TOPICS ON LINEAR GROUPS

EMMANUEL BREUILLARD

LECTURE NOTES WRITTEN BY CONSTANTIN KOGLER

Contents

These are lecture notes for a graduate course given at Oxford in Trinity term 2023. The following topics are covered:

(1) Torsion linear groups.
(2) The Tits alternative and its topological version.
(3) Proximal elements and results of Abels-Margulis-Soifer and Golsheid-Margulis.
(4) The eigenvalue spectrum of Zariski dense subgroups and the Benoist cone.
(5) Galois generic elements following Prasad-Rapinchuk.
(6) Bounded generation and diophantine properties of Zariski-dense subgroups.

1. Jordan-Selberg-Schur

1.1. **Jordan's Theorem.** As was shown by Camille Jordan in 1878, a finite linear group over a field of characteristic zero is close to being abelian.

Theorem 1.1. *(Jordan 1878,* [Jor78]*) For every n there exists a constant $J(n)$ such that any finite subgroup of $\mathrm{GL}_n(K)$ over a field of characteristic zero has a normal abelian subgroup of index $\leq J(n)$.*

Jordan's original proof established no explicit bound on $J(n)$. A shorter argument was found by Bierberbach and Frobenius (1911), whose ideas we exploit to show that $J(n) \leq 9^{2n^2}$.

We proceed with two reductions, first to the case that $K = \mathbb{C}$ and we then may assume that the finite group is contained in the group of unitary matrices. To show the first reduction, observe that without loss of generality K is finitely generated, i.e. there are elements, $\alpha, \ldots, \alpha_\ell \in K$ such that $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_\ell)$. Indeed, we may replace K with the field generated by the coefficients of all the matrices of our given finite group. The next lemma shows that we can set $K = \mathbb{C}$.

Lemma 1.2. *A finitely generated field K of characteristic zero can be embedded into $\mathbb{C}$.*

Proof. We can consider K as a finite extension of a purely transcendental extension $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_\ell)$ (cf. [Lan12] Chapter VIII). Since $\mathbb{C}$ has infinite transcendence degree over $\mathbb{Q}$, L embeds into $\mathbb{C}$. The claim follows using that $\mathbb{C}$ is algebraically closed and therefore for any algebraic element x over L, we can embedded $L(x)$ into $\mathbb{C}$. Indeed if $P \in L[X]$ is the minimal polynomial of x and $y \in \mathbb{C}$ is a root of P then mapping x to y yields a field embedding $L(x) \longrightarrow \mathbb{C}$. Iterating the last observation, the proof is concluded as K is a finite extension of L. □

For the remainder of the proof we denote by G a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$. We next show that we can assume without loss of generality that $G \subset U_n(\mathbb{C})$, where

$$U_n(\mathbb{C}) = \{g \in \mathrm{GL}_n(\mathbb{C}) \,:\, g^{-1} = g^*\}$$

is the group of unitary matrices.

Lemma 1.3. *G is conjugated to a subgroup of $U_n(\mathbb{C})$.*

Proof. Consider the G-invariant hermitian inner product on $\mathbb{C}^n$ defined by

$$\langle x, y\rangle_G := \frac{1}{|G|}\sum_{g\in G}\langle gx, gy\rangle$$

for $x, y \in \mathbb{C}^n$. As all hermitian inner products are equivalent up to a change of basis, there is $P \in \mathrm{GL}_n(\mathbb{C})$ such that $PGP^{-1} \subset U_n(\mathbb{C})$. □

Denote by $||\cdot||$ the operator norm $M_n(\mathbb{C})$ induced by the standard hermitian inner product and for $r > 0$,

$$B(r) = \{A \in M_n(\mathbb{C}) \,:\, ||A|| < r\}.$$

Lemma 1.4. *The ball $B(1)$ can be covered by at most 9^{2n^2} many balls of radius $\frac{1}{4}$.*

Proof. Let N be the maximal number of disjoint balls of radius $\frac{1}{8}$ contained in $B(1 + \frac{1}{8})$. Then the balls with the same center and radius $\frac{1}{4}$ cover $B(1)$ as otherwise the previous collection of balls would not be maximal. Denote by vol the

euclidean volume on $M_n(\mathbb{C}) \cong \mathbb{C}^{n^2} \cong \mathbb{R}^{2n^2}$. Then it holds for $r > 0$, $\mathrm{vol}(B(r)) = r^{2n^2}\mathrm{vol}(B(1))$. Therefore by volume comparison,

$$\frac{N}{8^{2n^2}}\mathrm{vol}(B(1)) \leq \mathrm{vol}(B(1+\tfrac{1}{8})) = (1+\tfrac{1}{8})^{2n^2}\mathrm{vol}(B(1)),$$

showing that $N \leq 9^{2n^2}$. □

We now turn to the proof of Jordan's Theorem. A central ingredient in the proof is the commutator shrinking property of $U_n(\mathbb{C})$. Indeed, for $x, y \in U_n(\mathbb{C})$ it holds for the commutator $[x,y] = xyx^{-1}y^{-1}$ that

$$\begin{aligned} ||[x,y]-1|| &= ||xy - yx|| \\ &= ||(x-1)(y-1) - (y-1)(x-1)|| \\ &\leq 2||y-1||\,||x-1||. \end{aligned} \tag{1.1}$$

Proof. (of Theorem 1.1) Consider the subgroup

$$A = \langle B_G(\tfrac{1}{2})\rangle,$$

where $B_G(\frac{1}{2}) = \{x \in G : ||x-1|| < \frac{1}{2}\}$. If $xA \neq yA$ with $x, y \in G$ then $x^{-1}y \notin B_G(\frac{1}{2})$ and therefore $||1 - x^{-1}y|| = ||x-y|| > \frac{1}{2}$. Therefore x and y are not contained in the same ball of radius $\frac{1}{4}$ and thus by Lemma 1.4, $[G:A] \leq 9^{2n^2}$.

We claim that A is a normal abelian subgroup. Notice that for any $g, h \in U_n(\mathbb{C})$,

$$||h-1|| = ||h - g^{-1}g|| = ||ghg^{-1} - 1||.$$

Therefore $B_G(\frac{1}{2})$ is invariant under conjugation and A is a normal subgroup of G.

It remains to show that A is abelian and we may assume without loss of generality that A acts irreducibly on $\mathbb{C}^n$, i.e. that there are no non-trivial A-invariant subspaces. Indeed, if the action is reducible, and the restriction of A to each of the subspaces is abelian, then A must be abelian.

It therefore holds by Schur's Lemma that the center $Z(A)$ of A consists of scalar matrices. If the latter would not be case, the eigenspaces of central elements form non-trivial invariant subspaces.

We assume for a contradiction that $A \backslash Z(A)$ is non-empty. Since A is finite we may pick $x \in A \backslash Z(A)$ that minimizes the quantity

$$\min_{\lambda \in \mathbb{S}^1} ||x - \lambda||.$$

Similar to the commutator shrinking property, it holds for all $y \in B_G(\frac{1}{2})$ and $\lambda \in \mathbb{S}^1$,

$$\begin{aligned} ||[x,y]-1|| &= ||xy - yx|| \\ &= ||(x-\lambda)(y-1) - (y-1)(x-\lambda)|| \\ &\leq 2||y-1||\,||x-\lambda|| \\ &< ||x-\lambda||. \end{aligned}$$

Therefore $[x,y] \in Z(A)$ is a scalar matrix and we write $[x,y] = e^{i\phi} \cdot \mathrm{Id}_n$ for $\phi \in \mathbb{R}$.

We claim that indeed $[x,y] = \mathrm{Id}_n$. Observe $xyx^{-1} = e^{i\phi}y$. So y and $e^{i\phi}y$ are conjugate and therefore have the same eigenvalues. More precisely, if $e^{i\theta}$ is an eigenvalue of y, then so is $e^{i(\theta+\phi)}$. Yet since all eigenvalues are contained in $\{|z-1| < \frac{1}{2}\} \subset \mathbb{C}$ as $y \in B_G(\frac{1}{2})$, it follows that $\phi \equiv 0 \bmod 2\pi$. This shows that $x \in Z(A)$, a contradiction, concluding the proof. □

We discuss a few remarks to Jordan's Theorem.

(1) By Jordan's Theorem there are only finitely many simple subgroups of $\mathrm{GL}_n(\mathbb{C})$. Therefore, since $\mathrm{SL}_n(\mathbb{F}_p)$ is simple, it cannot be embedded into $\mathrm{GL}_n(\mathbb{C})$ for sufficiently large p.
(2) The above proof also applied to locally finite subgroups of $U_n(\mathbb{C})$, i.e. groups where every finite subset generates a finite subgroup.
(3) By a result of Blichfeldt [Bli17] from 1917, it can be shown that $J(n) \leq e^{O(\frac{n^2}{\log n})}$. This implies that finite subgroups of $U_n(\mathbb{C})$ are *thin*, i.e. their metric entropy, which can be calculated as $\log N(G, \frac{1}{10})$ with $N(G, \frac{1}{10})$ the covering number of G by balls of radius $\frac{1}{10}$, is $\ll \frac{n^2}{\log n}$. Therefore the metric entropy of finite subgroups of $U_n(\mathbb{C})$ is much smaller than the metric entropy of $U_n(\mathbb{C})$, which is n^2.
(4) Jordan's Theorem is false for characteristic $p > 0$. Indeed, $\mathrm{GL}_n(\mathbb{F}_p)$ has no normal abelian subgroup of bounded index. On the other hand, Larsen-Pink [LP11] gave a version of Jordan's Theorem for subgroups of $\mathrm{GL}_n(\overline{\mathbb{F}_p})$.
(5) Using the classification of finite simple groups, Collins [Col07] established that $J(n) = (n+1)!$ for $n > 71$. This bound is sharp by considering the action of the symmetric group $\mathrm{Sym}(n+1)$ on the hyperplane $\{v \in \mathbb{C}^{n+1} : \sum_{i=1}^{n+1} v_i = 0\}$.

1.2. **Some recollections on local fields.** In this subsection we recall some facts about local fields as they are necessary for proving Selberg's Lemma in the next subsection. For proofs of the discussed results we refer to [Cas86].

Definition 1.5. *Let k be a field with an absolute value, i.e. a map $|\cdot| : k \to \mathbb{R}_+$ such that $|0| = 0$, $|1| = 1$ and for all $x, y \in k$,*

$$|xy| = |x| \cdot |y| \quad \text{and} \quad |x+y| \leq |x| + |y|.$$

*Then k is a **local field** if the topology induced by $|\cdot|$ is locally compact.*

Let p be a prime and consider on $\mathbb{Q}$ the p-adic absolute value $|\cdot|_p$ defined for a reduced fraction $r = \frac{a}{b} \in \mathbb{Q}$ as

$$|r|_p = p^{v_p(b) - v_p(a)},$$

where $v_p(n)$ for $n \in \mathbb{Z}$ is the p-adic valuation, i.e. $n = p^{v_p(n)}m$ with $\gcd(p, m) = 1$. The local field of p-adic numbers $\mathbb{Q}_p$ are the metric completion of $\mathbb{Q}$ with respect to the p-adic absolute value. For the p-adic number a stronger form of the traingle inequality holds, namely the ultrametric inequality, i.e. for all $x, y \in \mathbb{Q}_p$

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}.$$

The p-adic integers are defined as $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. $\mathbb{Z}_p$ is a local ring as $p\mathbb{Z}_p$ is the unique maximal ideal and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. Denote by $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x|_p = 1\}$ the group of units. Then we have a short exact sequence

$$1 \longrightarrow 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{F}_p^\times \to 1,$$

where the third map is the reduction mod p. This short exact sequence splits, resulting in an isomorphism

$$\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times (\mathbb{Z}_p, +) \cong \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p, \cdot).$$

In addition, the roots of unity of $\mathbb{Q}_p$ are in $\mathbb{Z}_p^\times$ and are in bijection with $\mathbb{F}_p^\times$.

We recall Ostrowski's theorem.

Theorem 1.6. *(Ostrowski) Let k be a local field of characteristic zero. Then*

(1) either k is archimedean, i.e. $k = \mathbb{R}$ ot $k = \mathbb{C}$,
(2) or k is a p-adic local field, i.e. a finite extension of $\mathbb{Q}_p$.

For a general p-adic local field k the above discussed properties also hold. Indeed the ring of integers $\mathcal{O}_k = \{x \in k : |x| \leq 1\}$ has the unique maximal ideal $\mathfrak{m} = \{x \in k : |x| < 1\}$. The quotient $\mathcal{O}_k/\mathfrak{m}$ is a finite field isomorphic to $\mathbb{F}_q$, where $q = p^f$ for some $f \geq 1$. The number f is called the residual degree of k. Write $\mathcal{O}_k^\times = \{x \in k : |x| = 1\}$ and again consider the short exact sequence

$$1 \longrightarrow 1 + \mathfrak{m} \longrightarrow \mathcal{O}_k^\times \longrightarrow \mathcal{O}_k/\mathfrak{m} \longrightarrow 1$$

that splits and therefore

$$\mathcal{O}_k^\times \cong \mathbb{F}_q^\times \times (\mathcal{O}_k, +) \cong \mathbb{F}_q^\times \times (1 + \mathfrak{m}, \cdot) \tag{1.2}$$

There roots of unity in k are in $\mathcal{O}_k^\times$ and are in bijection with $\mathbb{F}_q^\times$.

We furthermore recall the following facts.

(1) Given $n \in \mathbb{N}$, there are only finitely many extensions of $\mathbb{Q}_p$ of degree n.
(2) There is a unique way to extent the absolute value on k to the algebraic closure $\overline{k}$.
(3) Hensel's Lemma: Let $f \in \mathcal{O}_k[X]$ and let $\overline{f}$ be the reduction of f modulo $\mathfrak{m}$. Then every root $x_0 \in \mathcal{O}_k/\mathfrak{m}$ of $\overline{f}$ with $\overline{f}'(x_0) \neq 0$ can be lifted to a root x of f in $\mathcal{O}_k$ such that $x = x_0 \mod \mathfrak{m}$.

1.3. **Selberg's Lemma.** We recall that a group is called torsion free if the only element of finite order is the identity. In this subsection we discuss Selberg's Lemma.

Theorem 1.7. *(Selberg's Lemma,* [Sel60]*) Every finitely generated subgroup of $\mathrm{GL}_n(K)$ over a field of characteristic zero has a torsion free subgroup of finite index.*

Our strategy of proof relies on the following proposition by Cassels.

Proposition 1.8. *(Cassels,* [Cas76]*) Let K be a finitely generated field extension of $\mathbb{Q}$ and let $\alpha_1, \ldots, \alpha_\ell \in K \backslash \{0\}$. Then there are infinitely many primes p such that K embeds into $\mathbb{Q}_p$ in such a way that $\alpha_i \in \mathbb{Z}_p^\times$.*

Proof. We leave the general case to [Cas76], yet show that if K is a number field it embeds into $\mathbb{Q}_p$ for infinitely many p. By the primitive element theorem there is $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. Upon multiplying α by a rational integer, we may assume that α is in the ring of integers $\mathcal{O}_K$. Let P be the minimal polynomial of α in $\mathbb{Z}$.

We claim that if $P \in \mathbb{Z}[X]$ is non-constant then the set

$$\{\text{primes } p : p \text{ divides } P(n) \text{ for some integer } n\}$$

is infinite. To see this notice that $|P(\mathbb{Z}) \cap [-N, N]| \gg N^\varepsilon$ for every $\varepsilon > \frac{1}{\deg(P)}$ as $P(n) \ll n^{\deg(P)}$. On the other hand, if only finitely many primes appear in the prime factorization of integers in a set $E \subset \mathbb{Z}$, then $|E \cap [-N, N]| \ll (\log(N))^{O(1)}$ as $p_1^{k_1} \cdots p_m^{k_m} \leq N$ implies $k_i \leq \log N$ for each i.

To conclude the proof, recall that the resultant (cf. [Lan12] Chapter IV) of two polynomials P and Q is a number that is a polynomial expression with integer

coefficients in the coefficients of P and Q and it vanishes if and only if P and Q are not relatively prime, i.e. have non-constant common divisor. Take any prime p as above satisfying $p > \mathrm{res}(P, P')$. Then there is $n \in \mathbb{Z}$ such that p divides $P(n)$. Therefore P has a root in $\mathbb{F}_p$. Yet as $p > \mathrm{res}(P, P')$ and P is a minimal polynomial, P and P' are relatively prime also in the reduction mod p. So P' does not have a common root with P in $\mathbb{F}_p$ and therefore P has a root, which is simple in $\mathbb{F}_p$. By Hensel's lemma, P therefore has a root in $\mathbb{Z}_p$ and thus K embeds into $\mathbb{Q}_p$. □

Denote

$$\mathrm{GL}_n(\mathbb{Z}_p) = \{g \in M_n(\mathbb{Z}_p) \,:\, \det(g) \in \mathbb{Z}_p^\times\}.$$

Then we have the following consequence of the above proposition.

