p-adic absloute value** $|\cdot|_p$ on $\mathbb{Q}$ by*

$$|x|_p = p^{-m} \quad \text{where } x = p^m \frac{a}{b} \text{ with } p \nmid a, b.$$

Denote the usual absolute value by $|\cdot|_\infty$.

It is straightforward to check that $|\cdot|_p$ is indeed a well-defined absolute value. In fact, it satisfies a slightly stronger condition than (iii), which makes it a *non-archimedian* absolute value:

Definition 7.1.2. *Let $|\cdot|$ be an absolute value on a field $\Bbbk$. Then $|\cdot|$ is said to be **non-archimedian** if it satisfies*

(iv) $|x + y| \leq \max\{|x|, |y|\}$ *for all x, $y \in \Bbbk$.*

We remarked above that if two absolute values $|\cdot|$ and $|\cdot|'$ on a field $\Bbbk$ are related by $|\cdot|' = |\cdot|^\alpha$ for some $\alpha \in \mathbb{R}_+$ then they define the same topology on $\Bbbk$. Conveniently, the converse is also true (see the statement and solution of Problem 65 in [Gouv.]). This motivates the following definition.

Definition 7.1.3. *Two absolute values $|\cdot|$ and $|\cdot|'$ on a field $\Bbbk$ are said to be **equivalent** if there exists $\alpha \in \mathbb{R}_+$ such that*

$$|x|' = |x|^\alpha \qquad \forall x \in \Bbbk.$$

Remark. [Gouv.] defines two absolute values to be equivalent if they define the same topology on $\Bbbk$, but in view of the preceding remarks this is equivalent to the definition here.

It is straightforward to check that, for any distinct primes p and q, the absolute values $|\cdot|_p$ and $|\cdot|_q$ are not equivalent, and also that these are not equivalent to the ordinary absolute value. A key theorem in the subject of absolute values on $\mathbb{Q}$, due to Ostrowski, says that these are the *only* non-equivalent non-trivial absolute values on $\mathbb{Q}$.

[7] It is easy to find examples in $\mathbb{R}$ where property (iii) from Definition 4.2.1 fails if $\alpha > 1$; for non-archimedian absolute values (see later) any positive real α will work.

Theorem 7.1.4 (Ostrowski's Theorem)**.** *Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. Then either $|\cdot|$ is equivalent to the ordinary absolute value on $\mathbb{Q}$ or it is equivalent to $|\cdot|_p$ for some prime p.*

For a proof see Theorem 3.1.3 of [Gouv.].

7.2 Completions and Extensions

In Section 7.1 we defined the family of p-adic absolute values $|\cdot|_p$ on $\mathbb{Q}$, and observed that they each induced a different topology on $\mathbb{Q}$. Just like for the ordinary topology, $\mathbb{Q}$ is not complete for any of the p-adic topologies, so we would like to construct completions of $\mathbb{Q}$ with respect to each of these new topologies. In this subsection we will very briefly sketch the construction found in Sections 3.2 and 3.3 of [Gouv.], and highlight some of its properties.

For the ordinary absolute value, the well-known completion of $\mathbb{Q}$ is of course $\mathbb{R}$; the corresponding completions with respect to the p-adic absolute values, the ***p-adic fields*** $\mathbb{Q}_p$, may be constructed by considering the set of Cauchy sequences in $\mathbb{Q}$ with respect to $|\cdot|_p$ as a ring $\mathcal{C}_p$ and defining $\mathbb{Q}_p$ to be the quotient of that ring by the maximal ideal

$$\mathcal{N}_p = \{\, (x_n) \in \mathcal{C}_p : |x_n|_p \to 0 \,\}.$$

[Gouv.] defines an extension of $|\cdot|_p$ to $\mathbb{Q}_p$ as follows. Given $\xi \in \mathbb{Q}_p$, we take a sequence $(x_n) \in \mathcal{C}_p$ that is a representative of ξ and define $|\xi|_p = \lim_{n\to\infty} |x_n|_p$. This is a well-defined non-archimedian absolute value on $\mathbb{Q}_p$.

This allows us to define

$$\mathbb{Z}_p := \{\, x \in \mathbb{Q}_p : |x|_p \leq 1 \,\}$$

to be the closed unit ball around zero. One can check that $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, which explains the choice of notation.

$\mathbb{Z}_p$ is obviously complete, and is in fact also totally bounded because it is covered by $\{\, \overline{B}(x, p^{-n}) : x = 0, 1, \ldots, p^{n-1} \,\}$. This is true because $\mathbb{Z}_p/p^n\mathbb{Z}_p$ is a finite quotient, which is proved in detail in Proposition 3.3.4 and its corollaries in [Gouv.]. Since it is complete and totally bounded, $\mathbb{Z}_p$ is therefore a compact neighbourhood of 0 in $\mathbb{Q}_p$, and so $\mathbb{Q}_p$ is locally compact.