Corollary 1.9. *Let K be a field of characteristic zero and let Γ be a finitely generated subgroup of $\mathrm{GL}_n(K)$. Then there are infinitely many primes p such that Γ embeds into $\mathrm{GL}_n(\mathbb{Z}_p)$.*

Proof. Assume $\Gamma = \langle s_1^{\pm 1}, \ldots, s_m^{\pm 1}\rangle$ and let K be the field generated by the matrix entries of $s_1^{\pm 1}, \ldots, s_m^{\pm 1}$. We then apply Proposition 1.8 to K and the α_i being the non-zero coefficients of $s_1^{\pm 1}, \ldots, s_m^{\pm 1}$ together with $\det(s_1^{\pm 1}), \ldots, \det(s_m^{\pm 1})$, showing the claim. □

By Corollary 1.9 it suffices to show that $\mathrm{GL}_n(\mathbb{Z}_p)$ has a finite index torsion free subgroup. To do so consider for $m \geq 1$ the maps

$$\varphi_m : \mathrm{GL}_n(\mathbb{Z}_p) \to \mathrm{GL}_n(\mathbb{Z}_p/p^m\mathbb{Z}_p) \cong \mathrm{GL}_n(\mathbb{Z}/p^m\mathbb{Z}). \tag{1.3}$$

To conclude the proof of Selberg's Lemma, we show that $\ker(\varphi_1)$ is torsion free for $p > 2$. Indeed, we show the stronger property that $\ker(\varphi_1)$ is net, as defined below.

Definition 1.10. *Let k be an algebraically closed field and let $g \in \mathrm{GL}_n(k)$. Denote by $A(g)$ the multiplicative subgroup of $k^\times$ generated by the eigenvalues of g. We say that g is **net** if*

$$A(g) \cap \{\textit{roots of unity of } k\} = \{1\}.$$

*A subgroup Γ of $\mathrm{GL}_n(k)$ is called **net** if every $g \in \Gamma$ is net.*

As $A(g)^n \subset A(g^n)$, it therefore follows that a net subgroup is torsion free. Thus Selberg's Lemma, and indeed the stronger result that the finite index subgroup can be taken to be net, follows by establishing the next lemma, which is due to Raghunathan [Rag72].

Lemma 1.11. $\ker(\varphi_1)$ *is net for $p > 2$ and therefore torsion free.*

Proof. Let $g \in \ker(\varphi_1)$ with eigenvalues $\lambda_1(g), \ldots, \lambda_\ell(g)$ in $\overline{\mathbb{Q}_p}$. Denote by k the splitting field of the characteristic polynomial $\det(X - g) \in \mathbb{Q}_p[X]$. Then k is a local field and $A(g) \subset k^\times$. Moreover, since $GL_n(\mathbb{Z}_p)$ is compact it must hold that $|\lambda_i(g)| = 1$ for all $1 \leq i \leq \ell$ and therefore $A(g) \subset \mathcal{O}_k^\times$.

Let $\mathfrak{m}$ be the maximal ideal of k. Then by (1.2), $\mathcal{O}_k^\times \cong \mathbb{F}_q^\times \times (1 + \mathfrak{m})$ and the roots of unity of k are in correspondence with $\mathbb{F}_q^\times$. Therefore it suffices to show for $1 \leq i \leq \ell$, $\lambda_i(g) \in 1 + \mathfrak{m}$. Indeed to prove this let $x_i \in k^n$ be an eigenvector of $\lambda_i(g)$, i.e. $gx_i = \lambda_i(g)x_i$. As $g \in \ker(\varphi_1)$ we can write $g = 1 + ph$ for $h \in M_n(\mathbb{Z}_p)$ and hence $(\lambda_i(g) - 1)x_i = phx_i$. This it follows that $|\lambda_i - 1| < 1$ and hence $\lambda_i \in 1 + \mathfrak{m}$. □

1.4. **Malcev's Theorem and Schur's Theorem.** We next give two consequences of the previously established results.

Corollary 1.12. *(Malcev) Let K be a field of characteristic zero and let Γ be a finitely generated subgroup of $\mathrm{GL}_n(K)$. Then Γ is residually finite, i.e. for every $\gamma \in \Gamma \backslash \{0\}$ there is a finite group G and a group homomorphism $\pi : \Gamma \to G$ such that $\pi(\gamma) \neq 1$.*

Proof. By Corollary 1.9, it suffices to show that $\mathrm{GL}_n(\mathbb{Z}_p)$ is residually finite. To see this, we note that

$$\bigcap_{m \geq 1} \ker \varphi_m = \{1\}.$$

Indeed, if $g \equiv I_n \mod p^m$ then $g = I_n \in \mathrm{GL}_n(\mathbb{Z}_p)$ as $|g_{ij} - \delta_{ij}| < |p^m| \to 0$ as $m \to \infty$. □

A group is called torsion if every element has finite order.

Theorem 1.13. *(Schur) A torsion subgroup Γ of $\mathrm{GL}_n(\mathbb{C})$ is*

(1) locally finite, i.e. every finite subset generates a finite group,
(2) can be conjugated into $U_n(\mathbb{C})$ and
(3) has an abelian normal subgroup of index at most $J(n)$.

Proof. (1) follows from Selberg's Lemma. We leave (2) as an exercise to the reader. One reduces to the case when Γ is irreducible and then exploits that the space of Γ-invariant inner products on $\mathbb{C}$ is one-dimensional. The details are left as an exercise to the reader. Using (1) and (2), (3) follows as the proof of Jordan's Theorem. □

1.5. **Exercises.**

1.5.1. Let p be a prime. A group is called a p-group is every element has order p^m for some $m \geq 1$. Furthermore a group G is called pro-p if it is profinite and for every open normal subgroup $N < G$ the quotient show G/N is a p-group. Recall the maps φ_m defined in (1.3). Then $\ker(\varphi_1)$ is a pro-p group.

1.5.2. Complete the proof of Theorem 1.13.

1.5.3. Classification of finite subgroups of $\mathrm{SO}_3(\mathbb{R})$:

a) Let $\mathbb{S}^2$ be the unit sphere in $\mathbb{R}^3$. Then every non-identity element in $\mathrm{SO}_3(\mathbb{R})$ has exactly two fixed points and the fixed points are antipodal.

b) Let G be a finite subgroup of $\mathrm{SO}_3(\mathbb{R})$ and denote by P the set of fixed points on $\mathbb{S}^2$ of non-identity elements in G. Then

$$|G| - 1 = \frac{1}{2} \sum_{p \in P} (\mathrm{Stab}_G(p) - 1).$$

c) Let $a_1, a_2, \ldots, a_r$ be the sizes of the stabilizers of distinct orbits of the $\mathrm{SO}_3(\mathbb{R})$ action on $\mathbb{S}^2$. Then deduce from b) and the orbit stabilizer theorem that

$$2 - \frac{2}{|G|} = \sum_{i=1}^{r} \left(1 - \frac{1}{a_i}\right).$$

d) Use c) to classify all conjugacy classes of finite subgroups of $\mathrm{SO}_3(\mathbb{R})$. The resulting conjugacy classes are given in table 1. All of the finite subgroups arise as symmetry groups of regular geometric objects.

Group	Order	Symmetry Object
Cyclic Group C_n	n	oriented regular polygon
Dihedral Group D_n	$2n$	regular polygon
A_4	12	tetrahedron
S_5	24	cube or octahedron
A_5	60	dodecahedron or icosahedron

TABLE 1. Classification of Finite Subgroups of $\mathrm{SO}_3(\mathbb{R})$

As A_5 is simple, it follows that $J(2) \geq 60$ and it turns out that this bound is sharp (c.f. [Rob]).

1.5.4. Blichfeldt's bound for Jordan's theorem:

a) A finite subgroup G of $\mathrm{GL}_n(\mathbb{C})$ is said to be *primitive* if there is no non-trivial direct sum decomposition of $\mathbb{C}^n = V_1 \oplus \ldots \oplus V_d$ such that the finite set of subspaces is invariant under G (in particular for a finite group G - as it is completely reducible - primitive implies irreducible). Show that an abelian normal subgroup of a finite primitive group is central. In particular the conclusion of the main lemma in the proof of Jordan's theorem can be strengthened when G is assumed to be primitive as $B_G(\frac{1}{2})$ is then contained in the center of G.

b) If G is finite and primitive, and A is a maximal abelian subgroup of G, then the center $Z(G)$ has index at most 7^n in A. Hint: use a similar metric covering argument as in the proof of Jordan's theorem.

c) If $G \leq \mathrm{GL}_n(\mathbb{C})$ is a finite p-group (i.e. $|G|$ is a power of a prime p), then G is monomial, i.e. $\mathbb{C}^n$ has a decomposition as above with each V_i of dimension 1 and the V_i are permuted by G. Hint: recall that every p-group has a non-trivial center and show that, if non-abelian, it also has a normal abelian subgroup not contained in the center.

d) If $G \leq \mathrm{GL}_n(\mathbb{C})$ is a finite p-group, then it contains an abelian subgroup whose index divides $n!$

e) Using character theory, Blichfeldt proved that every subgroup G of $\mathrm{GL}_n(\mathbb{C})$ of order $|G| = ab$ with b not divisible by any prime $p \leq n+2$ contains an abelian subgroup of order b (cf. Chapter 14 of [Isa76], [Fei64]). Use this together with b) and d) above to prove Blichfeldt's bound: If G is a primitive finite subgroup of $\mathrm{GL}_n(\mathbb{C})$, then $[G : Z(G)] \leq e^{O(n^2/\log n)}$.

f) Deduce that $J(n) \leq e^{O(n^2/\log n)}$ in Jordan's theorem.

2. The Tits Alternative

We recall that a group Γ is called solvable if its derived series $D^{i+1}(\Gamma) = [D^i(\Gamma), D^i(\Gamma)]$ with $D^0(\Gamma) = \Gamma$ is eventually trivial, i.e. if there is $n \geq 0$ such that $D^n(\Gamma) = \{1\}$. Furthermore we say that Γ satisfies a given property virtually if Γ has a finite index subgroup satisfying the property, e.g. Γ is virtually solvable if it has a finite index solvable subgroup.

Theorem 2.1. *(Tits Alternative, 1972* [Tit72]*) A finitely generated subgroup of* $\mathrm{GL}_n(K)$ *over any field is either virtually solvable or contains a non-abelian free subgroup.*

We note the following:

(1) The alternative is exclusive as a group containing a non-abelian free group is never virtually solvable.
(2) The Tits alternative is false if one does not assume that the finitely generated group is contained in $\mathrm{GL}_n(K)$. Indeed, there are infinite torsion subgroups as for example constructed by Grigorchuk [Gri80]. A further example are Tarski-Monsters, i.e. infinite groups such that there exists a prime p with every non-identity element having order p (cf. [Ošš80]).
(3) As constructed by Juschenko-Monod [JM13] there are also infinite finitely generated simple groups without free subgroups (they are even amenable).

2.1. **Ping-Pong.** A crucial ingredient in the proof of the Tits alternative is the ping-pong argument, whose exposition we begin by discussing an example due to Felix Klein (cf. [Mas65]). Consider the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ endowed with the Riemannian metric $\frac{\sqrt{dx^2+dy^2}}{y}$. The group $\mathrm{PSL}_2(\mathbb{R})$ acts isometrically on $\mathbb{H}$ via Möbius transformations, namely for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{R})$ and $z \in \mathbb{H}$ we define

$$gz = \frac{az+b}{cz+d}.$$

For $t, \theta \in \mathbb{R}$ consider the matrices

$$g_t = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \quad \text{and} \quad r_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

as well as

$$h_{t,\theta} = r_\theta g_t r_\theta^{-1} = r_\theta g_t r_{-\theta}.$$

Lemma 2.2. *For every* $\theta \neq 0$ *there is* $t_\theta > 0$ *such that* g_t *and* $h_{t,\theta}$ *generate a free subgroup of* $\mathrm{PSL}_2(\mathbb{R})$ *if* $t > t_\theta$.

Proof. We encourage the reader to visualise the following argument geometrically. For $\varepsilon > 0$ denote

$$D_\varepsilon^- = \{z \in \mathbb{H} : |z| < \varepsilon\} \quad \text{and} \quad D_\varepsilon^+ = \{z \in \mathbb{H} : |z|^{-1} < \varepsilon\}.$$

Observe that $g_t(D_\varepsilon^-)^c \subset D_\varepsilon^+$ and $g_t^{-1}(D_\varepsilon^+)^c \subset D_\varepsilon^-$ provided that $e^{2t} > \varepsilon^{-2}$. For our chosen parameter θ, consider $E_\varepsilon^- = r_\theta D_\varepsilon^-$ and $E_\varepsilon^+ = r_\theta D_\varepsilon^+$. Then analogously, $h_t(E_\varepsilon^-)^c \subset E_\varepsilon^+$ and $h_t^{-1}(E_\varepsilon^+)^c \subset E_\varepsilon^-$. Choose $\varepsilon > 0$ small enough such that all of the sets $D_\varepsilon^-, D_\varepsilon^+, E_\varepsilon^-, E_\varepsilon^+$ are disjoint and $e^{2t} > \varepsilon^{-2}$ for the given choice of ε.

Consider the open set $U = D_\varepsilon^- \cup D_\varepsilon^+ \cup E_\varepsilon^- \cup E_\varepsilon^+$ and choose $x_0 \in \mathbb{H} \backslash U$. Then for every word w in two letters,

$$w(g_t, h_{t,\theta})x_0 \in U \quad \text{and therefore} \quad w(g_t, h_{t,\theta})x_0 \neq x_0.$$

Thus $w(g_t, h_{t,\theta}) \neq I_2$, showing the claim as w was arbitrary. □

Generalizing the example due to Klein, we arrive at the following proposition.

Proposition 2.3. *(Abstract Ping-Pong) Let Γ be a group acting on a set X and suppose that Γ is generated by subgroups $\Gamma_1, \dots, \Gamma_k$. Suppose further that for each i there is a subset $D_i \subset X$ such that the following properties are satisfied:*

(1) $D_i \cap D_j = \emptyset$ if $i \neq j$.
(2) There is $x_0 \in X$ such that $x_0 \notin \bigcup_{i=1}^k D_i$.
(3) If $\gamma \in \Gamma_i \backslash \{1\}$ then $\gamma x_0 \in D_i$ and $\gamma D_j \subset D_j$ if $j \neq i$.

Then $\Gamma = \Gamma_1 * \ldots * \Gamma_k$ is the free product of $\Gamma_1, \dots, \Gamma_k$.

Proof. Let $x_0 \in X$ such that $x_0 \notin \bigcup_{i=1}^k D_i$. Given a non-empty word w in k letters it holds that $w(\gamma_1, \dots, \gamma_k)x_0 \in \bigcup_{i=1}^k D_i$ for any $\gamma_1, \dots, \gamma_k$ with $\gamma_i \in \Gamma_i \backslash \{1\}$, implying that $w(\gamma_1, \dots, \gamma_k)$ is not the identity. □

To give a further example, we leave as an exercise to the reader to show that for $t \in \mathbb{R}$ with $|t| \geq 2$ the matrices

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \tag{2.1}$$

generate a free group. Furthermore for any $t \in \mathbb{R}$ that is transcendental, the matrices (2.1) generate a free group as the entries of any word evaluated at these matrices are polynomial in t. On the other hand, $\mathrm{SL}_2(\mathbb{Z}) = \langle (\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)) \rangle$ is not free, yet virtually free. It is a well-known open problem, called the Lyndon-Ullman problem [LU69] (see also [Gil08],[KK22]), to show that the matrices (2.1) do not generate a free group for any $t \in \mathbb{Q} \cap (-2, 2)$.

Recall the matrix groups

$$\mathrm{SO}_n(\mathbb{R}) = \{g \in M_n(\mathbb{R}) \,:\, gg^T = g^T g = \mathrm{Id}_n \text{ and } \det(g) = 1\}$$

and

$$\mathrm{SU}_n(\mathbb{C}) = \{g \in \mathrm{U}_n(\mathbb{C}) \,:\, \det(g) = 1\}.$$

We prove that $\mathrm{SO}_3(\mathbb{R})$ also contains a free group, a result due to Hausdorff. Indeed, we again consider the matrices g_t and $h_{t,\theta}$ from Lemma 2.2, yet with also allowing complex values t. We fix a value of θ such that r_θ has algebraic entries, for example $\theta = 2\pi/3$ with

$$r_\theta = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}.$$

Since we know that g_t and $h_{t,\theta}$ generate a free subgroup of $\mathrm{SL}_2(\mathbb{R})$ for at least some (real) value of t by the above construction, it follows that it also generates a free subgroup for all values of t (possibly complex) for which e^t is transcendental. Therefore we choose $t = i\varphi$ with $\varphi \in \mathbb{R}$ such that e^t is transcendental. Then g_t and $h_{t,\theta}$ generate a free subgroup of $\mathrm{SU}_2(\mathbb{C})$. Since $\mathrm{SU}_2(\mathbb{C})$ is a double cover of $\mathrm{SO}_3(\mathbb{R})$, the existence of a free subgroup of $\mathrm{SO}_3(\mathbb{R})$ follows.