$|\cdot|_p$ also extends to a non-archimedian absolute value on any finite extension of $\mathbb{Q}_p$, as discussed in 5.3 of [Gouv.]. Since such a finite extension may be viewed as a vector space over $\mathbb{Q}_p$, the extension must necessarily also be locally compact, and this is the only property of the extension that we will need, apart, of course, from its existence.

7.3 A Helping Hand from Weil

We are now in a position to cover the real content of Section 7, a result that essentially shows that an algebraic number that is not a root of 1 can always be given an absolute value that is not 1.

Proposition 7.3.1. *Let $\Bbbk$ be a finite algebraic extension of $\mathbb{Q}$, and let $x \in \Bbbk^\times$. Then*

$$|x|_p = 1 \,\forall p \qquad \Longleftrightarrow \qquad \exists m \in \mathbb{N} : x^m = 1.$$

Note that $\forall p$ here includes the case $p = \infty$, although the result would not change.

This, and a positive-characteristic equivalent, are immediate from Theorem 8 of Chapter IV §4 in [Weil]. It would be simple enough to cite this theorem and move on, but its (apparently six-line) proof relies on quite a lot of background and is the culmination of a number of previous results, which means that the argument is not all that transparent, and so we will give a sketch of it in this subsection. Thankfully, by weakening the result slightly we can avoid some of the theory, and by restricting to characteristic zero are able to give more direct proofs of some of the preliminary results and avoid even more.

At the same time, this section is designed partly as a guide to help the interested reader navigate the relevant theory from [Weil] that leads up to the Theorem 8 mentioned above, which should also make it easier for that reader to reconstruct the theorem in the general case.

We begin with a brief exploration of *adeles* of algebraic number fields, along the lines followed in IV §1 of [Weil]. For the remainder of Section 7.3 $\Bbbk$ will be a finite algebraic extension of $\mathbb{Q}$ (the characteristic-zero version of what are called $\mathbb{A}$-*fields* in [Weil]), and $\Bbbk_p$ (with p possibly infinite) will denote the completion of $\Bbbk$ with respect to $|\cdot|_p$.

Definition 7.3.2. *The* ***adele ring*** *of* $\Bbbk$ *is the set*

$$\Bbbk_{\mathbb{A}} = \{\, (x_p) \in \prod_p \Bbbk_p : |x_p|_p \leq 1 \text{ for all but finitely many } p \,\}.$$

The adele ring is given a ring structure by defining addition and multiplication componentwise; see IV §1 [Weil] for full details.

The following lemma shows that the 'diagonal elements' (x_p) with $x_p = \xi$ for all p, where ξ is some element of $\Bbbk$, are elements of $\Bbbk_{\mathbb{A}}$.

Lemma 7.3.3. *Let* $\xi \in \Bbbk$. *Then* $|\xi|_p \leq 1$ *for all but finitely many* p.

Proof. It suffices to prove the lemma for p finite. Since ξ is algebraic over $\mathbb{Q}$ we may write

$$\xi^m = a_{m-1}\xi^{m-1} + \cdots + a_0$$

with the coefficients a_i in $\mathbb{Q}$. But the non-archimedian property of $|\cdot|_p$ then gives

$$|\xi^m|_p \leq \max\{|a_{m-1}\xi^{m-1}|_p, \ldots, |a_0|_p\},$$

which for all p not featuring in the denominators of any of the a_i (and hence for all but finitely many p) yields

$$|\xi^m|_p \leq \max\{|\xi^{m-1}|_p, \ldots, 1\}$$

and hence $|\xi|_p \leq 1$. □

Remark 7.3.4. Theorem 3 of III §1 in [Weil] proves this result differently, deducing it from earlier results, but this more direct proof should be more transparent for the non-specialist. The theorem from [Weil] also features a separate proof for characteristic p.

Lemma 7.3.3 conveniently allows us to embed $\Bbbk$ canonically in $\Bbbk_{\mathbb{A}}$, and from now on we will often identify $\Bbbk$ with this canonical image in $\Bbbk_{\mathbb{A}}$.

The reason for introducing $\Bbbk_{\mathbb{A}}$ at this point is that it allows us to restate the conclusion of Proposition 7.3.1 in a particularly useful way, as observed in IV §4 of [Weil]. In our new language, what we are seeking to show is that

$$\Bbbk \cap \{\, (x_p) \in \Bbbk_{\mathbb{A}} : |x_p|_p = 1 \,\forall p \,\} \quad = \quad \{\, x \in \Bbbk : \exists m \in \mathbb{N} : x^m = 1 \,\}.$$

The first thing to note is that the set on the left-hand side of this extression is a subgroup of $\Bbbk^\times$. The second thing to note is that $\{\, (x_p) \in \Bbbk_{\mathbb{A}} : |x_p|_p = 1 \,\forall p \,\}$ is compact, so that if we can show that $\Bbbk$ is discrete in $\Bbbk_{\mathbb{A}}$ then we will have that $\Bbbk \cap \{\, (x_p) \in \Bbbk_{\mathbb{A}} : |x_p|_p = 1 \,\forall p \,\}$ is a finite group, and hence has only elements of finite order.