The existence of a free subgroup of $\mathrm{SO}_3(\mathbb{R})$ is a useful observation. Indeed, consider for a non-trivial word w in two letters the word variety

$$V_w = \{(x, y) \in \mathrm{SO}_3(\mathbb{R}) \times \mathrm{SO}_3(\mathbb{R}) \,:\, w(x, y) = \mathrm{Id}_3\}.$$

As $\mathrm{SO}_3(\mathbb{R})$ contains a free subgroup, V_w is a proper sub-variety and therefore is an analytic manifold of dimension strictly less than $\dim(\mathrm{SO}_3(\mathbb{R}) \times \mathrm{SO}_3(\mathbb{R}))$. Therefore

V_w has zero measure with respect to the Haar measure on $\mathrm{SO}_3(\mathbb{R}) \times \mathrm{SO}_3(\mathbb{R})$. As there are only countably many words, the same holds for $\bigcup_{w \neq 1} V_w$. Thus if we choose two elements at random with respect to the Haar measure, they generate a free group almost surely.

Another application is the Hausdorff-Banach-Tarski paradox (cf. [Wag85]). Indeed, a free subgroup of $\mathrm{SO}_3(\mathbb{R})$ can be used to give a paradoxical decomposition of $\mathbb{S}^2$. More precisely, one can write $\mathbb{S}^2 = A_1 \sqcup \ldots \sqcup A_{2m}$ (for some $m \geq 2$, one can even take $m = 2$) as a disjoint union of subsets such that there exists elements $\gamma_1, \ldots, \gamma_m \in \mathrm{SO}_3(\mathbb{R})$ satisfying

$$\gamma_1 A_1 \sqcup \ldots \sqcup \gamma_m A_m = \mathbb{S}^2 = \gamma_{m+1} A_{m+1} \sqcup \ldots \sqcup \gamma_{2m} A_{2m}.$$

The latter decomposition shows that there is no finitely additive rotation invariant measure on $\mathbb{S}^2$ defined on all subsets.

We finally discuss a further open problem. Consider the matrices

$$a = \begin{pmatrix} -t & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -t \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1-t & -t^{-1} & t^{-1} \\ 1-t^2 & -t^{-1} & 0 \\ 1 & -t^{-1} & 0 \end{pmatrix}.$$

It is unknown if there exists some t such that a and b generate a free subgroup. To motivate this open problem, consider the braid group B_4, which has the presentation

$$B_4 = \langle \sigma_1, \sigma_2, \sigma_3 \,:\, \sigma_1\sigma_3 = \sigma_3\sigma_1,\, \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2,\, \sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3 \rangle.$$

The Burau representation of B_4 is given for $t \in \mathbb{R}_{\neq 0}$ as

$$\rho(\sigma_1) = \begin{pmatrix} -t & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho(\sigma_2) = \begin{pmatrix} 1 & 0 & 0 \\ t & -t & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho(\sigma_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & t & -t \end{pmatrix}.$$

It is a well-known open problem to show that the Burau representation of B_4 is faithful for some t. It was shown by Joan Birman [Bir74] (see also [BB21]) that ρ is faithful if and only if a and b generate a free group, where $a = \rho(\sigma_1)\rho(\sigma_3)^{-1}$ and $b = \rho(\sigma_2)a\rho(\sigma_2)^{-1}$. Moreover, if the Burau representation of B_4 is not faithful, then the Jones polynomial does not detect unknots (c.f. [Big02], [Ito15]).

2.2. **The Zariski topology.** For proofs of the results stated in this section we refer to [Hum75]. Let K be a field. A set $V \subset K^n$ is called Zariski closed if $V = \{x \in K^n \,:\, P(x) = 0 \text{ for all } P \in \mathscr{F}\}$, where $\mathscr{F} \subset K[X_1, \ldots, X_n]$ is a family of polynomials. The closed sets define the Zariski topology on K^n, which has the property that polynomial maps $K^n \to K^m$ are continuous.

For a subset $X \subset K^n$ we define the Zariski closure $\overline{X}^Z$ as the intersection of all Zariski closed subsets of K^n containing X.

Note that the Zariski topology on K^n induces a topology on each subset X of K^n. In particular, for two subsets $X \subset Y \subset K^n$, X is Zariski dense in Y if every polynomial that vanishes on X vanishes on Y.

A subset $X \subset K^n$ is said to be irreducible if it is not a union of two proper subsets that are Zariski closed in X. We note that if X is irreducible and φ is a polynomial map, then $\varphi(X)$ is also irreducible. Using that $K[X_1, \ldots, X_n]$ is noetherian, we see that every subset of K^n has a finite number of maximal irreducible subsets whose union is the whole set.

We may view $\mathrm{GL}_n(K)$ as a Zariski open subset of $M_n(K) \cong K^{n^2}$ as the determiniant is a polynomial. Moreover, $\mathrm{GL}_n(K)$ can be viewed as a Zariski closed set of $M_{n+1}(K)$ via the embedding

$$A \in \mathrm{GL}_n(K) \mapsto \begin{pmatrix} A & 0 \\ 0 & \det(A)^{-1} \end{pmatrix},$$

whose image is a Zariski closed subset of $M_{n+1}(K)$, the block diagonal matrices $diag(A, x)$ with $x \det A = 1$.

If $\Gamma \subset \mathrm{GL}_n(K)$ is an arbitrary subgroup, then the Zariski closure $\overline{\Gamma}^Z$ is also a group as the equations ensuring that Γ is a group are polynomials. Equally, if Γ is abelian, nilpotent or solvable so is $\overline{\Gamma}^Z$.

Write $\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_k$ with Γ_i being irreducible. If $1 \in \Gamma_1$, then Γ_1 is a subgroup and each Γ_i is a coset of Γ_1. We then call Γ_1 the connected component (of the identity) of Γ and denote it as Γ°. Every subgroup of finite index of Γ has the same connected component of the identity as Γ.

We say that a subgroup $\Gamma \subset \mathrm{GL}_n(K)$ is strongly irreducible if it does not preserve a finite union of proper subspaces of K^n. We leave as an exercise to show that Γ is strongly irreducible if and only if Γ° is irreducible, i.e. there are no Γ°-invariant subspaces of K^n.

2.3. **Proof of Tits Alternative.** We only give a proof of the Tits alternative in characteristic zero and therefore all fields in this section are assumed to be of characteristic zero.

Definition 2.4. *Let k be a local field. An element $g \in M_n(k)$ is called **proximal** if it has a unique eigenvalue of maximal modulus. More precisely, there is an ordering of the eigenvalues $\lambda_1(g), \ldots, \lambda_n(g)$ in the algebraic closure of k, counted with multiplicity, satisfying*

$$|\lambda_1(g)| > |\lambda_2(g)| \geq \ldots \geq |\lambda_n(g)|.$$

Recall that the absolute value of k admits a unique extension to the algebraic closure. If $x \in k_1 \subset \overline{k}$ for k_1 a finite extension of k, then $|x| = |\mathrm{N}_{k_1 \,|\, k}(x)|^{\frac{1}{[k_1 : k]}}$. In particular, the absolute Galois group $\mathrm{Gal}(\overline{k} \,|\, k)$ acts by isometries on the algebraic closure $\overline{k}$ of the local field k and permutes the eigenvalues of any element $g \in M_n(k)$. Since k has characteristic zero, the fixed field of the absolute Galois group is k it self (cf. Lang [Lan12] Chapter V Proposition 6.11). Therefore if $g \in M_n(k)$ is proximal, the maximal eigenvalue $\lambda_1(g)$ is fixed by the absolute Galois group and hence to belongs to k. In turn, the up to scalar multiple unique eigenvector of g with eigenvalue $\lambda_1(g)$ is in k^n.

We note further that proximality is an open condition. Recall furthermore that $\pi \in M_n(k)$ is a rank one projection if $\pi^2 = \pi$ and $\dim(\mathrm{Im}(\pi)) = 1$ and that every rank one projection is proximal. Note that a rank one matrix $\pi \in M_n(k)$ is a projection if and only $\mathrm{Im}(\pi) \nsubseteq \ker(\pi)$.

Lemma 2.5. *An element $g \in M_n(k)$ is proximal if and only if there is a sequence $\alpha_n \in k^\times$ such that $\alpha_n g^n$ converges to a rank one projection.*

Proof. If g is proximal, then the claim follows by setting $\alpha_n = (\lambda_1(g))^{-n}$ and considering the Jordan normal form of g. For the converse direction, as proximality is an open condition, it follows that for n large enough $\alpha_n g^n$ is proximal, showing that g is proximal. □

Towards the proof of the Tits alternative we note that a proximal element $g \in M_n(k)$ has interesting contraction properties when acting on projective space $\mathbb{P}(k^n)$. Indeed denote by H_g the sum of the characteristic subspaces of g with eigenvalues λ_i for $2 \leq i \leq n$. Let $x_g^+ \in k^n$ be a non-zero eigenvector of g with eigenvalue $\lambda_1(g)$ and write $v_g^+ = [x_g^+] \in \mathbb{P}(k^n)$. Then for all $x \in \mathbb{P}(k^n) \backslash [H_g]$ it holds that $g^n x \to v_g^+$. Using these observations, we can apply the Ping-Pong proposition to deduce the following.

Lemma 2.6. *Let k be a local field and let $\Gamma \subset \mathrm{GL}_n(k)$ be a subgroup, $n \geq 2$. Assume that Γ is Zariski-connected and acts irreducibly on k^n and that there is an element $\gamma \in \Gamma$ such that γ and γ^{-1} are proximal. Then there exists $h \in \Gamma$ such that for n large enough γ^n and $h\gamma^n h^{-1}$ generate a free subgroup of $\mathrm{GL}_n(k)$.*

Proof. It suffices to find $h \in \Gamma$ such that $hv_\gamma^+ \notin H_\gamma \cup H_{\gamma^{-1}}$ and $hv_{\gamma^{-1}}^+ \notin H_\gamma \cup H_{\gamma^{-1}}$. Indeed notice that if $\gamma^\pm$ is proximal, then so is $h\gamma^\pm h^{-1}$ and we have that $v_{h\gamma^\pm h^{-1}} = hv_{\gamma^\pm}$. To apply the ping-pong argument, we choose D_1 to be a neighborhood of $\{v_\gamma^+, v_{\gamma^{-1}}^+\}$ and D_2 one of $\{v_{h\gamma h^{-1}}^+, v_{h\gamma^{-1}h^{-1}}^+\}$, where we choose the neighborhoods to be sufficiently small such that they are disjoint and don't cover $\mathbb{P}(k^n)$. Replacing γ by powers of itself, γ^n and $h\gamma^n h^{-1} = (h\gamma h^{-1})^n$ become increasingly contracting on $\mathbb{P}(k^n)$ and therefore Proposition 2.3 applies. We refer to [BG03] for a definition of a metric on $\mathbb{P}(k^n)$, allowing to make the last argument more precise.

It remains to show that there exists $h \in \Gamma$ such that $hv_\gamma^+ \notin H_\gamma \cup H_{\gamma^{-1}}$ and $hv_{\gamma^{-1}}^+ \notin H_\gamma \cup H_{\gamma^{-1}}$. Indeed consider the Zariski-closed subspaces $X_1, \dots, X_4$ given by $\{g \in \mathrm{GL}_n(k) : gv_{\gamma^{\pm 1}}^+ \subset H_{\gamma^{\pm 1}}\}$. Assume for a contradiction that there is no element $h \in \Gamma$ as above. Then $\Gamma \subset X_1 \cup X_2 \cup X_3 \cup X_4$. Since Γ is Zariski connected, it holds that $\Gamma \subset X_i$ for some i. This is impossible however. For example if $\Gamma v_\gamma^+ \subset H_{\gamma^{-1}} \subsetneq k^n$, then $\langle \Gamma v_\gamma^+ \rangle$ is a non-trivial Γ-invariant subspace, a contradiction to irreducibility. □

To complete the proof of the Tits alternative, we require to achieve the assumptions from Lemma 2.6. The next lemma simplifies the assumption from Lemma 2.6.

Lemma 2.7. *Let $\Gamma \subset \mathrm{GL}_n(k)$ be a Zariski-connected and irreducible subgroup and assume there exists a proximal element $g \in \Gamma$. Then there is $\gamma \in \Gamma$ such that γ and γ^{-1} are proximal.*

Proof. By Lemma 2.5, since g is proximal there is a sequence α_n such that $\alpha_n g^n$ converges to a rank one projection π. Furthermore denote by β_n the maximal modulus of the eigenvalues of g^{-n}. Then upon choosing a subsequence, we may assume that $\beta_n g^{-n}$ converges to the non-zero matrix $A \in M_n(k)$.

For two elements $h_1, h_2 \in \Gamma$ denote $\gamma_n = g^n h_1 g^{-n} h_2$ and observe that

$$\alpha_n \beta_n \gamma_n = \alpha_n g^n h_1 \beta_n g^{-n} h_2 \longrightarrow \pi h_1 A h_2$$

as $n \to \infty$ and similarly $\alpha_n \beta_n \gamma_n^{-1} \to h_2^{-1} \pi h_1^{-1} A$. To conclude the claim we just need to show that $\pi_1 = \pi h_1 A h_2$ and $\pi_2 = h_2^{-1} \pi h_1^{-1} A$ are rank one projections.

As π has rank one, the maps π_1 and π_2 have rank at most one and therefore it suffices to show that

$$\mathrm{Im}(\pi_i) \nsubseteq \ker(\pi_i)$$

for $i = 1, 2$. This amounts to proving that $h_1 A h_2 \mathrm{Im}(\pi) \not\subset \ker(\pi)$ and $h_1^{-1} A h_2^{-1} \mathrm{Im}(\pi) \not\subset \ker(\pi)$. Exploiting strong irreducibility of Γ as in the proof of Proposition 2.6, we

first find $h_2 \in \Gamma$ such that $h_2\mathrm{Im}(\pi) \not\subseteq \ker(A)$ and $h_2^{-1}\mathrm{Im}(\pi) \not\subseteq \ker(A)$ and then find a suitable h_1 similarly. □

Lemma 2.8. *(*[Tit72] *Lemma 4.1) Let K be a finitely generated field and let $\alpha \in K$ be an element that is not a root of unity. There there is a field embedding $K \hookrightarrow k$ into a local field k such that $|\alpha|_k > 1$.*

Proof. We give a proof in the case that K has characteristic zero. We may assume that $K = \mathbb{Q}(\alpha)$ as we can always extend a field embedding $\mathbb{Q}(\alpha) \hookrightarrow k$ to one of K in the algebraic closure $\overline{k}$. If $\alpha \in K$ is transcendental over $\mathbb{Q}$, then simply choose a transcendental element $\omega \in \mathbb{C}$ with $|\omega| > 1$ and extend the map $\alpha \to \omega$ to a field embedding $\mathbb{Q}(\alpha) \to \mathbb{C}$.

On the other hand, if $\alpha \in K$ is algebraic, consider the minimal polynomial of α

$$P(X) = a_n X^n + \ldots + a_1 X + a_0 = \prod_{i=1}^{n}(X - \alpha_i)$$

with relatively prime integer a_i's. Assume first that α is an algebraic integer, in other words that $a_n = 1$. Then by Kronecker's Theorem, since α is not a root of unity, one of the Galois conjugates satisfies $|\alpha_i| > 1$. Extending the map $\alpha \to \alpha_i$ to a field embedding $\mathbb{Q}(\alpha) \to \mathbb{C}$, the claim follows.

It remains to treat the case when α is not an algebraic integer. Choose a prime number p that divides a_n and consider a splitting field k of P over $\mathbb{Q}_p$ such that

$$P(X) = a_n \prod_{i=1}^{n}(X - \alpha_i)$$

with $\alpha_i \in k$. Assume for a contradiction that $|\alpha_i|_k \leq 1$ for all $1 \leq i \leq n$. It holds that $|a_n|_p < 1$ and therefore since the field is non-archimedean we conclude $|a_i|_k \leq |a_n|_k < 1$ for all $1 \leq i \leq n$ showing that p divides $a_0, \ldots, a_n$. This is a contradiction to the assumption that the a_i are relatively prime. Therefore it follows that $|\alpha_i|_k > 1$ for some $1 \leq i \leq n$ and $\mathbb{Q}(\alpha)$ embeds into $\mathbb{Q}_p(\alpha_i) \subset k$. □

Lemma 2.9. *(see also Chapter 17.5* [Hum75]*) Let K a field and $\Gamma \subset \mathrm{GL}_n(K)$ a subgroup all of whose elements are unipotent. Then Γ is conjugate to a subgroup of*

$$\left\{ \begin{pmatrix} 1 & * & \ldots & * \\ 0 & 1 & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \right\},$$

the subgroup of upper triangular matrices with ones on the diagonal.

Proof. We consider the subalgebra A of $M_n(K)$ generated by $\gamma - 1$ with $\gamma \in \Gamma$ and note that A is the $\mathbb{C}$-span of $\{\gamma - 1 : \gamma \in \Gamma\}$ since $(\gamma_1 - 1)(\gamma_2 - 1) = (\gamma_1\gamma_2 - 1) - (\gamma_1 - 1) - (\gamma_2 - 1)$ for any $\gamma_1, \gamma_2 \in \Gamma$. As γ is unipotent, by writing γ in Jordan normal form it follows that $\mathrm{tr}(\gamma - 1) = 0$ for all $\gamma \in \Gamma$ and therefore $\mathrm{tr}(a) = 0$ for all $a \in A$. The claim of the lemma is implied from Wedderburn's theorem that subalgebras of $M_n(K)$ consisting of matrices of trace zero are nilpotent and hence can be put in upper triangular form with zeros on the diagonal in some basis (see Section 2.4 below). For a similar treatment using Burnside's theorem we refer to section 17.5 of [Hum75]. □

We are now in a suitable position to conclude the proof of the Tits alternative. By Selberg's Lemma, up to passing to a finite index subgroup, we can assume that Γ is torsion free. Furthermore, since the connected component has finite index, one reduces to the case that Γ is Zariski connected.