The reader will be pleased to hear that this is indeed the case, as the next few results will show.

Definition 7.3.5. *For each prime p, let*

$$\mathbb{Q}^{(p)} = \{\, \xi \in \mathbb{Q} : |\xi|_{p'} \leq 1 \quad \forall p' \text{ prime, } p' \neq p \,\}$$

Clearly $\mathbb{Q}^{(p)}$ consists of the numbers of the form $p^{-n}a$ with $n \in \mathbb{N}$ and $a \in \mathbb{Z}$.

Lemma 7.3.6. *Let p be prime. Then $\mathbb{Q}_p = \mathbb{Q}^{(p)} + \mathbb{Z}_p$.*

Proof. Let $\frac{c}{d} \in \mathbb{Q}$ be written in reduced form. We claim that there exists $\frac{a}{p^n} \in \mathbb{Q}^{(p)}$ such that

$$\left| \frac{c}{d} - \frac{a}{p^n} \right|_p \leq 1. \tag{1}$$

Indeed, if $p \nmid d$ then $|\frac{c}{d}|_p \leq 1$ and so taking $a = 0$ will suffice. If $p|d$ then write $d = bp^n$, where $p \nmid b$. Then b is invertible mod p^n and so we may define $a = b^{-1}c \pmod{p^n}$ so that $p^n|(c - ab)$. Hence $|(c - ab)|_p \leq p^{-n}$. But then

$$\left| \frac{c}{d} - \frac{a}{p^n} \right|_p = \left| \frac{c}{bp^n} - \frac{a}{p^n} \right|_p = \left| \frac{c - ab}{p^n} \right|_p \leq 1$$

and the claim is proved.

Hence $\mathbb{Q} \subset \mathbb{Q}^{(p)} + \mathbb{Z}_p$. To show that $\mathbb{Q}_p \subset \mathbb{Q}^{(p)} + \mathbb{Z}_p$, consider an arbitrary element $\xi \in \mathbb{Q}_p$ and let (ξ_n) be a sequence in $\mathbb{Q}$ such that $\xi_n \to \xi$. By considering the tail of this sequence we may assume that $|\xi_1 - \xi|_p < 1$.

But (1) implies that there exists $\zeta \in \mathbb{Q}^{(p)}$ such that $|\xi_1 - \zeta|_p \leq 1$. Hence $|\xi - \zeta|_p \leq 1$ by the non-archimedian property. Since ξ was arbitrary, this proves the lemma. □

Remark 7.3.7. This is Lemma 1 from IV §2 from [Weil]. Again, Weil gives a proof of this that is based on earlier results, but we presented this more direct proof for the characteristic-zero case with a non-specialist audience in mind.

We now show that $\Bbbk$ is discrete in $\Bbbk_{\mathbb{A}}$ for the special case that $\Bbbk = \mathbb{Q}$, following the proof of Theorem 2 from IV §2 of [Weil].

Lemma 7.3.8. *$\mathbb{Q}$ is discrete in $\mathbb{Q}_{\mathbb{A}}$.*

Proof. Write $A_\infty = \mathbb{R} \times \prod_p \mathbb{Z}_p \subset \mathbb{Q}_\mathbb{A}$. We claim that, viewing $\mathbb{Q}$ as a subset of $\mathbb{Q}_\mathbb{A}$ as described above, we have $\mathbb{Q}_\mathbb{A} = \mathbb{Q} + A_\infty$.

Indeed, let $x = (x_p) \in \mathbb{Q}_\mathbb{A}$, and write P for the set of primes p for which $x_p \notin \mathbb{Z}_p$, which is finite by definition. For each $p \in P$, Lemma 7.3.6 shows that we may write $x_p = \xi_p + x'_p$ with $\xi_p \in \mathbb{Q}^{(p)}$ and $x'_p \in \mathbb{Z}_p$. For notational convenience, for $p \notin P$ or $p = \infty$ set $x'_p = x_p$.

Now define $\xi \in \mathbb{Q}$ by $\xi = \sum_{p \in P} \xi_p$, recalling that P is finite, and define $y \in \mathbb{Q}_\mathbb{A}$ by

$$y_p = x'_p - \sum_{p' \in P \setminus \{p\}} \xi_{p'}.$$

The terms in this right-hand sum are all in $\mathbb{Z}_p$ by the definition of $\mathbb{Q}^{(p)}$, and x'_p is in $\mathbb{Z}_p$ by assumption, and hence y_p is also in $\mathbb{Z}_p$ by the non-archimedian property. Hence $y \in A_\infty$ with $x = \xi + y$, and so $\mathbb{Q}_\mathbb{A} = \mathbb{Q} + A_\infty$ and the claim is proved.

Now, for each finite p the set $\mathbb{Z}_p$ is open as well as closed (a straightforward application of the non-archimedian property), so A_∞ is open in $\mathbb{Q}_\mathbb{A}$. Thus if we can show that $\mathbb{Q}$ is discrete in A_∞ then we may deduce that $\mathbb{Q}$ is discrete in $\mathbb{Q}_\mathbb{A}$. It would be sufficient to show that $\mathbb{Q}$ was discrete in any of the factors of the product A_∞. But clearly $\mathbb{Q} \cap A_\infty = \mathbb{Z}$, and so in particular the projection of $\mathbb{Q} \cap A_\infty$ onto the first factor $\mathbb{R}$ of the product A_∞ is $\mathbb{Z}$, which is discrete in $\mathbb{R}$. □

We now move on to the general case. Viewing $\mathbb{k}$ as a finite-dimensional vector space over $\mathbb{Q}$, we begin by defining, for an arbitrary finite-dimensional $\mathbb{k}$-vector space E, an analogue of the adele ring of $\mathbb{k}$.

Definition 7.3.9. *Let E be a finite-dimensional vector space over $\mathbb{k}$. Then write*

$$E_\mathbb{A} = E \otimes_\mathbb{k} \mathbb{k}_\mathbb{A},$$

We can naturally embed E in $E_\mathbb{A}$ via the mapping $e \mapsto e \otimes 1$, where 1 is viewed as an element of $\mathbb{k}_\mathbb{A}$ via the previously-discussed embedding of $\mathbb{k}$ into $\mathbb{k}_\mathbb{A}$.

An intuitively helpful way of thinking of $E_\mathbb{A}$ is as follows. Fixing a basis of E determines an isomorphism of $\mathbb{k}^n$ onto E, and hence of $(\mathbb{k}_\mathbb{A})^n$ onto $E_\mathbb{A}$. We define the topology on $E_\mathbb{A}$ to be the topology of $(\mathbb{k}_\mathbb{A})^n$ when the two spaces are identified via this isomorphism. It is straightforward to check that this does not depend on the choice of basis for E.

Definition 7.3.10. *Let $\mathbb{k}'$ be a finite algebraic extension of $\mathbb{k}$. Viewing $\mathbb{k}'$ as finite-dimensional vector space over $\mathbb{k}$, which we will temporarily call $E(\mathbb{k})$, define $(\mathbb{k}'/\mathbb{k})_\mathbb{A}$ by $(\mathbb{k}'/\mathbb{k})_\mathbb{A} := E(\mathbb{k})_\mathbb{A}$.*

Of course, as with the general $\mathbb{k}$-vector space E above, we have a natural embedding of $\mathbb{k}'$ into $(\mathbb{k}'/\mathbb{k})_\mathbb{A}$. Furthermore, if $[\mathbb{k}' : \mathbb{k}] = n$ and we fix a $\mathbb{k}$-basis of $\mathbb{k}'$ we have an isomorphism of $(\mathbb{k}_\mathbb{A})^n$ onto $(\mathbb{k}'/\mathbb{k})_\mathbb{A}$, which is the identity from the natural image of $\mathbb{k}'$ in $(\mathbb{k}_\mathbb{A})^n$ to the natural image of $\mathbb{k}'$ in $(\mathbb{k}'/\mathbb{k})_\mathbb{A}$.

On the other hand, $\mathbb{k}'$ is an algebraic number field in its own right and embeds naturally into its own adele ring $\mathbb{k}'_\mathbb{A}$. Conveniently, these embeddings end isomorphisms lead naturally to the following result, a detailed proof of which can be seen in Theorem 1 of IV, §1, [Weil].

Lemma 7.3.11. *Let $\Bbbk'$ be a finite algebraic extension of $\Bbbk$. Then there is a surjective isomorphism*

$$\psi : (\Bbbk'/\Bbbk)_{\mathbb{A}} \to \Bbbk'_{\mathbb{A}}$$

such that $\psi(\Bbbk') = \Bbbk'$ with respect to the natural embeddings and the restriction $\psi|_{\Bbbk'}$ is the identity.

This allows us to prove Lemma 7.3.8 in general.

Lemma 7.3.12. *Let $\Bbbk$ be an algebraic number field. Then $\Bbbk$ is discrete in $\Bbbk_{\mathbb{A}}$.*

Proof. Write $n := [\Bbbk' : \Bbbk]$. By Lemma 7.3.11 we may identify $\Bbbk_{\mathbb{A}}$ with $(\mathbb{Q}_{\mathbb{A}})^n$, respecting the natural embedding of $\Bbbk$ in each. Viewing $\Bbbk$ as $\mathbb{Q}^n$, we may therefore identify $\Bbbk \subset \Bbbk_{\mathbb{A}}$ with $\mathbb{Q}^n \subset (\mathbb{Q}_{\mathbb{A}})^n$. But by Lemma 7.3.8 we have that $\mathbb{Q}$ is discrete in $\mathbb{Q}_{\mathbb{A}}$, and hence $\mathbb{Q}^n$ is discrete in $(\mathbb{Q}_{\mathbb{A}})^n$ and so $\Bbbk$ is discrete in $\Bbbk_{\mathbb{A}}$. □

At last we are able to prove Proposition 7.3.1, following the corresponding part of the proof of Theorem 8 in IV §4 of [Weil].