To prove the Tits alternative, we proceed with assuming that Γ is not virtually solvable. Combining Lemma 2.7 together with Lemma 2.6, it remains to check that we can achieve that Γ is irreducible and contains a proximal element. Observe that not all elements from $[\Gamma, \Gamma]$ are unipotent. Indeed if this was the case, by Lemma 2.9 it would follow that $[\Gamma, \Gamma]$ itself is unipotent and hence solvable and so Γ would be solvable too.

Since Γ is torsion free, we can choose an element $\gamma \in [\Gamma, \Gamma]$ that has an eigenvalue that is not a root of unity. Therefore by the Lemma 2.8, there is a local field k and an embedding $K \hookrightarrow k$ such that $|\alpha|_k > 1$. As we have chosen $\gamma \in [\Gamma, \Gamma]$, $\det(\gamma) = 1$ and therefore the product of the eigenvalues of γ is 1. This shows that there is $1 \leq \ell \leq n-1$ such that

$$|\lambda_1(\gamma)| = \ldots = |\lambda_\ell(\gamma)| > |\lambda_{k+1}(\gamma)| \geq \ldots \geq |\lambda_n(\gamma)|.$$

The final trick is to use the wedge product $\Lambda^\ell k^n$ of k^n, inducing a representation

$$\Lambda^\ell : \mathrm{GL}(k^n) \to \mathrm{GL}(\Lambda^\ell k^n).$$

Since the eigenvalues of $\Lambda^\ell \gamma$ are products of ℓ distinct eigenvalues of γ it follows that $\Lambda^\ell \gamma$ is proximal.

While Γ doesn't necessarily act irreducibly on $\Lambda^\ell k^n$, we can pass to a suitable quotient. Indeed choose a filtration $\Lambda^\ell k^n = W_0 \supsetneq W_1 \supsetneq W_2 \ldots$ of Γ-invariant subspaces such that W_i/W_{i+1} are irreducible. We note that as $\gamma \in [\Gamma, \Gamma]$ it follows that $\det(\Lambda^\ell \gamma|_{W_i/W_{i+1}}) = 1$. Finally pick i_0 such that $\lambda_1(\Lambda^\ell \gamma)$ appears in W_{i_0}/W_{i_0+1}. Then since $\det(\Lambda^\ell \gamma|_{W_{i_0}/W_{i_0+1}}) = 1$ it follows that $\dim(W_{i_0}/W_{i_0+1}) \geq 2$ and we may apply Lemma 2.6. This concludes the proof.

2.4. **Subalgebras of $M_n(K)$.** We include here some basic recollections on the structure of (associative) subalgebras of $M_n(K)$, which we needed in the proof of Lemma 2.9 and also yield Burnside's theorem. This material can be found for instance in Wedderburn's Lectures on Matrices [Wed34], or in more recent textbooks such as Lang ([Lan12], Chapter XVII).

If $A \leq M_n(K)$ is a K-subalgebra, then it is easy to check that it contains a largest nilpotent bilateral ideal N (nilpotent means that $N^k = 0$ for some integer $k \geq 1$ and bilateral ideal means that aN and Na lie in N for each $a \in A$). It is called the radical (or Jacobson radical) of A. Wedderburn showed that A can be decomposed as a direct sum:

$$A = S + N$$

where N is the radical of A, and S is a semi-simple subalgebra. Wedderburn moreover showed that S is a direct sum of simple (i.e. with no non-trivial ideal) subalgebras, and that each simple K-algebra is of the form $M_d(D_K)$ where D_K is a division algebra (i.e. every non-zero element is invertible). If K is algebraically closed then K is the only division K-algebra.

It is straightforward to check that every nilpotent subalgebra N of $M_n(K)$ can be put in upper triangular form with zeroes on the diagonal in some basis of K^n. Indeed one shows that there is a non-zero subspace killed by all elements of N and then inducts on the dimension. Similarly, we get that if K is algebraically closed,

every subalgebra $A \leq M_n(K)$ can be put in block upper-triangular form, where each non-zero diagonal block is a full matrix algebra $M_d(K)$ for $d \leq n$. From this the following is immediate:

Lemma 2.10. *(Wedderburn) Let K be a field and $A \leq M_n(K)$ a K-subalgebra spanned by elements with zero trace, then A is nilpotent and can be conjugated into upper triangular form with zeroes on the diagonal in some K-basis of K^n.*

Similarly:

Lemma 2.11. *If K is algebraically closed and $A \leq M_n(K)$ is a K-subalgebra preserving no non-trivial invariant subspace of K^n, then $A = M_n(K)$.*

Corollary 2.12. *(Burnside) If $G \leq \mathrm{GL}_n(\mathbb{C})$ is a subgroup acting irreducibly on $\mathbb{C}^n$, then the $\mathbb{C}$-span of all $g \in G$ is all of $M_n(\mathbb{C})$.*

Indeed the $\mathbb{C}$-span is an irreducible subalgebra.

2.5. **Exercises.**

2.5.1. For $t \in \mathbb{R}$ with $|t| \geq 2$ show that

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

generate a free group. Hint: Use $\mathbb{R}^2$ as a ping-pong table.

2.5.2. Consider the Lie algebra

$$\mathfrak{su}(2) = \{x \in M_2(\mathbb{C}) \,:\, x^* = -x \text{ and } \mathrm{tr}(x) = 0\}.$$

Show that $\mathrm{SU}_2(\mathbb{C})$ is a double cover of $\mathrm{SO}_3(\mathbb{R})$ by checking that the sequence

$$1 \longrightarrow \{\pm I_2\} \longrightarrow \mathrm{SU}_2(\mathbb{C}) \longrightarrow \mathrm{SO}_3(\mathbb{R}) \longrightarrow 1$$

is exact, where the map from $\mathrm{SU}_2(\mathbb{C}) \to \mathrm{SO}_3(\mathbb{R})$ is given as

$$g \mapsto (x \in \mathfrak{su}(2) \mapsto gxg^{-1} \in \mathfrak{su}(2)).$$

Hint: Note that $\mathfrak{su}(2) \cong \mathbb{R}^3$ and find a suitable inner product on $\mathfrak{su}(2)$.

2.5.3. Show that $\Gamma \subset \mathrm{GL}_n(K)$ is strongly irreducible if and only if Γ° is irreducible.

2.5.4. $\mathrm{SO}_3(\mathbb{R})$ contains a copy of $\mathrm{PSL}_2(\mathbb{Z})$:

a) Show that $\mathrm{PSL}_2(\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z})$ by considering the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and checking that $\mathrm{PSL}_2(\mathbb{Z}) = \langle S, T \,:\, S^2 = 1, (ST)^3 = 1 \rangle$.

b) We consider two rotations around the origin in $\mathbb{R}^2$, one with angle $2\pi/3$, call it a, and another with angle π, called b. Let θ be the angle between their axes. If $\theta = \pi/4$, then $\langle a, b \rangle$ is the free product $(\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z})$. Deduce that the same holds if $\cos(\theta)$ is transcendental. Hint: Show that in a suitable basis $a^{\pm 1}b = \frac{1}{2}c_\pm$ for $c_\pm \in M_3(\mathbb{Z}[\sqrt{3}])$ and that modulo 2 it holds that $c_+ = c_- = c_\pm^2$ is non-zero.

2.5.5. If $G = \langle a, b \,|\, a^3 = b^2 = 1 \rangle$, then *babab* and *ababa* generate a free subgroup.

2.5.6. Show that a discrete and torsion free subgroup Γ of $\mathrm{SL}_2(\mathbb{R})$ which is not cocompact is free. Hint: View Γ as the fundamental group of a surface $\mathbb{H}/\Gamma$ and show that the fundamental group of a connected orientable surface is either a surface group or a free group.

2.5.7. Show Kronecker's theorem: if $P = \prod(X - \alpha_i) \in \mathbb{Z}[X]$ is monic and all its roots are in the (closed) unit disc, then its roots are roots of unity. Hint: show that there are only finitely many such polyonomials of given degree and that each $P_n = \prod(X - \alpha_i^n)$ is one of them.

2.5.8. Let $x \in \mathrm{SL}_2(\mathbb{R})$ be an element generating a discrete subgroup. Then there is a non-empty open subset U of $\mathrm{SL}_2(\mathbb{R})$ such that $\langle x, y\rangle$ is discrete for all $y \in U$.

3. Dense Subgroups

3.1. **Recollections from the theory of Lie groups and algebraic groups.** For proofs of the results on Lie groups we refer to [Kna02]. Recall that a Lie group is a group that is a smooth manifold such that the group multiplication and the inverse map are smooth. The prime example of Lie groups are closed subgroups of $\mathrm{GL}_n(\mathbb{R})$, that all form Lie groups by the Cartan-von Neumann Theorem.

Given a Lie group G, the Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$ of G is the tangent space at the identity element $1 \in G$. The Lie algebra is endowed with a Lie bracket $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, which is a bilinear map satisfying $[X, X] = 0$ for all $X \in \mathfrak{g}$ and the Jacobi identity

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0$$

for all $X, Y, Z \in \mathfrak{g}$. For example, if $G \leq \mathrm{GL}_n(\mathbb{R})$ is a closed subgroup and $X, Y \in \mathfrak{g} \subset M_n(\mathbb{R}) = \mathrm{Lie}(\mathrm{GL}_n(\mathbb{R})) = \mathfrak{gl}_n(\mathbb{R})$ it holds that $[X, Y] = XY - YX$.

The Lie algebra is connected to the Lie group by the exponential map $\exp : \mathfrak{g} \to G$ that sends $0 \in \mathfrak{g}$ to $1 \in G$ and for a small enough neighbourhood around the identity the exponential map is a homeomorphism onto its image. For $M \in \mathfrak{gl}_n(\mathbb{R})$ it holds that $\exp(M) = \sum_{k=0}^{\infty} \frac{M^n}{n!} \in \mathrm{GL}_n(\mathbb{R})$.

For $g \in G$ we consider the conjugation map $C_g : G \to G, h \mapsto ghg^{-1}$. The derivative at e of the is the adjoint map $\mathrm{Ad}_g = D_e C_g : \mathfrak{g} \to \mathfrak{g}$. The map $g \mapsto \mathrm{Ad}_g$ forms a representation $G \to \mathrm{GL}(\mathfrak{g})$. For $g \in \mathrm{GL}_n(\mathbb{R})$, it holds that $\mathrm{Ad}_g(X) = gXg^{-1}$ with $X \in \mathfrak{gl}_n(\mathbb{R})$. The derivative of the group homomorphism $Ad : G \to \mathrm{GL}(\mathfrak{g})$ is denoted ad_X and evaluates as $\mathrm{ad}_X(Y) = [X, Y]$ for all $X, Y \in \mathfrak{g}$. The map $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ is also referred to as the adjoint representation and is a Lie algebra representation. Therefore following diagram is commutative:

$$\begin{array}{ccc} G & \xrightarrow{\mathrm{Ad}} & \mathrm{GL}(\mathfrak{g}) \\ \uparrow{\scriptstyle \exp} & & \uparrow{\scriptstyle \exp} \\ \mathfrak{g} & \xrightarrow{\mathrm{ad}} & \mathfrak{gl}(\mathfrak{g}) \end{array}$$

Given a Lie algebra $\mathfrak{g}$, a subspace $\mathfrak{h} \subset \mathfrak{g}$ is called an ideal if $[\mathfrak{g}, \mathfrak{h}] \subset \mathfrak{h}$. A Lie algebra is called **simple** if it has no non-trivial ideal and **semisimple** if it is a direct sum of simple Lie algebras. Every real Lie algebra $\mathfrak{g}$ has a Levi decomposition, i.e. it can be written as $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{r}$ with $\mathfrak{s}$ being semisimple and $\mathfrak{r}$ the maximal solvable ideal in $\mathfrak{g}$.

Let $\mathfrak{g}$ be a complex semisimple Lie algebra. We choose a Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$, i.e. a maximal abelian subalgebra such that for every element $X \in \mathfrak{h}$ the linear map ad_X is diagonalizable. By the Jacobi identity, the collection of operators ad_X for $X \in \mathfrak{h}$ commute and therefore they are jointly diagonalizable.

So there exists a finite subset $\Sigma \subset \mathrm{Hom}(\mathfrak{h}, \mathbb{C})$ such that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Sigma} \mathfrak{g}_\alpha,$$

where $\mathfrak{g}_\alpha = \{Y \in \mathfrak{g} : [X, Y] = \alpha(X)Y \text{ for all } X \in \mathfrak{h}\}$. The linear forms Σ are called the **roots** and the above decomposition is called the **root space decomposition**. It can be shown that $\dim \mathfrak{g}_\alpha = 1$.

We may choose a subset of **positive** roots $\Sigma^+ \subset \Sigma$ such that for each $\alpha \in \Sigma$ it either holds that $\alpha \in \Sigma^+$ or $-\alpha \in \Sigma^+$ and for all $\alpha, \beta \in \Sigma^+$ we have that $\alpha + \beta \in \Sigma^+$ provided $\alpha + \beta \in \Sigma$. A root $\alpha \in \Sigma^+$ is called **simple** if it cannot be

written as a sum of roots in Σ^+. Denote by $\pi \subset \Sigma$ the set of simple roots. If $\alpha \in \pi$ and $\mathfrak{g}_\alpha = \langle e_\alpha \rangle_{\mathbb{C}}$, then $h_\alpha = [e_\alpha, e_{-\alpha}]$ is in $\mathfrak{h}$ and it holds that $\mathfrak{h} = \bigoplus_{\alpha \in \pi} \langle h_\alpha \rangle_{\mathbb{C}}$. Therefore $\dim \mathfrak{h} = |\pi|$, which is called the **rank** of $\mathfrak{g}$.

To give a concrete example, consider

$$\mathfrak{g} = \mathfrak{sl}_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \,:\, \mathrm{tr}(A) = 0\}$$

for $n \geq 2$. We choose the Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$ to be the subalgebra of diagonal matrices. Denote by E_{ij} the matrix that is 1 at the entry (i, j) and zero otherwise and by E_{ij}^* the induced dual map on $M_n(\mathbb{C})$. The roots are the maps $E_{ii}^* - E_{jj}^* \in \mathrm{Hom}(\mathfrak{h}, \mathbb{C})$ for $i \neq j$ and a collection of simple roots is $\pi = \{E_{ii}^* - E_{i+1,i+1}^* \,:\, 1 \leq i \leq n-1\}$. Then

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{i \neq j} \langle E_{ij} \rangle_{\mathbb{C}}$$

is the root space decomposition.

We furthermore discuss the relationship between Lie groups and algebraic groups. For the purposes of these notes, we consider an algebraic group to be a closed subgroup of $\mathrm{GL}_n(K)$ for some field K. References for the theory of algebraic groups are [Bor91], [Hum75] and [OV80].

To each complex semisimple Lie algebra $\mathfrak{g}$, there exists a simply connected complex Lie group G with Lie algebra $\mathfrak{g}$. As follows by the classification of complex semisimple Lie algebras, G can be endowed with the structure of an algebraic group and it has finite center Z. All Lie groups with Lie algebra $\mathfrak{g}$ are of the form G/Z_0 where $Z_0 \subset Z$. Given G/Z_0 we call G/Z the adjoint group. The groups G/Z_0 and G/Z are called isogenous.

Moreover we recall that every complex semisimple Lie group G is a product $G_1 \cdots G_k$ for the collection of non-trivial commuting simple subgroups. Moreover

$$G \cong G_1 \times \ldots \times G_k/Z$$

and the the groups G_i are called the simple factors of G.

We note that these results are wrong over $\mathbb{R}$ as the universal cover of $\mathrm{SL}_2(\mathbb{R})$ is a simply connected real Lie group that is not algebraic. A real form of G is an algebraic group H defined over $\mathbb{R}$ such that $H(\mathbb{C}) \cong G$.

3.2. **Kuranishi's results.**

Proposition 3.1. *(Kuranishi* [Kur49]*) Every real semisimple Lie group $\mathfrak{g}$ is generated by two elements. Moreover, the set $\{(A, B) \in \mathfrak{g} \times \mathfrak{g} \,:\, A, B$ generate $\mathfrak{g}\}$ is a non-empty Zariski open subset.*

Proof. We first assume that $\mathfrak{g}$ is a complex semisimple Lie algebra and recall the root space decomposition as introduced above. First choose $A \in \mathfrak{h}$ such that $\alpha(A) \neq \beta(A)$ for all roots $\alpha \neq \beta$. Such an element exists since the kernel of $\alpha - \beta$ is a hypersuface in $\mathfrak{g}$. Furthermore set $B = \sum_{\alpha \in \Sigma} e_\alpha$.

We claim that A, B generate $\mathfrak{g}$ as a Lie algebra. Indeed notice that $\mathrm{ad}_A^k(B) = \sum_{\alpha \in \Sigma} \alpha(A)^k B$ and consider the elements $\{\mathrm{ad}_A^k(B)\}_{0 \leq k \leq |\Sigma|-1}$. Then the latter set of elements spans $\bigoplus_{\alpha \in \Sigma} \mathfrak{g}_\alpha$ since the representation matrix of these elements with respect to the basis $\{e_\alpha\}_{\alpha \in \Sigma}$ is a Vandermonde matrix. Indeed, by the construction of A it follows that the latter matrix has non-zero determinant and therefore e_α is in the span of the Lie algebra generated by A and B. Since the matrices $h_\alpha = [e_\alpha, e_{-\alpha}]$ for $\alpha \in \pi$ generate $\mathfrak{h}$, the claim follows.

We proceed with showing that for a complex semisimple Lie algebra $\mathfrak{g}$ the set $\{(A,B) \in \mathfrak{g} \times \mathfrak{g} : A, B \text{ generate } \mathfrak{g}\}$ contains a Zariski open subset. Indeed, the latter set is the $\mathbb{C}$-span of all the possible brackets generated by A and B of length at most $\dim \mathfrak{g} + 1$. Therefore A and B generate $\mathfrak{g}$ if and only if a finite collection of products of matrices of A and B span $\mathfrak{g}$. This is a rank condition and results in polynomial conditions, where all of the polynomials are defined over $\mathbb{R}$.

Finally we notice that the real case follows from the complex one. Indeed, if $\mathfrak{g}$ is a real semisimple Lie algebra, then $\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes \mathbb{C}$ is a complex semisimple Lie algebra. Since the above polynomial conditions are over $\mathbb{R}$, the claim also follows for $\mathfrak{g}$ in $\mathfrak{g}_{\mathbb{C}}$. □

Proposition 3.2. *(Kuranishi* [Kur49]*) Let G be a connected semisimple Lie group. Then there is a neighborhood $\Omega \subset \mathfrak{g}$ of 0 in $\mathfrak{g}$ such that two elements $A, B \in \Omega$ generate $\mathfrak{g}$ as a Lie algebra if and only if the $\exp(A)$ and $\exp(B)$ generate a dense subgroup of G.*

Lemma 3.3. *(Zassenhauss) Let G be a connected Lie group. Then there is a neighborhood U of the identity such that every discrete subgroup generated from elements in U is nilpotent.*

Proof. Similarly to the commutator shrinking property (1.1), there exists a constant c_G such that for $x, y \in U$ for U a sufficiently small neighborhood of $1 \in G$,

$$d(1, xyx^{-1}y^{-1}) \leq c_G d(1,x) d(1,y), \tag{3.1}$$

where d is a left-invaraint metric on G. Let S be a set in U generating a discrete subgroup. Then by (3.1), commutators of elements in S will be closer and closer to the identity and therefore, since the group generated by S is discrete, sufficiently deep commutators are trivial. It follows that the group generated by S is nilpotent (see Exercise 3.5.9). □

Proof. (of Proposition 3.2) We choose $\Omega \subset \mathfrak{g}$ such that the exponential map is a homeomorphism and the image is a Zassenhauss neighborhood. Denote $a = \exp(A)$, $b = \exp(B)$ for $A, B \in \Omega$ and $\Gamma = \langle a, b \rangle$.

Assume first that A and B generate $\mathfrak{g}$. We show that Γ is not discrete. Indeed, if Γ was discrete, then Γ would be nilpotent by Lemma 3.3. Also if $z \in \Gamma$ is the closest non-trivial element to the identity, by the commutator shrinking property it would follow that z is in the center of Γ. Therefore $Z = \log(z)$ commutes with A and B and thus is a non-zero central element of $\mathfrak{g}$, a contradiction as $\mathfrak{g}$ has no center.

Since Γ is not discrete, the connected component of the closure of Γ is a Lie group of non-zero dimension. Denote by $\mathfrak{h} = \mathrm{Lie}(\overline{\Gamma}) \subset \mathfrak{g}$. It follows that $\mathfrak{h}$ is invariant under Ad_a and Ad_b and therefore also under $\mathrm{ad}_A = \log \mathrm{Ad}_a$ and $\mathrm{ad}_B = \log \mathrm{Ad}_b$. So $\mathfrak{h}$ is an ideal of $\mathfrak{g}$ and thus $H = \overline{\Gamma}^{\circ}$ is a normal subgroup. Upon replacing G by G/H we may induct on the dimension to conclude the claim.

For the other direction one proceeds along similar lines, establishing that $\mathfrak{h} = \langle A, B \rangle$ is a Lie ideal and then inducting on the dimension. □

Corollary 3.4. *Let G be a semisimple Lie group and $k \geq 2$. Then the condition that a k-tuple generates a dense subgroup is open.*

Proof. We give a proof in the case when $k = 2$ and leave the analogous general case to the reader. Near the identity, the claim follows by Proposition 3.2. More

precisely, there are proper subspaces $V_1, \dots, V_k$ of $\mathfrak{g} \times \mathfrak{g}$ such that any two elements $(a, b) \in \exp(\Omega) \times \exp(\Omega)$ generate a dense subgroup if and only if $(a, b) \notin \exp(\cup_i V_i \cap \Omega \times \Omega)$, where Ω is the neighborhood from Proposition 3.2.

Let now $a, b \in G$ be two words not necessarily close to the identity that generate a dense subgroup. Then there are two words w_1 and w_2 in a and b such that w_1 and w_2 are in Ω and generate a dense subgroup. Therefore, there are two neighborhoods U and V of w_1 and w_2 such that any two elements $w_1' \in U$ and $w_2' \in V$ generate a dense subgroup. Choosing then elements a' and b' close enough to a and b, the same words evaluated at a' and b' will still lie in U and V, therefore generating a dense subgroup and implying the claim. □

Corollary 3.5. *Let G be a semisimple Lie group and let Γ be a dense subgroup generated by n elements. Then for all neighborhoods U of the identity in G there are $t_1, \dots, t_{n+2} \in U \cap \Gamma$ such that $\Gamma = \langle t_1, \dots, t_{n+2} \rangle$.*

Proof. By Proposition 3.2, choosing U sufficiently small, there are $a, b \in U \cap \Gamma$ generating a dense subgroup of G. Assume that Γ is generated by $\langle s_1, \dots, s_n \rangle$. Then there are words in $w_1, \dots, w_n$ in a and b such that $s_i w_i \in U$. Therefore it follows that Γ is generated by the elements $\{s_1 w_1, \dots, s_n w_n, a, b\}$, implying the claim. □

Proposition 3.6. *Let G be a complex semisimple algebraic group. Then the set*

$$\{(a, b) \in G \times G : \langle a, b \rangle \text{ generate a Zariski-dense subgroup of } G\}$$

is a non-empty Zariski open set.

Proof. We give a proof in the case that $G \subset \mathrm{GL}_n(\mathbb{C})$ is simple. We claim that there are two finite dimensional irreducible representation (ρ_1, V_1) and (ρ_2, V_2) such that $\langle a, b \rangle$ is Zariski dense if and only if $\langle a, b \rangle$ acts irreducibly on V_1 and V_2. Assuming the claim, the proposition is a straightforward consequence as an action being irreducible is a Zariski open condition.

To show the claim, we will take (ρ_1, V_1) to be the representation $(\mathrm{Ad}, \mathfrak{g})$ and (ρ_2, V_2) to be an irreducible representation of dimension larger than $J(n)$, the constant from Jordan's theorem (Theorem 1.1). Such a representation exists as there are irreducible representation of arbitrarily high dimension [Hum75]. Notice that subrepresentations of the adjoint representation correspond to ideals in $\mathfrak{g}$ and therefore, since we assume $\mathfrak{g}$ to be simple, $(\mathrm{Ad}, \mathfrak{g})$ is also an irreducible representaion. Therefore it follows that if Γ is Zariski-dense, then Γ acts irreducibly on V_1 and V_2. For the other direction assume that Γ acts irreducibly on V_1 and V_2.

To prove the claim, write $\Gamma = \langle a, b \rangle$ let $H = \overline{\Gamma}^Z$ and assume for a contradiction that H is a proper subgroup of G. We show that Γ must be infinite. Indeed if Γ is finite, by Jordan's Theorem, there is an abelian normal subgroup A in Γ such that $[\Gamma : A] \leq J(n)$. Since A is abelian, there is $v \in V_2$ such that $Av \subset \langle v \rangle_{\mathbb{C}}$. Notice that the space $\langle \Gamma v \rangle_{\mathbb{C}} \subset V_2$ is Γ-invariant and has dimension $\leq J(n)$. Thus V_2 cannot be irreducible, a contradiction to the assumption.

As Γ is infinite, we consider the proper Lie algebra $\mathfrak{h} = \mathrm{Lie}(H)$ of non-zero dimension. The Lie algebra $\mathfrak{h}$ is fixed under $\mathrm{Ad}(a)$ and $\mathrm{Ad}(b)$ and therefore, as we assume that $\mathrm{Ad}(\Gamma)$ acts irreducibly on $\mathfrak{g}$, we arrive at a contradiction to $\mathfrak{h}$ being proper. Thus $G = H$ and the proof is concluded. □

3.3. **Examples of dense subgroups.** In this subsection we discuss examples of dense subgroups of Lie groups coming from arithmetic constructions. We first recall some material from the theory of arithmetic lattices.

Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\sigma_1, \dots, \sigma_{r_1}$ be the collection of real embeddings and $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ the complex ones. Then $[K : \mathbb{Q}] = r_1 + 2r_2$. We recall that by the map

$$\mathcal{O}_K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \qquad x \mapsto (\sigma_i(x))$$

embeds $\mathcal{O}_K$ as a lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. The theorem of Borel-Harish-Chandra generalizes this result to algebraic groups. A discrete subgroup Γ in a Lie group G is called a lattice if the associated homogeneous space G/Γ has finite volume. If $\Gamma \subset G_1 \times \ldots \times G_k$ is a lattice in a product of Lie groups, then Γ is called irreducible if the projection to each factor is dense.

Theorem 3.7. *(Borel-Harish-Chandra, cf.* [PR94] *Chapter IV) Let G be a semisimple complex alegbraic group defined over K and write $G(\mathcal{O}_K) = G \cap \mathrm{GL}_n(\mathcal{O}_K)$. Then the image of*

$$G(\mathcal{O}_K) \hookrightarrow \prod_{i=1}^{r_1} G^{\sigma_i}(\mathbb{R}) \times \prod_{i=r_1+1}^{r_2} G^{\sigma_i}(\mathbb{C})$$

is an irreducible lattice.

To give a concrete example, $\mathrm{SL}_2(\mathbb{Z}[\sqrt{2}])$ is an irreducible lattice in $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$. We note that Margulis' arithmeticity theorem [Mar84] establishes, under the assumption that G has higher rank, a converse to the Borel-Harish-Chandra Theorem namely stating that every irreducible lattice is arithmethic, i.e. arises from a number field as above. As irreducible lattices have dense image when projected to each factor, the Borel-Harish-Chandra theorem provides many examples of finitely generated dense subgroups of Lie groups.

A similar result also holds for p-adic Lie groups. Recall that a place is an equivalence class of absolute values on K. Denote by V^K the set of all places of K. A place is called finite if the induced completion on K is a non-archimedean local field. Finite places correspond to prime ideals in $\mathcal{O}_K$. The non-finite places are called infinite places and we recall that the completion of K with respect to an infinite place is either $\mathbb{R}$ or $\mathbb{C}$. Therefore the infinite places correspond to field embeddings into $\mathbb{C}$ and there are only finitely many of them. Likewise, for each prime number p the finite places above p correspond to embeddings ot K into $\mathbb{C}_p$ the completion of the algebraic closure of $\mathbb{Q}_p$. We denote the finite places as V_f^K and the infinite ones as V_∞^K.

Let $S \subset V^K$ be a finite set of places and define

$$\mathcal{O}_{K,S} = \{x \in K : |x|_v \leq 1 \text{ for all } v \in V^K \backslash S\}.$$

We assume in the following that S contains V_∞^K. Then similarly to before, $\mathcal{O}_{K,S}$ is a lattice in $\prod_{v \in S} K_v$, where K_v is the completion of K with respect to v. Moreover, generalizing the Borel-Harish-Chandra theorem (cf. [PR94] Chapter V), if G is a complex semisimple algebraic group, the image of the embedding

$$G(\mathcal{O}_{K,S}) \hookrightarrow \prod_{v \in S} G(K_v)$$

is a lattice. To have a concrete example in mind, $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) \hookrightarrow \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$ is a lattice.

We proceed with discussing the examples of dense subgroups due to Lubotzky-Phillips-Sarnak and Margulis. Indeed, consider the Hamiltionian quaternions

$$\mathbb{H}(\mathbb{R}) = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + k\mathbb{R},$$

where $i^2 = j^2 = k^2 = 1$ and $ij = k$ and recall that they form the only non-commutative division ring over $\mathbb{R}$. For an element $\alpha = a_0 + ia_1 = ja_2 + ka_3$ we denote $\overline{\alpha} = a_0 - ia_1 - ja_2 - ka_3$ and the norm of α is defined as

$$N(\alpha) = \alpha \cdot \overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

Every non-zero element $\alpha \in \mathbb{H}(\mathbb{R})$ has therefore non-zero norm and thus $\alpha^{-1} = N(\alpha)^{-1}\overline{\alpha}$. Write $\mathbb{H}(\mathbb{R})^\times = \mathbb{H}(\mathbb{R})\backslash\{0\}$ the group of invertible elements of $\mathbb{H}(\mathbb{R})$.

Notice that by mapping

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

yields an embedding of $\mathbb{R}$-algebras $\Phi : \mathbb{H}(\mathbb{R}) \to M_2(\mathbb{C})$ satisfying $N(\alpha) = \det(\Phi(\alpha))$. Therefore there is a short exact sequence of groups,

$$1 \longrightarrow \mathrm{SU}_2(\mathbb{C}) \longrightarrow \mathbb{H}(\mathbb{R})^\times \longrightarrow \mathbb{R}_{>0} \longrightarrow 1$$

where the third map is the norm and

$$\mathbb{H}(\mathbb{R})^\times / Z(\mathbb{H}(\mathbb{R})^\times) \cong \mathrm{SU}_2(\mathbb{C})/\{\pm 1\} \cong \mathrm{SO}_3(\mathbb{R}),$$

where $Z(\mathbb{H}(\mathbb{R})^\times) \simeq \mathbb{R}^\times$ is the center.

Let $p \equiv 1 \bmod 4$ be a prime number. Then a theorem of Jacobi asserts that the set

$$\{\alpha \in \mathbb{H}(\mathbb{Z}) \,:\, N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = p\}$$

contains $8(p+1)$ elements. Notice that $\mathbb{H}(\mathbb{Z})^\times = \{\pm 1, \pm i, \pm j, \pm k\}$. As $p \equiv 1 \bmod 4$, if $\alpha \in \mathbb{H}(\mathbb{Z})$ satisfies $N(\alpha) = p$, then exactly one of a_0, a_1, a_2 or a_3 is odd. So there is a unique unit $\varepsilon \in \mathbb{H}(\mathbb{Z})^\times$ such that $\varepsilon\alpha \equiv 1 \bmod 2$.

Finally consider the set

$$S = \{\alpha \in \mathbb{H}(\mathbb{Z}) \,:\, N(\alpha) = p \text{ and } \alpha \equiv 1 \bmod 2\}.$$

Then by the above, $|S| = p + 1$. We consider the image of $\langle S \rangle$ in $\mathrm{SO}_3(\mathbb{R}) = \mathbb{H}^\times(\mathbb{R})/Z(\mathbb{H}^\times(\mathbb{R}))$. We state the following theorem of Lubotzky-Phillips-Sarnak and refer to their papers for a definition of spectral gap.

Theorem 3.8. *(Lubotzky-Phillips-Sarnak,* [LPS86], [LPS87]*) The group $\langle S \rangle \subset \mathrm{SO}_3(\mathbb{R})$ is a free dense subgroup on $p+1$ generators and has optimal spectral gap.*

In rough terms, spectral gap measures how quickly products of elements of S become dense in $\mathrm{SO}_3(\mathbb{R})$. As the spectral gap is optimal, the elements of the power set S^n are therefore very well distributed.

As established in [LPS88], one can furthermore use the set S to construct a $(p+1)$-regular Cayley graph in $\mathrm{PGL}_2(\mathbb{F}_q)$, where $q \equiv 1 \bmod 4$ is further prime distinct of p. Then similarly to Theorem 3.8, the powers of S are *optimally* distributed in $\mathrm{PGL}_2(\mathbb{F}_q)$. Moreover, if $\left(\frac{q}{p}\right) = -1$ (i.e. q is not a square mod p) and the resulting graphs satisfy the best known girth estimates, namely as shown in [LPS88] together with [BB90],

$$\mathrm{girth}(\mathrm{Cay}(\mathrm{PGL}_2(\mathbb{F}_q), S)) = \left(\frac{4}{3} - o_q(1)\right) \log_p(|\mathrm{PGL}_2(\mathbb{F}_q)|),$$

where the girth of a graph is the length of its shortest cycle, and $o_q(1)$ tends to 0 as q tends to infinity.