Proposition 7.3.1. *Let $\Bbbk$ be a finite algebraic extension of $\mathbb{Q}$, and let $x \in \Bbbk^\times$. Then*

$$|x|_p = 1 \,\forall p \qquad \Longleftrightarrow \qquad \exists m \in \mathbb{N} : x^m = 1.$$

Proof. Write $R := \Bbbk \cap \{\, (x_p) \in \Bbbk_{\mathbb{A}} : |x_p|_p = 1 \,\forall p \,\}$.

As discussed above, the conclusion of the proposition is equivalent to the statement that R is precisely the set of roots of 1 in $\Bbbk^\times$. It is clear that $\{\, (x_p) \in \Bbbk_{\mathbb{A}} : |x_p|_p = 1 \,\forall p \,\}$ is compact, and by Lemma 7.3.12 we know that $\Bbbk$ is discrete in $\Bbbk_{\mathbb{A}}$. Hence R is a finite group, and so has only elements of finite order. Conversely, any $\xi \in \Bbbk$ that is a root of 1 must always have $|\xi| = 1$ for any absolute value $|\cdot|$, and hence $\xi \in R$. □

Remark 7.3.13. As was alluded to in various remarks throughout this subsection, Proposition 7.3.1 is a slightly weakened version of the characteristic-zero case of Theorem 8 from IV §4 of [Weil]. In the original theorem, Weil proved that

$$|x|_p \leq 1 \,\forall p \qquad \Longleftrightarrow \qquad \exists m \in \mathbb{N} : x^m = 1,$$

with an at-most sign on the left-hand side where we have an equals sign. The extra strength comes from Artin's product formula, which is proved as Theorem 5 of from IV §4 of [Weil] and states that, for each x in $\Bbbk$,

$$\prod_p |x|_p = 1.$$

This is easy to see for $x \in \mathbb{Q}$ (remembering to include the case $p = \infty$), but much less so for arbitrary algebraic x. Indeed, the fact that it is obvious for $x \in \mathbb{Q}$ masks a certain subtlety, which is that there was nothing in our construction of the p-adic absolute values to guarantee that the product formula should hold even in this easy case. Replacing a single p-adic absolute value $|\cdot|_p$ with a distinct but equivalent absolute value, say $|\cdot|_p^{1/2}$, would invalidate the product formula, despite being at first sight a purely cosmetic change.

This could make the product formula seem like a happy accident. However, the construction of absolute values followed in [Weil] reveals something deeper. Rather than picking absolute values on a field $\Bbbk$ and then costructing the corresponding completions, Weil starts with the collection of non-discrete locally-compact flields that extend $\Bbbk$ and in which $\Bbbk$ is dense. Given such a locally-compact field he then defines an absolute value in terms of its Haar measure, via something called the 'module' of an automorphism. This construction works for so-called $\mathbb{A}$-fields over arbitrary characteristic, and in each case yields a version of the product formula. Full details are given in III of [Weil]; the 'module' via which the absolute values are constructed is defined in I §2 of the same source.

7.4 The Proof of Proposition 7.1

We now recall and prove Proposition 7.1, which is Lemma 4.1 in [Tits].

Proposition 7.1. *Let $\Bbbk \subset \mathbb{C}$ be a finite field extension of $\mathbb{Q}$ and let $\lambda \in \Bbbk^\times$ be an element of infinite order. Then there exists an extension of $\Bbbk$ to a locally-compact field $\Bbbk'$ endowed with an absolute value $|\cdot|$ for which $|\lambda| \neq 1$.*

Proof. Let $\Bbbk_a$ be the algebraic closure of $\mathbb{Q}$ in $\Bbbk$, so that $\Bbbk_a$ is a finite algebraic extension of $\mathbb{Q}$, and let T be a transcendence basis for $\Bbbk$ over $\Bbbk_a$, chosen to include λ if $\lambda \notin \Bbbk_a$. Note that T is finite, since $\Bbbk$ is a finite extension of $\Bbbk_a$.

If $\lambda \in T$ then let $\varphi : T \cup \{1\} \to \mathbb{C}$ be an injection such that:

(i) $\varphi(1) = 1$

(ii) $\varphi(T)$ is algebraically independent over $\mathbb{Q}$ (possible since the transcendence degree of $\mathbb{C}$ over $\mathbb{Q}$ is infinite)

(iii) $|\varphi(\lambda)| \neq 1$ (so send λ to your favourite transcendental number of absolute value $\neq 1$).