3.4. **Dense and free subgroups of Lie groups.**

Theorem 3.9. *(Topological Tits Alternative* [BG03]*) Let G be a semisimple Lie group and $\Gamma \subset G$ a dense subgroup. Let $a_1, a_2 \in G$. Then for all neighborhoods of the identity U there are $b_1 \in a_1U \cap \Gamma$ and $b_2 \in a_2U \cap \Gamma$ such that $\langle b_1, b_2\rangle$ is a non-abelian free subgroup of Γ.*

In particular, every dense subgroup contains a dense and free subgroup.

We note that the second claim in Theorem 3.9 follows from the first as generating a dense subgroup is an open condition by Corollary 3.4.

We only give a sketch of the proof and refer to [BG03] for the full details. The main difficulty compared to the classical Tits alternative is that we are not able to take high powers of elements of G, since those may leave the neighborhoods a_iU.

Towards the proof, let k be a local field and we define a metric on $\mathbb{P}(k^n)$. For $x, y \in k^n$, if we express $x = \sum x_i e_i$ and $y = \sum_j x_j e_j$ for $e_1 \dots, e_n$ the standard basis, it follows by multi-linearity,

$$x \wedge y = \sum_{i<j} (x_i y_j - x_j y_i) \cdot (e_i \wedge e_j) \in \Lambda^2 k^n.$$

We furthermore endow k^n with the norm $||\cdot||$, which is the standard euclidean/hermitian norm if $k = \mathbb{R}$ or $\mathbb{C}$ of the supremum norm $||x|| = \max_i |x_i|$ if k is a non-archimedean local field. The metric on $\mathbb{P}(k^n)$ is then defined for $x, y \in k^n \backslash \{0\}$ as

$$d([x], [y]) = \frac{||x \wedge y||}{||x|| \cdot ||y||}. \tag{3.2}$$

We next recall the Cartan decomposition on $\mathrm{SL}_n(k)$, which is a decomposition of the form

$$\mathrm{SL}_n(k) = KA^+K,$$

for K a maximal compact subgroup and A^+ a suitable abelian subgroup. For example if $k = \mathbb{R}$ or $\mathbb{C}$, then $K = \mathrm{SO}_n(\mathbb{R})$ or $K = SU_n(\mathbb{C})$ respectively and

$$A^+ = \{\mathrm{diag}(a_1, \dots, a_n) \,:\, a_1 \geq \dots \geq a_n > 0 \text{ and } a_1 \cdots a_n = 1\}.$$

On the other hand if k is a non-archimedean local field, then $K = \mathrm{SL}_n(\mathcal{O}_k)$ for $\mathcal{O}_k = \{x \in k \,:\, |x| \leq 1\}$ and

$$A^+ = \{\mathrm{diag}(\pi^{k_1}, \dots, \pi^{k_n}) \,:\, k_1 \leq \dots \leq k_n \text{ and } k_1 + \dots + k_n = 0 \text{ where } k_i \in \mathbb{Z}\},$$

where π is a uniformizer of k, i.e. an element such that $\pi\mathcal{O}_k$ is the maximal ideal in $\mathcal{O}_k$. We leave as an exercise to check that the metric (3.2) is K-invariant, i.e. $d(k[x], k[y]) = d([x], [y])$ and satisfies the triangle inequality

$$d([x], [y]) \leq d([x], [z]) + d([z], [y])$$

for any x, y, z in $k^n \setminus \{0\}$.

Towards the proof of Theorem 3.9, we state a series of definitions and lemmas from [BG03] or [BG07] without proof.

Definition 3.10. *An element $g \in \mathrm{PGL}_n(k)$ is called ε-contracting if there is $v_g \in \mathbb{P}(k^n)$ and a projective hyperplane H_g (which can be viewed as an element from $\mathbb{P}((k^n)^*)$) such that for all $x \in \mathbb{P}(k^n)$ if $d(x, H_g) > \varepsilon$, then $d(gx, v_g) < \varepsilon$.*

Lemma 3.11. *Let $g = k_1 a k_2 \in KA^+K$. Then the following properties are equivalent for all $\varepsilon > 0$ and up to comparable constants c_i, $i = 1, ..., 4$ independent of g, ε:*

(i) g is $c_1\varepsilon$-contacting.
(ii) g is $c_2\varepsilon$-contracting with respect to $H_g = k_2^{-1}\langle e_2, \dots, e_n\rangle$ and $v_g = k_1 e_1$.
(iii) $|a_2/a_1| \leq c_3\varepsilon^2$.
(iv) g is $c_4\varepsilon$-Lipschitz on some open set of $\mathbb{P}(k^n)$.

The proof of the previous lemma reduces easily to the case when $g = a$ is diagonal and is left as an exercise.

Definition 3.12. *Suppose that $0 < \varepsilon < r^2 < 1$. Then an element $g \in \mathrm{SL}_n(k)$ is called (r, ε)-**proximal** if it is ε-contracting and $d(v_g, H_g) \geq r$.*

Lemma 3.13. *If $\varepsilon < r^2/4$, then a (r, ε)-proximal element is proximal.*

Definition 3.14. *Let $r > 0$ and $m \in \mathbb{N}$. A finite set $F \subset \mathrm{PGL}_n(k)$ is called (m, r)-**separating** if for all $v_1, \dots, v_m \in \mathbb{P}(k^n)$ and all projective hyperplanes $H_1, \dots, H_m$ there is $f \in F$ such that*

$$d(f^{\pm 1}v_i, H_j) > r$$

for all i, j.

Lemma 3.15. *If $\Gamma \subset \mathrm{GL}_n(k)$ is Zariski connected and irreducible, given any $m \in \mathbb{N}$, every Zariski dense subset of Γ contains a finite (m, r)-separating set for some $r > 0$.*

Proof. For $\gamma \in \Gamma$, consider the subset V_γ of $X := \mathbb{P}(k^n)^m \times \mathbb{P}((k^n)^*)$ made of points v_i and hyperplanes H_j such that either $\gamma v_i \in H_j$ or $\gamma^{-1}v_i \in H_j$ for at least one pair (v_i, H_j). It is clear that the V_γ form Zariski-closed subsets of X. The Zariski connectedness and irreducibility of Γ together force their intersection (as γ ranges in Γ) to be empty. By notherianity, some finite intersection of already empty. This gives F and hence r by compactness of X. □

Lemma 3.16. *(Lemma 2.1 of* [BG07]*) Let R be a finitely generated integral domain, and let $I \subset R$ be an infinite subset. Then there exists a local field k and an embedding $\iota : R \to k$ such that $\iota(I)$ is unbounded.*

We note that this Lemma 3.16 generalizes Lemma 2.8 by considering the case $I = \{\alpha^n : n \in \mathbb{Z}\}$.

Having stated these results, the remainder of the proof comprises the following steps. Note that we can assume without loss of generality that Γ is finitely generated.

(1) Let I be the set of matrix coefficients of all elements $\Gamma \cap U$. Then by the Lemma 3.16 there is a local field k such that I can be embedded into an unbounded collection of elements.
(2) Pass to a power representation $\Lambda^i k$ for some $i \geq 1$ such that $\Gamma \cap U$ has ε-contracting elements for all $\varepsilon > 0$. Then pick an irreducible diagonal block and consider the associated quotient.
(3) Find a separating set F.
(4) Prove and use the following variant of the Ping-Pong Lemma: There is $C > 0$ such that the following holds. Let F be a finite $(2m, r)$-separating set and

let γ be an ε-contracting element. Then there are $a_1, \dots, a_m \in \mathrm{PGL}_n(k)$ and $f_1, \dots, f_m, g_1, \dots, g_m \in F$ such that the elements

$$(g_i \gamma a_i f_i)_{1 \le i \le m}$$

are $(r/C, C\varepsilon)$-proximal and free generators of a free group of rank m.

3.5. **Exercises.**

3.5.1. Show that a free subgroup of $\mathrm{SO}_3(\mathbb{R})$ is topologically dense.

3.5.2. Construct a free subgroup and a finitely generated dense subgroup of $\mathrm{SO}_n(\mathbb{R})$ for $n \ge 3$.

3.5.3. Show that if you choose two random elements on $\mathrm{SO}_n(\mathbb{R})$ (with respect to the Haar measure), they almost surely generate a topologically dense free subgroup of $\mathrm{SO}_n(\mathbb{R})$ for $n \ge 3$.

3.5.4. Using that $\mathrm{SL}_n(\mathbb{R})$ is a simple Lie group, show that a Zariski dense subgroup of $\mathrm{SL}_n(\mathbb{R})$ is either discrete or topologically dense for $n \ge 2$.

3.5.5. If G is a compact Lie group, show that the set of torsion elements is dense.

3.5.6. Give concrete examples of finitely generated dense subgroups of $\mathrm{SL}_d(\mathbb{R})$.

3.5.7. Let $G = \mathrm{SL}_2(\mathbb{R})$ and consider for $R > 0$ the set $B_R = \{g \in G : ||g||_{\mathrm{op}} \le R\}$. In this exercise we want to understand the probability that two random elements of B_R generate a discrete and free subgroup. Denote

$$P(R) = \frac{\mathrm{vol}_{G \times G}(\{(g,h) \in B_R \times B_R : \langle g, h\rangle \text{ is discrete and free}\})}{\mathrm{vol}_G(B_R)^2}.$$

Notice that by Proposition 3.2, $P(R) = 0$ for small R. Show that

$$\lim_{R \to \infty} P(R) = 1.$$

3.5.8. Let G be a connected Lie group. Show that there is a constant $c_G > 0$ such that if $x, y \in G$ are close to 1, then

$$d(1, xyx^{-1}y^{-1}) \le c_G d(1,x) d(1,y),$$

where d is a left-invariant metric on G.

3.5.9. Let $\Gamma = \langle S \rangle$ and assume that all commutators of order k in S vanish, i.e. that

$$[s_1, [s_2, [\dots, s_k] \dots]] = 1$$

for all $s_1, \dots, s_k \in S$. Show that then Γ is nilpotent of class at most k. Hint: Use induction on k.

3.5.10. Show that in Corollary 3.5 it suffices to choose only $(n+1)$ many elements $t_1, \dots, t_{n+1} \in U \cap \Gamma$ generating Γ.

3.5.11. Let G be a semisimple Lie group. Then there exists a neighborhood U of the identity in G such that for all $a_1, a_2, a_3 \in U$ there are elements $b_i \in a_i U$ such that $\langle b_1, b_2, b_3 \rangle$ is not free.

3.5.12. Check that (3.2) indeed defines a K-invariant distance (with triangle inequality).

3.5.13. Prove Lemma 3.16 in the case when $R = \mathbb{Z}[X]$ and I is any sequence of polynomials with degree tending to infinity. For example

$$I = \left\{ P_n(X) = \prod_{|i| \leq n} (X - i) \in \mathbb{Z}[X], n \geq 1 \right\}.$$

4. Eigenvalues of subgroups of $\mathrm{SL}_n(\mathbb{R})$ and the Benoist limit cone

We start this section by a general observation how the real numbers differ from other local fields.

Proposition 4.1. *A compact subgroup of $\mathrm{GL}_n(\mathbb{R})$ is Zariski closed and therefore an algebraic subgroup.*

Proof. We show that every orbit of a G-action on $\mathbb{R}^m$ for some $m \geq 1$ is Zariski closed. This implies the lemma by considering the action of G on $\mathbb{R}^{n^2} \cong M_n(\mathbb{R})$ and by noting that $G \subset M_n(\mathbb{R})$ is the orbit of the identity matrix.

It suffices to show that for all $x, y \in \mathbb{R}^m$ with $y \notin Gx$ there exists a polynomial $f \in \mathbb{R}[X_1, \ldots, X_m]$ such that $f(Gx) = 0$ yet $f(y) \neq 0$. We use the Stone-Weierstrass theorem, which only holds over $\mathbb{R}$. Indeed since Gx and Gy are compact and disjoint, there is a continuous function φ on $\mathbb{R}^n$ such that $\varphi = 0$ on Gx and $\varphi = 1$ on Gy. Then by Stone-Weierstrass there is a polynomial $P \in \mathbb{R}[X_1, \ldots, X_n]$ such that

$$\sup_{z \in Gx \cup Gy} |\varphi(z) - P(z)| < 1/10.$$

To make the function G-invariant, consider the average $f(z) = \int P(gz)\, dg$ and note that f is still a polynomial. Then $|f(x)| < 1/10$ and $|1 - f(y)| < 1/10$ and therefore $f - f(x)$ vanishes on Gx, yet not on y. □

We note that Proposition 4.1 is wrong over $\mathbb{C}$ and $\mathbb{Q}_p$. Indeed $\mathbb{S}^1 \subset \mathbb{C}$ and $\mathbb{Z}_p \subset \mathbb{Q}_p$ as well as $\mathrm{SU}_n(\mathbb{C}) \subset \mathrm{SL}_n(\mathbb{C})$ and $\mathrm{SL}_n(\mathbb{Z}_p) \subset \mathrm{SL}_n(\mathbb{Q}_p)$ are all examples of compact subgroups that are Zariski dense in the additive group and in SL_n respectively.

4.1. Golsheid-Margulis and Abels-Margulis-Soifer.

Theorem 4.2. *(Golsheid-Margulis* [GdM89]*) Let $\Gamma < \mathrm{GL}_n(\mathbb{R})$ be a semigroup acting strongly irreducibly on $\mathbb{R}^n$. Then Γ contains a proximal element if any only if its Zariski closure $\overline{\Gamma}^Z$ contains one.*

We note again that these statements are wrong over $\mathbb{C}$ and $\mathbb{Q}_p$ by the same examples as before. To give a further example, we may view $G = \mathrm{SL}_n(\mathbb{C})$ as a real algebraic subgroup of $\mathrm{GL}_{2n}(\mathbb{R})$. While G acts irreducibly on $\mathbb{R}^{2n}$, it has no proximal elements as all the resulting eigenvalues come in pairs of same modulus.

Definition 4.3. *An element $g \in \mathrm{SL}_n(\mathbb{R})$ is called **regular** if all of its eigenvalues are distinct. It is moreover called $\mathbb{R}$-**regular** if the modulus of all eigenvalues are distinct.*

An element $g \in \mathrm{SL}_n(\mathbb{R})$ is regular whenever the centralizer $Z_{\mathrm{SL}_n(\mathbb{C})}(g)$ is a full diagonal subgroup. We note that the set of regular elements is Zariski open. Indeed if χ_g is the characteristic polynomial of g, then χ_g has distinct roots if and only if χ_g and its derivative χ_g' have no common factor. Recall that the resultant of two polynomials is a polynomial in their coefficients that is zero whenever the two polynomials have a common factor. Therefore g is regular if and only if $\mathrm{Res}(\chi_g, \chi_g') \neq 0$, which is a polynomial condition in g.

If $g \in \mathrm{SL}_n(\mathbb{R})$ is $\mathbb{R}$-regular, then all of its eigenvalues are real as the complex conjugate of an eigenvalue is again an eigenvalue. Moreover, $g \in \mathrm{SL}_n(\mathbb{R})$ is $\mathbb{R}$-regular if and only if $\Lambda^i g$ is proximal for all $1 \leq i \leq n$. We leave as an exercise

to show that being $\mathbb{R}$-regular is not a Zariski-open condition and the set of non-$\mathbb{R}$-regular elements is Zariski-dense.

Theorem 4.4. *(Abels-Margulis-Soifer* [AMS95]*) Let $\Gamma \subset \mathrm{SL}_n(\mathbb{R})$ be a Zariski-dense semigroup. Then Γ has a Zariski-dense set of $\mathbb{R}$-regular elements. Indeed, there is a finite set $F \subset \Gamma$ such that for all $g \in \mathrm{SL}_n(\mathbb{R})$ there is $f \in F$ such that gf is $\mathbb{R}$-regular.*

The first statement in Theorem 4.4 follows from the second as if the set of $\mathbb{R}$-regular elements V is not Zariski dense, then by the second statement $\Gamma \subset VF^{-1}$ and Γ would not be Zariski dense either. The first statement was initially obtained by a dynamical argument in Benoist-Labourie [BL93] and independently with an algebraic proof by Prasad [Pra94].

We mention the following result of Prasad-Rapinchuk [PR03] (see next section): Given a finitely-generated field $L \subset \mathbb{R}$, then there is a Zariski-dense subset of Γ consisting of $\mathbb{R}$-regular elements γ such that the characteristic polynomial χ_γ is irreducible over L and $\langle\gamma\rangle$, the group generated by γ, is Zariski dense in the centralizer $Z(\gamma)$.

Towards the proof of Theorem 4.2 we mention the following lemma.

Lemma 4.5. *Let K a field and $\Gamma \subset \mathrm{GL}_n(K)$ a semigroup. Then its Zariski closure $\overline{\Gamma}^Z$ is a group.*

Proof. The proof is left as an exercise to the reader. □

Lemma 4.6. *Suppose that $\Gamma \subset \mathrm{GL}_n(\mathbb{R})$ is a semigroup acting irreducibly and suppose there is a constant $M > 0$ such that $|\mathrm{tr}(\gamma)| \leq M$ for all $\gamma \in \Gamma$. Then $\overline{\Gamma}$ is compact.*

We remark that the assumption of irreducibility is necessary as the example $\{\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) : t \in \mathbb{R}\}$ shows.

Proof. By Burnside's theorem (Corollary 2.12) the algebra $\mathbb{C}[\Gamma] = M_n(\mathbb{C})$ as Γ is irreducible. Therefore there are $\gamma_1, \ldots, \gamma_{n^2}$ such that $M_n(\mathbb{C}) = \mathrm{span}_{\mathbb{C}}\gamma_1, \ldots, \gamma_{n^2}$. Furthermore we exploit that $(A, B) \mapsto \mathrm{tr}(AB)$ is a non-degenerate bilinear form on $M_n(\mathbb{C})$. So there is a basis $(E_i)_{1 \leq i \leq n^2}$ of $M_n(\mathbb{C})$ such that $\mathrm{tr}(E_i\gamma) = \delta_{ij}$ for all i, j. So for all $\gamma \in M_n(\mathbb{C})$ it holds that

$$\gamma = \sum_{i=1}^{n^2} \mathrm{tr}(\gamma\gamma_j)E_j.$$

Thus by the assumption, $|\mathrm{tr}(\gamma\gamma_i)| \leq M$ for all $\gamma \in \Gamma$ showing that Γ is bounded. Therefore $\overline{\Gamma}$ is compact. □

Proof. (of Theorem 4.2) Throughout this proof we denote $G = \overline{\Gamma}^Z$. We may assume that Γ is Zariski connected. Indeed, if Γ is not, we replace it by $\Gamma^\circ = \Gamma \cap G^\circ$, which is still irreducible since Γ is strongly irreducible and which contains a proximal element if and only Γ contains one as Γ° has finite index in Γ and an element is proximal if and only if any power of it is proximal.

We first assume that for all $\gamma \in \Gamma$, all eigenvalues of γ have the same modulus. Then consider $\Gamma_1 = \{g \in \mathbb{R}\Gamma : \det(g) = \pm 1\}$ and note that Γ_1 is an irreducible semigroup and that $|\mathrm{tr}(\gamma)| \leq n$ since $|\lambda_i(\gamma)| = 1$ for all i. Thus by Lemma 4.6 and Lemma 4.1, $\overline{\Gamma_1}$ is compact and hence algebraic, showing that all elements of $\overline{\Gamma_1}^Z$

have eigenvalues of modulus 1. The same follows for G since $G \subset \mathbb{R}\overline{\Gamma_1}^Z$. Therefore each element in G has all eigenvalues of same modulus. We note, putting Γ in block upper-triangular form with irreducible blocks, that the same conclusion holds even if Γ is not assumed irreducible.

For the general case, we note that similarly to Lemma 2.5, Γ contains a proximal element if and only if $\overline{\mathbb{R}\Gamma} \subset M_n(\mathbb{R})$ contains a rank one projection. We assume that there is a rank one projection $P \in \overline{\mathbb{R}G}$.

Let $A \in \overline{\mathbb{R}\Gamma}$ be non-zero and of minimal rank. By irreducibility, it suffices to show that $\dim(\mathrm{Im}(A)) = 1$. Indeed, this sufficient as, since Γ is irreducible, there is $\gamma \in \Gamma$ such that $\mathrm{Im}(\gamma A) \not\subset \ker(\gamma A)$ and therefore γA is a projection.

As Γ is irreducible and Zariski connected, there is $\gamma_1 \in \Gamma$ such that $\gamma_1 \mathrm{Im}(P) \not\subset \ker(A) \cup \ker(P)$. Thus upon replacing P by $\gamma_1 P$, we can assume that $\mathrm{Im}(P) \not\subset \ker(A)$ so that AP has rank 1. Similarly, there is $\gamma_2 \in \Gamma$ with $\gamma_2 \mathrm{Im}(A) \not\subset \ker(A)$ and $\gamma_2 A \mathrm{Im}(P) \not\subset \ker(P)$. Therefore by replacing A by $\gamma_2 A$ if necessary, we can furthermore assume that $A^2 \neq 0$ and that AP is a rank one projection.

Observe that for all $B \in \overline{\mathbb{R}\Gamma}$ either $B\mathrm{Im}(A) \subset \ker(A)$ or $B\mathrm{Im}(A) \cap \ker(A) = 0$. Indeed, if the latter is not the case $BA \neq 0$ while $\mathrm{rk}(BA) < \mathrm{rk}(A)$, a contradiction to the definition of A.

Denote $S := A\overline{\mathbb{R}\Gamma}|_{\mathrm{Im}(A)}$. Then $S\backslash\{0\} \subset \mathrm{GL}(\mathrm{Im}(A))$. Notice that S is a semigroup without proximal elements and all of its eigenvalues are of the same modulus, as otherwise A is not of minimal rank. So by applying the previous case, we conclude that all elements of $\overline{S}^Z$ have eigenvalues of the same modulus. On the other hand, $\overline{S}^Z \supset AG|_{\mathrm{Im}(A)}$ and thus, since S is scalar invariant,

$$\overline{S}^Z \supset A\mathbb{R}G|_{\mathrm{Im}(A)} \text{ and thus } \overline{S}^Z \supset A\overline{\mathbb{R}G}|_{\mathrm{Im}(A)} \ni AP|_{\mathrm{Im}(A)},$$

yet AP is a rank one projection, so $\dim \mathrm{Im}(A) = 1$. □

Proof. (of Theorem 4.4)(Sketch of proof) We first sketch how to show that if $\Gamma \subset \mathrm{GL}_n(\mathbb{R})$ acts strongly irreducibly with a proximal element, then there is $r > 0$ such that for all $\varepsilon < r$ there is a finite set $F \subset \Gamma$ such that for all $g \in \mathrm{GL}_n(\mathbb{R})$ there is $f \in F$ such that fg is (r, ε)-proximal.

First one uses strong irreducibility to show (see Lemma 3.15) that there is a finite subset $F_0 \subset \Gamma$ that is $(1, r)$-separating, i.e. for all $v \in \mathbb{P}(\mathbb{R}^n)$ and all hyperplanes H there is $f \in F_0$ such that $d(fv, H) > r$. Next one picks $\gamma \in \Gamma$ an (r, ε)-proximal element for some $r > 0$ and $\varepsilon < r$ (given the assumption that there is a proximal element in Γ a suitable power of it will achieve this). If now $g \in \mathrm{GL}_n(\mathbb{R})$ then we consider the Cartan decomposition $g = k_1 a k_2$ and note that g is 2-Lipschitz near $k_2^{-1} e_1$ on $\mathbb{P}(\mathbb{R}^n)$. We then pick f_1 such that $d(f_1 k_1 e, H_\gamma) > r$. So (see Lemma 3.11) $\gamma f_1 g$ will be $(c\varepsilon)$-Lipschitz on some open set of $\mathbb{P}(\mathbb{R}^n)$, where c is a fixed constant only depending on (the Lipschitz constants of) F. So by Lemma 3.11, $\gamma f_1 g$ is $(c'\varepsilon)$-contracting for some other constant c'. Finally, to conclude the proof, we may pick $f_2 \in F_0$ such that $f_2 \gamma f_1 g$ is $(r, c'\varepsilon)$-proximal. Setting $F = F_0 \gamma F_0$ ends the proof of the above claim.

We turn to the proof of Theorem 4.4, so let $\Gamma \subset \mathrm{SL}_n(\mathbb{R})$ be a Zariski dense semigroup. We leave as an exercise to the reader to check that an element $g \in \mathrm{SL}_n(\mathbb{R})$ is $\mathbb{R}$-regular if and only if $\Lambda^{n(n-1)/2}\mathrm{Ad}(g)$ acting on $\Lambda^{n(n-1)/2}\mathfrak{sl}_n(\mathbb{R})$ is proximal. Moreover, there is an irreducible representation of $\Lambda^{n(n-1)/2}\mathfrak{sl}_n(\mathbb{R})$ such

that g is $\mathbb{R}$-regular if and only if $\rho(g)$ is proximal. Using the latter and Theorem 4.2, there is $\gamma \in \Gamma$ such that $\rho(\gamma)$ is proximal. We then apply the above claim. □

By a similar argument to the above proof one can do this uniformly over any fixed finite set of irreductible representations, namely:

Corollary 4.7. *Let $\Gamma \subset \mathrm{SL}_n(\mathbb{R})$ be a Zariski dense semigroup and let $\rho_1, \dots, \rho_k$ be irreducible representations of $\overline{\Gamma}^Z$ such that for all $1 \leq i \leq k$ the group $\rho_i(\overline{\Gamma}^Z)$ contains a proximal element. Then there exists $r > 0$ such that for all $\varepsilon < r$ there is a finite set $F \subset \Gamma$ such that for all $g \in \overline{\Gamma}^Z$ there is $f \in F$ such that $\rho_i(fg)$ is (r, ε)-proximal for each $i = 1, ..., k$.*

4.2. **The Benoist cone.** We first review the Cartan and Jordan projections of $\mathrm{SL}_n(\mathbb{R})$. Consider the Weyl chamber

$$\mathfrak{a}^+ = \{\mathrm{diag}(\alpha_1, \dots, \alpha_n) : \alpha_1 + \dots + \alpha_n = 0 \text{ and } \alpha_1 \geq \dots \geq \alpha_n\},$$

which is a cone in the Lie algebra $\mathfrak{a} = \mathrm{Lie}(A)$.

For each element $g = k_1 a k_2 \in KA^+K$ there is a unique element $\kappa(g) \in \mathfrak{a}^+$ such that $a = \exp(\kappa(g))$. The element $\kappa(g) \in \mathfrak{a}^+$ is called the **Cartan projection** of g.

Recall that an element $g \in \mathrm{SL}_n(\mathbb{R})$ has the **Jordan decomposition** into $g = g_s g_u = g_u g_s$, where g_s is a **semisimple** element (i.e. diagonalizable over $\mathbb{C}$) and g_u is unipotent. We can moreover further decompose g_s into $g_s = g_e g_h = g_h g_e$, where g_h is a **hyperbolic** element meaning that it is diagonalizable over $\mathbb{R}$ and g_e is an **elliptic** element so is conjugate to a matrix

$$r_{\theta_1} \boxplus \dots \boxplus r_{\theta_\ell} \boxplus 1 \boxplus \dots \boxplus 1,$$

where $r_\theta = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$ and $\boxplus$ is the direct sum of the matrices.

The **Jordan projection** $j(g)$ is the unique element of $\mathfrak{a}^+$ such that $\exp(j(g))$ is conjugate to g_h. Indeed, $j(g) = \mathrm{diag}(\log|\lambda_1|, \dots, \log|\lambda_n|)$ with λ_i the eigenvalues of g satisfying $|\lambda_1| \geq \dots \geq |\lambda_n|$.

Definition 4.8. *Let $\Gamma \subset \mathrm{SL}_n(\mathbb{R})$ be a semigroup. The **Benoist cone** $\mathcal{C}_\Gamma \subset \mathfrak{a}^+$ is defined as the closure of all rays $\langle j(\gamma)\rangle_{\mathbb{R}_+}$ with $\gamma \in \Gamma$.*

Theorem 4.9. *(Benoist* [Ben97]*) If Γ is a Zariski dense subgroup of $\mathrm{SL}_n(\mathbb{R})$, then the Benoist cone $\mathcal{C}_\Gamma$ is convex and has non-empty interior.*

In particular, the subgroup of $\mathfrak{a}$ generated by the Jordan projections $j(\gamma)$ with $\gamma \in \Gamma$ is not contained in a hyperplane of $\mathfrak{a}$. In fact, as is shown in [Ben97], the latter set is dense in $\mathfrak{a}$.

Moreover, we note that assuming Schanuel's Conjecture as shown in Prasad-Rapinchuk [PR05], there are n elements $\gamma_1, \dots, \gamma_n \in \Gamma$ such that $(j(\gamma_i))_{1 \leq i \leq n}$ generate a dense subgroup of $\mathfrak{a}$.

Lemma 4.10. *Suppose that $\gamma_1, \gamma_2 \in \mathrm{SL}_n(\mathbb{R})$ are proximal and that $v^+_{\gamma_1} \notin H_{\gamma_2}$ and $v^+_{\gamma_2} \notin H_{\gamma_2}$. Then*

$$|\lambda_1(\gamma_1^{n_1}\gamma_2^{n_2})| = |\lambda(\gamma_1)|^{n_1} \cdot |\lambda_1(\gamma_2)|^{n_2} \cdot e^{o(n_1+n_2)}$$

as n_1 and n_2 tend to $+\infty$.

Proof. Recall that by the spectral radius formula, $||g^n||^{1/n} \to |\lambda_1(g)|$ as $n \to \infty$ for $g \in \mathrm{SL}_n(\mathbb{R})$. Moreover, $||\gamma_1^{n_1}\gamma_2^{n_2}|| \leq ||\gamma_1^{n_1}||\,||\gamma_2^{n_2}|| \ll |\lambda_1(\gamma_1)^{n_1}|\,|\lambda_1(\gamma_2)^{n_2}|$, which readily implies that $|\lambda_1(\gamma_1^{n_1}\gamma_2^{n_2})| \ll |\lambda(\gamma_1)|^{n_1} \cdot |\lambda_1(\gamma_2)|^{n_2} \cdot e^{o(n_1+n_2)}$.

For the other inequality, we recall that by Lemma 2.2.1 of [Ben97], if g is (r,ε)-proximal then

$$\lambda_1(g) \leq ||g|| \leq C(r,\varepsilon)|\lambda_1(g)|, \tag{4.1}$$

where $C(r,\varepsilon)$ is a constant only depending on r and ε and not on g. Furthermore given $r > 0$, it holds that $C(r,\varepsilon) \to 1$ as $\varepsilon \to 0$.

To conclude the proof, write $v^+_{\gamma_2} = \alpha v^+_{\gamma_1} + v^-_2$, where $v^-_2 \in H_{\gamma_1}$. Then $\gamma_2^{n_2} v^+_{\gamma_2} = \lambda_1(\gamma_2)^{n_2} v^+_{\gamma_2}$ and therefore

$$\gamma_1^{n_1}\gamma_2^{n_2} v^+_{\gamma_2} = \alpha\lambda_1(\gamma_2)^{n_2}\lambda_1(\gamma_1)^{n_1} v^+_{\gamma_1} + \lambda_1(\gamma_2)^{n_2}\gamma_1 v^-_2,$$

where $||\gamma_1 v^-_2|| \ll |\lambda_1(\gamma_1)|^{n_1(1-\delta)}$. This shows that $||\gamma_1^{n_1}\gamma_2^{n_2}|| \geq \alpha|\lambda_1(\gamma_1)^{n_1}\lambda_1(\gamma_2)^{n_2}|+$ (lower order terms). Using (4.1), the claim follows. □

Proof. ($\mathcal{C}_\Gamma$ is convex) Denote by ρ_i the representation $\Lambda^i\mathbb{R}^n$ for $1 \leq i \leq n-1$. Let $\gamma_1, \gamma_2 \in \Gamma$ and choose N a sufficiently large number to be determined later and $f_1, f_2 \in F$ such that $\rho_i(f_1\gamma_1^N)$ and $\rho_i(f_2\gamma_2^N)$ are (r,ε)-proximal. Then by (4.1),

$$\lambda_1(\rho_i(f_i\gamma_i^N)) \asymp ||\rho_i(f_i\gamma_i^N)|| \asymp ||\rho_i(\gamma_i^N)|| \asymp e^{N(\log|\lambda_1(\gamma_i)|+\ldots+\log|\lambda_i(\gamma_j)|)}$$

for $i = 1, 2$. Thus by choosing N sufficiently large, there is $\delta_i \in \Gamma$ such that $\langle j(\delta)\rangle_{\mathbb{R}_+}$ is arbitrarily close to $\langle j(\gamma)\rangle_{\mathbb{R}_+}$ and such that $\rho_i(\delta)$ is (r,ε)-proximal for all $1 \leq i \leq n-1$. Moreover we can ensure that $v^+(\delta_1) \notin H_{\delta_2}$ and $v^+(\delta_2) \notin H_{\delta_1}$ in each ρ_i. Therefore by Lemma 4.10,

$$\log(\rho_i(\delta_1^{n_1}\delta_2^{n_2})) = n_1 \log|\lambda_1(\rho_i(\delta_1))| + n_2 \log|\lambda_1(\rho_i(\delta_1))| + o(n_1+n_2),$$

which readily implies that $\mathcal{C}_\Gamma$ is convex. □

Now that we know that $\mathcal{C}_\Gamma$ is a convex cone based at the origin, in order to prove the second part of Theorem 4.9, namely that $\mathcal{C}_\Gamma$ has non-empty interior, it remains only to prove that $\mathcal{C}_\Gamma$ is not entirely contained in a hyperplane in $\mathfrak{a}$. We will not give the proof of this fact in this course (we refer the reader to Benoist's original article as well as to the book by Benoist and Quint for two very different proofs of this fact). We will only mention that it is easy to see that $\mathcal{C}_\Gamma$ is not contained in a rational hyperplane, i.e. one defined by a linear form with rational coefficients when expressed as a linear combinations of the $\log|\lambda_i|$. Indeed, being contained in such a hyperplane would mean that there are integers $k_1, \ldots, k_n$, not all equal, such that every $\mathbb{R}$-regular element γ of Γ satisfies the relation $\lambda_1(\gamma)^{k_1}\ldots\lambda_n(\gamma)^{k_n} = 1$. However semisimple elements in SL_n satisfying such a relation do not form a Zariski-dense subset (while $\mathbb{R}$-regular elements do by Theorem 4.4). To see it, note that it is contained in the constructible set of all conjugates of the proper algebraic subgroup of the diagonal group defined by this relation, hence has positive co-dimension. In the next section we will show even more: that there are $\mathbb{R}$-regular elements $\gamma \in \Gamma$ that satisfy none of those relations.