Extending φ to an injective field homomorphism $\widehat{\varphi} : \Bbbk_a(T) \hookrightarrow \mathbb{C}$ we may identify $\Bbbk_a(T)$ with a subfield of $\mathbb{C}$, and since $\mathbb{C}$ is algebraically closed and $\Bbbk$ is an algebraic extension of $\Bbbk_a(T)$ we may therefore identify $\Bbbk$ with a subfield of $\mathbb{C}$. Since $|\lambda| \neq 1$ under this identification, setting $\Bbbk' = \mathbb{C}$ proves the theorem for λ transcendental.[8]

If $\lambda \in \Bbbk_a$ then Proposition 7.3.1 shows that there exists p for which $|\lambda|_p \neq 1$. Let $\Bbbk_p$ be the completion of $\Bbbk_a$ with respect to $|\cdot|_p$; this is automatically locally compact as discussed at the end of Subsection 7.2. Since the transcendence degree of $\Bbbk_p$ over $\Bbbk_a$ is infinite there exists an injection $\varphi : T \cup \{1\} \to \Bbbk_p$ such that $\varphi(T)$ is algebraically independent in $\Bbbk_p$, just as there was with $\mathbb{C}$ before. Again, extending φ to an injective field homomorphism $\widehat{\varphi} : \Bbbk_a(T) \hookrightarrow \Bbbk_p$ allows us to identify $\Bbbk_a(T)$ with a subfield of $\Bbbk_p$. Since $\Bbbk$ is a finite algebraic extension of $\Bbbk_a(T)$, we may therefore take a finite algebraic extension $\Bbbk'$ of $\Bbbk_p$ and identify $\Bbbk$ with a subfield of $\Bbbk'$. Since $\Bbbk'$ is finite-dimensional as a vector space over

[8] We would now be done if we knew that elements of $\mathbb{C}$ of infinite order with absolute value 1 were transcendental. For $a \in \mathbb{R}$ algebraic, if $e^{ia\pi}$ is not a root of 1 then $a \in \mathbb{R}\backslash\mathbb{Q}$ and so the Gelfond-Schneider theorem (Theorem 3.1, Section 8.3, [Rose]) shows that $e^{ia\pi} = (-1)^a$ is trenscendental. However, I do not know what happens if a is transcendental, or even whether this is known.

the locally-compact field $\mathbb{k}_p$ it is locally compact itself, and hence satisfies the requirement of the lemma. $\square$

8 Proof of the Tits Alternative

We now begin the final part of the proof of Theorem 1. It has been necessary to collect a number of quite varied results along the way, so for the convenience of the reader we recall them here.

Lemma 1.1. *If G in Theorem 1 is not virtually solvable then we may assume its Zariski-closure to be a semisimple algebraic group.*

Corollary 2.1.5. *Let G be a semisimple algebraic group. Then G is perfect.*

Corollary 2.1.6. *Let $G < GL_n(\mathbb{k})$ be a semisimlpe linear algebraic group. Then $G \subset SL_n(\mathbb{k})$.*

Proposition 2.2.2. *Let G be a semisimple algebraic group. Then the set of semisimple elements of G contains a dense open subset of G.*

Proposition 3.1. *Let $G < GL_n(\mathbb{C})$ be a finitely-generated group of matrices acting irreducibly on $\mathbb{C}^n$, and let F be the set of all elements of finite order in G. Suppose F is Zariski-dense in G. Then G is finite.*

Lemma 4.1. *Let $G < GL_n(\mathbb{k})$ be a linear group over a locally-compact field $\mathbb{k}$ such that the Zariski-closure of G is Zariski-connected (and hence irreducible as a variety) in $GL_n(\mathbb{k})$ and the action of G leaves no subspace of $\mathbb{k}^n$ invariant. Suppose G possesses a diagonalisable element g with an attracting point and a repulsing point. Then there exist $g' \in G$ and $m \in \mathbb{N}$ such that g^m and $(g')^m$ generate a non-abelian free group.*

Lemma 5.1. *Let $\mathbb{k}$ be a locally-compact field, and let G be a Zariski-connected subgroup of $GL_n(\mathbb{k})$ acting irreducibly on $\mathbb{k}^n$. Suppose that G possesses a diagonalisable element g with a repulsing point r_g. Then the set*

$$X = \{\, x \in G : a_x \text{ and } r_x \text{ are points} \,\}$$

is Zariski-dense in G.

Proposition 6.1. *Let G be a perfect algebraic group with a non-trivial rational representation $\rho : G \to GL_n(\mathbb{k})$. Then G possesses a non-trivial irreducible rational representation.*

Lemma 6.2. *Let $\rho : G \to GL_n(\mathbb{k})$ be a rational representation of an algebraic group over an arbitrary field $\mathbb{k}$ endowed with an absolute value, let $\rho(g) \in \rho(G)$ be diagonal, and let d be the number of eigenvalues of G with maximum absolute value. Suppose $d < n$. Then there exists an absolutely irreducible representation of ρ' of G in which $\rho'(g)$ is diagonal and $d = 1$.*

Proposition 7.1. *Let $\mathbb{k} \subset \mathbb{C}$ be a finite field extension of $\mathbb{Q}$ and let $\lambda \in \mathbb{k}^\times$ be an element of infinite order. Then there exists an extension of $\mathbb{k}$ to a locally-compact field $\mathbb{k}'$ endowed with an absolute value $|\cdot|$ for which $|\lambda| \neq 1$.*

8.1 The Proof

We are finally in a position to prove the following, which by Lemma 1.1 immediately implies Theorem 1. The bulk of the following lemma is found in Proposition 4.3 of [Tits], although we have stripped out much of the conclusion in that paper concerning the density of elements generating free subgroups.

Lemma 8.1.1. *Let $G < GL_n(\mathbb{C})$ be a finitely-generated non-trivial linear group whose Zariski-closure $\mathfrak{G}$ is semisimple. Then G contains a non-abelian free subgroup.*

Proof. Proposition 6.1 shows that $\mathfrak{G}$ has a non-trivial irreducible rational representation, so without loss of generality we may assume that $\mathfrak{G}$ acts irreducibly on $GL_n(\mathbb{C})$.

By Proposition 3.1 the elements of G with finite order are not dense in $\mathfrak{G}$, and by Proposition 2.2.2 the semisimple elements of $\mathfrak{G}$ contain an open dense subset of $\mathfrak{G}$. Therefore, G must possess a semisimple element g of infinite order. Corollary 2.1.6 implies that $\mathfrak{G} < SL_n(\mathbb{C})$, and so $\det g = 1$.

Let $\{g_1, \ldots, g_r\}$ be a generating set of G, and fix a basis with respect to which g is diagonal. Let $\Bbbk$ be the finite field extension of $\mathbb{Q}$ generated by the coefficients of the matrices representing $g_1, \ldots, g_r$ and the eigenvalues of g. We may now consider G to be a subgroup of $GL_n(\Bbbk)$. As is remarked in the proof of Proposition 4.3 in [Tits], this does not change the Zariski topology on G.

The fact that g is of infinite order implies that one of its eigenvalues, say λ, is not a root of unity. Since $\Bbbk$ is a finite extension of $\mathbb{Q}$, by Proposition 7.1 we may extend $\Bbbk$ to a locally-compact field with an absolute value $|\cdot|$ for which $|\lambda| \neq 1$. Write d for the number of eigenvalues of g with maximum absolute value; since $\det g = 1$ we have $d < \dim V$.

Note that, since a subgroup of G is normal in G and solvable if and only if its closure is normal in $\mathfrak{G}$ and solvable (Proposition 1.2.4), we may still assume that the closure of G is semisimple. By Lemma 6.2, we may assume that $d = 1$ and that G acts absolutely irreducibly on $\Bbbk^n$, and so by Lemma 5.1 the set of elements of G that have both an attracting point and a repulsing point is dense in G. We may therefore pick one that is semisimple, say h. By absloute irreducibility we may finitely extend $\Bbbk$ so that h is diagonalisable, maintaining the irreducibility of the action of G. Lemma 4.1 then allows us to construct a pair of elements generating a free group. □

9 Encore

Theorem 2. *Theorem 1 remains true if G is not finitely generated.*

Proof. Let G be an arbitrary complex linear group, not necesssarily finitely generated, and suppose G is not virtually solvable. Let $\mathfrak{G}$ be the Zariski-closure of G; as before, if G is not virtually solvable then we may assume $\mathfrak{G}$ to be semisimple.

Let $\mathfrak{G}'$ be the connected subgroup of $\mathfrak{G}$ of greatest dimension that is the closure of a finitely-generated subgroup of G, and let G' be a finitely-generated subgroup of G that is dense in $\mathfrak{G}'$. For any $h \in G$ note that $h^{-1}\mathfrak{G}'h$ is connected and the closure of $h^{-1}G'h$, which is finitely generated, and so $h^{-1}\mathfrak{G}'h \subset \mathfrak{G}'$ and $\mathfrak{G}'$ is normalised by G. We stated in Proposition 1.2.4 that normalisers of closed subgroups are closed, and so $\mathfrak{G}'$ is normal in $\mathfrak{G}$.

Furthermore, for any $g \in G$ there exists $m \in \mathbb{N}$ such that the closure $\overline{\langle g^m \rangle}$ of $\langle g^m \rangle$ is a connected group, since $\overline{\langle g \rangle}^\circ$ has finite index in $\overline{\langle g \rangle}$. The closure of $\langle G', g^m \rangle$ is therefore connected, and so is contained in (and hence equal to) $\mathfrak{G}'$. We therefore have that $\mathfrak{G}'$ is a connected normal subgroup of $\mathfrak{G}$ containing a power of every element of G.

We now make use of a theorem of Schur (Theorem 36.14, [CurRei]), which states that any torsion subgroup of $GL_n(\mathbb{C})$ contains an abelian normal subgroup of index at most C, where C is a constant depending on n. Since $\mathfrak{G}$ is semisimple, G cannot have a normal solvable subgroup of finite index, and so this implies that G is not a torsion group and hence that $\mathfrak{G}'$ is not trivial.

But a non-trivial connected normal subgroup of a semisimple group is semisimple, and so G' is finitely generated and its closure $\mathfrak{G}'$ is semisimple. Hence Lemma 8.1.1 implies that there exists a non-abelian free subgroup $F < G' < G$. □

Remarks 9.1.

(i) This formed part of the proof of Theorem 3 in Section 4.5 of [Tits], where it was in fact shown that $\mathfrak{G}' = \mathfrak{G}$.

(ii) In the application of Schur's theorem here we have used the fact that the field is $\mathbb{C}$.

(iii) In [Tits] the example of the full linear group over an infinite algebraic extension of a finite field is given to show that the Tits Alternative is not necessarily satisfied by a linear group in non-zero characteristic if the group is not finitely generated.

10 Post Mortem

It would of course have been possible to have stated Theorem 1 for arbitrary complex linear groups and to have incorporated the proof of Theorem 2 from the beginning. Indeed, this was the approach taken in [Tits], and in a way it would have been slightly 'better' as it would have removed the need in the proof of Lemma 1.1 to appeal to the fact that a finite-index subgroup of a finitely-generated group is finitely generated.

This would also have removed the need to appeal, in demonstrating the perfection of a semisimple algebraic group in Section 2, to the fact that a semisimple group can be decomposed as the almost-direct product of simple subgroups. Free to consider arbitrary subgroups, not just those of finite index, we could have restricted attention to a single simple subgroup, the existence and perfection of which we established easily. However, this essay was intended to be entertaining as well as mathematically informative, and I felt that the former goal (and, indeed, the latter) would be well served by arranging the proof in the order that I did.

In any case, there was plenty of high-quality mathematics in Tits's proof. We dispensed with the theory early on, and from Section 3 onwards there were a number of particularly appealing moves. As I highlighted in the proof of Lemma 5.1, when constructing elements of the form $g^{-m}hg^mh^{-1}u$ that belonged to the set X there was an extremely cunning density argument that allowed us to pick a single integer m for which this held simultaneously for all $u \in U$. Without this trick the rest of the argument would not have worked.

Perhaps more obviously cunning was the change of field that allowed us, in the proof of Lemma 8.1.1, to force the absolute value of a particular eigenvalue not to equal 1. Even the construction of the free group in Section 4 was pleasing in its simplicity, and in the absence of the rest of the argument would still have provided a very nice proof that there exist free groups of matrices.

Since the original proof given by Tits in the '70s there have been some strengthenings of his alternative. Most recently (to the best of my knowledge), Emmanuel Breuillard ([Breu. 1] and [Breu. 2]) put a bound on the number of group generators of a non-virtually solvable group that one would need to combine in order to produce a pair of elements generating a free group. This bound depends only on the dimension of the space on which the group acts, and not on the field or on the choice of generating set.

Nonetheless, the original result remains remarkable and its proof ingenious, and I hope the reader has enjoyed this take on it.

References

[Borel] Borel, A. *Linear Algebraic Groups*, 2nd ed. Springer-Verlag, New York, 1991.

[Breu. 1] Breuillard, E. *A Height Gap Theorem for Finite Subsets of $SL_n(\overline{\mathbb{Q}})$ and Non Amenable Subgroups*, preprint April 2008.

[Breu. 2] Breuillard, E. *A Strong Tits Alternative*, preprint April 2008.

[CurRei] Curtis, C. W. & Reiner, I. *Representation Theory of Finite Groups and Associative Algebras*, Interscience, New York, 1962.

[Fult.] Fulton, W. *Algebraic Curves*, The Benjamin/Cummings Publishing Company, Manlo Park, CA, 1969.

[FulHar] Fulton, W. & Harris, J. *Representation Theory – A First Course*, Springer-Verlag, New York, 1991.

[Gouv.] Gouvêa, F. Q. *p-adic Numbers – An Introduction*, Springer-Verlag, Berlin, 1993.

[Hart.] Hartshorne, R. *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[Hump. 1] Humphreys, J. E. *Linear Algebraic Groups*, Springer-Verlag, New York, 1975.

[Hump. 2] Humphreys, J. E. *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, New York, 1972.

[Hump. 3] Humphreys, J. E. *Conjugacy Classes in Semisimple Algebraic Groups*, American Mathematical Society, Providence, RI, 1995.

[Lang] Lang, S. *Algebra*, 3rd ed., Springer-Verlag, New York, 2002.

[Rose] Rose, H. E. *A Course in Number Theory*, Oxford University Press, 1988.

[Spr.] Springer, T. A. *Linear Algebraic Groups*, 2nd ed., Birkhäuser, Boston, 1998.

[Tits] Tits, J. *Free Subgroups in Linear Groups*, Journal of Algebra **20** (1972), 250-270.

[Wehr.] Wehrfritz, B. A. F. *Infinite Linear Groups*, Springer-Verlag, Berlin, 1973.

[Weil] Weil, A. *Basic Number Theory*, Springer-Verlag, Berlin, 1967.