4.3. **Exercises.**

4.3.1. The collection of $\mathbb{R}$-regular elements is $g \in \mathrm{SL}_n(\mathbb{R})$ is not a Zariski-open set and the set of non-$\mathbb{R}$-regular elements is Zariski-dense. Hint: First consider the case $\mathrm{SL}_2(\mathbb{R})$.

4.3.2. Prove Lemma 4.5. Hint: Write $\overline{\Gamma}^Z = V_1 \cup \ldots \cup V_k$, where the V_i are the irreducible components. Then Γ permutes the components.

4.3.3. For an element $g \in \mathrm{SL}_n(\mathbb{R})$ the following properties are equivalent:

(i) g is $\mathbb{R}$-regular.
(ii) $\Lambda^i(g)$ is proximal for each $1 \leq i \leq n-1$.
(iii) $\Lambda^{n(n-1)/2}\mathrm{Ad}(g)$ acting on $\Lambda^{n(n-1)/2}\mathfrak{sl}_n(\mathbb{R})$ is proximal.

Moreover, there exist an irreducible subrepresentation ρ of $\Lambda^{n(n-1)/2}\mathfrak{sl}_n(\mathbb{R})$ such that g is $\mathbb{R}$-regular if and only if $\rho(g)$ is proximal.

4.3.4. Prove the claims around (4.1).

5. The Galois theoretic results of Prasad-Rapinchuk

The aim of this section is to show the following theorem. Recall that the Galois group $\mathrm{Gal}_K(P)$ of a polynomial P with coefficients in a field K is the Galois group of the splitting field K_P over K. We can view the latter group as a group of permutations acting on the roots of P.

Theorem 5.1. *(Prasad-Rapinchuk* [PR03]*) Let K be a finitely generated field of characteristic zero and let $\Gamma \leq \mathrm{SL}_n(K)$ be a finitely generated Zariski dense subgroup. Then there is a finite index subgroup $\Delta \leq \Gamma$ and a coset $x\Delta$ for $x \in \Gamma$ such that for all $\gamma \in x\Delta$ the following properties hold:*

(i) The characteristic polynomial $P_\gamma(X) = \det(XI_n - \gamma)$ is irreducible over K.
(ii) $\mathrm{Gal}_K(P_\gamma) \cong \mathrm{Sym}(n)$.
(iii) γ is regular semisimple and $\langle\gamma\rangle$ is Zariski-dense in the maximal torus $Z(\gamma)$, which is the centralizer of γ.

Theorem 5.1 allows us to deduce the following strengthening of Theorem 4.4.

Corollary 5.2. *If $\Gamma < \mathrm{SL}_n(\mathbb{R})$ is Zariski dense, there is a Zariski dense subset of $\mathbb{R}$-regular elements satisfying (i), (ii) and (iii).*

Proof. By Theorem 4.4, there is a finite set $F \subset \Delta$ such that for all $g \in \mathrm{SL}_n(\mathbb{R})$ there is $f \in F$ such that gf is $\mathbb{R}$-regular. Thus $x\Delta = (x\Delta \cap \{\mathbb{R}\text{-regular elements}\}) \cdot F^{-1}$ and so $x\Delta \cap \{\mathbb{R}\text{-regular elements}\}$ is Zariski dense. □

An element $\gamma \in \Gamma$ satisfying (i), (ii) and (iii) will be called K-Galois generic. Clearly condition (ii) implies (i) (since $\mathrm{Sym}(n)$ is transitive). We will show below that condition (ii) also implies (iii). We also mention that Prasad-Rapinchuk have shown Theorem 5.1 not only for a Zariski dense subgroup of SL_n, but more generally for any Zariski dense subgroup in a semisimple algebraic group $\mathbb{G}$. The analogue of being K-Galois generic is to say that the Galois group of the splitting field of $Z(\gamma)^\circ$ is the full Weyl group of $\mathbb{G}$.

5.1. Some facts on algebraic tori.

Denote by $\mathbb{G}_m$ the one dimensional multiplicative algebraic group such that $\mathbb{G}_m(K) = K^\times$ for any field K. An **(algebraic) torus** is an algebraic group T (defined over K) which is isomorphic over $\overline{K}$ to $\mathbb{G}_m^r$ for some $r \geq 1$. The number r is called the **absolute rank** of T.

A **character** of a torus T is an algebraic group homomorphism $\chi : T \to \mathbb{G}_m$. The set of all characters $\mathfrak{X}(T)$ of T is an additive group and it holds that

$$\mathfrak{X}(T) \cong \mathfrak{X}(\mathbb{G}_m^r) \cong \mathbb{Z}^r.$$

If T is defined over some field K (for example T is an algebraic subgroup of GL_n defined as the vanishing locus of a family of polynomials in the matrix entries with coefficients in K) then $\mathrm{Gal}(\overline{K}|K)$ acts on $T(\overline{K})$ and also on $X(T)$ by the formula

$$\chi^\sigma(t) = (\sigma\chi\sigma^{-1})(t).$$

We note that if T is a subgroup of GL_n, since χ is a morphism of algebraic varieties it can be written as a polynomial map in the matrix entries. In that situation this Galois action is just the Galois action on the coefficients of this polynomial map.

This gives a group homomorphism

$$\mathrm{Gal}(\overline{K}|K) \to \mathrm{Aut}(\mathbb{Z}^r) = \mathrm{GL}_r(\mathbb{Z}). \tag{5.1}$$

If $L \leq \overline{K}$ is an algebraic field extension of K, one says that a character χ is defined over L if the Galois group $\mathrm{Gal}(\overline{K}|L)$ fixes χ. One says that T splits over L if there is a basis of $\mathfrak{X}(T)$ of characters defined over L. Clearly, picking a basis of $\mathfrak{X}(T)$ and the finite field extension extension of K generated by the coefficients of each basis element, one sees that T splits over some finite extension of K. In particular, the image of (5.1) is a finite subgroup.

We note moreover, that there is a bijection

$$\{\text{algebraic subgroups of } T\} \longleftrightarrow \{\text{additive subgroups of } \mathfrak{X}(T) \cong \mathbb{Z}^r\}$$
$$T_0 \longleftrightarrow \{\chi \in \mathfrak{X}(T) \,:\, \chi|_{T_0} \equiv 1\}$$

The same map furthermore induces a bijection:

$$\{\text{connected algebraic subgroups of } T\} \longleftrightarrow \{\text{primitive subgroups of } \mathfrak{X}(T)\}, \quad (5.2)$$

where we call a subgroup of $\mathbb{Z}^r$ to be primitive if it is of the form $\mathbb{Z}^r \cap V$ for V a subspace.

In particular the algebraic subgroups of T that are defined over K correspond to additive subgroups of $X(T)$ that are fixed under the Galois group. This implies in particular that if $\mathrm{Gal}(\overline{K} \,|\, K)$ acts irreducibly on $\mathfrak{X}(T) \cong \mathbb{Z}^r$, then T has no proper connected algebraic subgroup defined over K and even no infinite proper algebraic subgroup defined over K.

5.2. **Proof of Theorem 5.1.** We first use the above established facts on algebraic tori to deduce in Theorem 5.1 that (i) and (ii) imply (iii). Indeed, if (i) and (ii) hold, then P_γ is irreducible and therefore has distinct roots. So γ is a regular semisimple element meaning that γ is diagonalizable and $Z(\gamma) = T_\gamma$ is a maximal torus in SL_n. Furthermore $\overline{\langle\gamma\rangle}^Z$ is defined over K, hence if (ii) holds, then it acts irreducibly on $\mathfrak{X}(T_\gamma) \cong \mathbb{Z}^{n-1}$ and therefore by (5.2), $\overline{\langle\gamma\rangle}^Z$ is either finite or all of $Z(\gamma)$. We will show in below proof that every element of $x\Delta$ will have infinite order and therefore (iii) is implied.

We proceed with the proof of (i) and (ii). We first show the following lemma of Jordan.

Lemma 5.3. *(Jordan) Let G be a finite group and let $H \subsetneq G$ be a proper subgroup. Then there is $g \in G$ such that $\mathrm{Cl}(g) \cap H = \emptyset$, where $\mathrm{Cl}(g) = \{fgf^{-1} \,:\, f \in G\}$ is the conjugacy class of g.*

Proof. We claim that any group of permutations acting transitively on $n \geq 2$ elements has a derangement, i.e. an element g such that $gx \neq x$ for all x. To prove the lemma, apply this claim to the G action on left cosets of H. By the claim there is $g \in G$ such that $gxH \neq xH$ for all $x \in G$ or equivalently $x^{-1}gx \notin H$, which implies the lemma.

Denote by G a group of permutations acting transitively on $n \geq 2$ elements. The claim follows from the following result due to Cauchy, that is sometimes called *the lemma that is not Burnside's*:

$$\mathbb{E}_G(|\mathrm{Fix}(g)|) = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}(g)| = |\{G\text{-orbits}\}|,$$

where $\mathrm{Fix}(g) = \{x : gx = x\}$. Indeed to prove the latter, note that $|\mathrm{Fix}(g)| = \sum_{x\in G} 1_{gx=x}$ and we apply the orbit stabilizer theorem,

$$\mathbb{E}_G(|\mathrm{Fix}(g)|) = \frac{1}{|G|}\sum_{x,g} 1_{gx=x} = \frac{1}{|G|}\sum_x |\mathrm{Stab}_G(x)| = \frac{1}{|G|}\sum_x \frac{1}{|G.x|} = |\{G\text{-orbits}\}|.$$

Since G is transitive, $\mathbb{E}_G(|\mathrm{Fix}(g)|) = 1$ and note that $|\mathrm{Fix}(e)| = n \geq 2$. So there must exist elements with $|\mathrm{Fix}(g)| = 0$, which are exactly the derangements. □

Write $G = \mathrm{Gal}_K(P_\gamma) \leq \mathrm{Sym}(n)$. By Lemma 5.3 it suffices to show that G intersects every conjugacy class of $\mathrm{Sym}(n)$, i.e. every cycle type. Recall that conjugacy classes of $\mathrm{Sym}(n)$ are in bijections with partitions of n. Indeed, if $n = n_1 + \ldots + n_k$ is a partition with $n_1 \geq \ldots \geq n_k$ then the corresponding conjugacy class consists of permutations σ expressible as distinct cycles $\sigma = \sigma_1 \cdots \sigma_k$ with $|\sigma_i| = n_i$ for $1 \leq i \leq k$.

Recall that by Corollary 1.9 there are infinitely many primes such that K embeds into $\mathbb{Q}_p$ in such a way that Γ is a subgroup of $\mathrm{SL}_n(\mathbb{Z}_p)$. We prove the following two useful lemmas.

Lemma 5.4. *If $\Gamma \leq \mathrm{SL}_n(\mathbb{Z}_p)$ is Zariski-dense, then $\overline{\Gamma}$ is open and closed in $\mathrm{SL}_n(\mathbb{Z}_p)$.*

Proof. The closure $\overline{\Gamma}$ is a p-adic Lie group with $\mathbb{Q}_p$-Lie algebra $\mathfrak{h}$. Since Γ is Zariski dense, $\mathfrak{h}$ is invariant under all of $\mathrm{Ad}(\mathrm{SL}_n(\mathbb{Q}_p))$. So it is an ideal in the simple Lie algebra $\mathfrak{sl}_n(\mathbb{Q}_p)$. Since $\mathrm{SL}_n(\mathbb{Z}_p)$ is compact and Γ is infinite, $\mathfrak{h}$ is non-trivial and thus it is all of $\mathfrak{sl}_n(\mathbb{Q}_p)$, which implies the claim. □

Lemma 5.5. *Let $\Gamma \leq \mathrm{SL}_n(K)$ be a finitely generated and Zariski dense subgroup and $p_1, \ldots, p_n$ be distinct primes such that $K \hookrightarrow \mathbb{Q}_{p_i}$ and $\Gamma \hookrightarrow \mathrm{SL}_n(\mathbb{Z}_{p_i})$. Then $\overline{\Gamma}$ is open and closed in the product $\mathrm{SL}_n(\mathbb{Z}_{p_1}) \times \cdots \times \mathrm{SL}_n(\mathbb{Z}_{p_n})$.*

Proof. Since $\mathrm{SL}_n(\mathbb{Z}_p)$ is a virtually pro-p group, it suffices by Lemma 5.4 to show that if G_i are pro-p groups and $G \leq G_1 \times \cdots \times G_n$ projects onto each G_i, then it is all of $G_1 \times \cdots \times G_n$. By induction on the number of factors, we can assume without loss of generality that G projects onto $H = G_2 \times \cdots \times G_n$. Yet since G_1 is pro-p_1, the maps $\Phi_n(x) = x^{p_1^n}$ are surjective on H and $\Phi_n(x) \to 1$ for all $x \in G_1$ as $n \to \infty$, it follows that $H \leq \lim_{n\to\infty} \Phi_n(G) \leq G$ and therefore $G = G_1 \times \cdots \times G_n$. □

We proceed with recalling some facts on finite extensions of $\mathbb{Q}_p$. For every $n \geq 1$, there is a unique unramified extension K of $\mathbb{Q}_p$ of degree n, where being unramified means that $\mathcal{O}_K/\mathfrak{m} \cong \mathbb{F}_q$ for $q = p^n$. We denote the latter extension by $\mathbb{Q}_p^{(n)}$ and note that $\mathbb{Q}_p^{(n)} = \mathbb{Q}_p(\zeta)$ for any primitive $(p^n - 1)$-th root of unity ζ. This is a Galois extension with cyclic Galois group generated by the Frobenius automorphism $\mathrm{Frob}_p(P(\zeta)) = P(\zeta^p)$ for $P \in \mathbb{Q}_p[X]$ so

$$\mathrm{Gal}(\mathbb{Q}_p^{(n)} \,|\, \mathbb{Q}_p) = \langle \mathrm{Frob}_p \rangle \cong \mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(\mathbb{F}_q \,|\, \mathbb{F}_p)$$

and $\mathbb{Q}_p^{(n)} = \mathbb{Q}_p \oplus \zeta\mathbb{Q}_p \oplus \ldots \oplus \zeta^{p^{n-1}}\mathbb{Q}_p$. In this basis, the multiplication on $(\mathbb{Q}_p^{(n)})^\times$ yields a homomorphism $(\mathbb{Q}_p^{(n)})^\times \hookrightarrow \mathrm{GL}_n(\mathbb{Q}_p)$ whose image is an n-dimensional torus defined over $\mathbb{Q}_p$, which we denote by $T_p^{(n)}$.

If $[n] = (n_1, \dots, n_k)$ is a partition of n we denote by $T_p^{[n]}$ the block diagonal $\mathbb{Q}_p$-torus of rank n in GL_n, namely

$$T_p^{[n]} = \mathrm{diag}((\mathbb{Q}_p^{(n_1)})^\times, \dots, (\mathbb{Q}_p^{(n_k)})^\times).$$

We say that an element $\gamma \in T_p^{[n]}$ is primitive if each component is a primitive element of $\mathbb{Q}_p^{(n_i)}$, i.e. generates $\mathbb{Q}_p^{(n_i)}$ as a field over $\mathbb{Q}_p$.

Proposition 5.6. *Let K be a finitely generated field, $\gamma \in \mathrm{GL}_n(K)$ a regular semisimple element and $\sigma : K \to \mathbb{Q}_p$ a field embedding such that $\sigma(\gamma)$ is conjugate to a primitive element of $T_p^{[n]}$. Then $\mathrm{Gal}_K(P_\gamma)$ has an element of cycle type $[n]$.*

Proof. Let $P_\gamma \in K[X]$ be the characteristic polynomial. Then $K[X]/(P_\gamma) \cong K[\gamma] \leq M_n(K)$ is a commutative semisimple K-algebra. Viewing K as a subfield of $\mathbb{Q}_p$, as γ is primitive, $K[\gamma] \otimes_K \mathbb{Q}_p \cong \bigoplus \mathbb{Q}_p^{(n_i)}$. The claim follows since Frob_p permutes the roots of P_γ with cycle type $[n]$. □

A key observation in concluding the proof is that the $\mathrm{GL}_n(\mathbb{Q}_p)$-conjugacy class of $T_p^{[n]}$ is open in $\mathrm{GL}_n(\mathbb{Q}_p)$ for all $[n]$ and furthermore intersects every neighborhood of the identity in $\mathrm{GL}_n(\mathbb{Q}_p)$ and $\mathrm{SL}_n(\mathbb{Q}_p)$.

Let k be the number of partitions of n and choose distinct primes $p_1, \dots, p_k$ such that $K \hookrightarrow \mathbb{Q}_{p_i}$ and $\Gamma \hookrightarrow \mathrm{SL}_n(\mathbb{Z}_{p_i})$. Then by Lemma 5.5 the image of the embedding $\Gamma \hookrightarrow \prod_i \mathrm{SL}_n(\mathbb{Z}_{p_i})$ has open closure. Therefore we can pick $x \in \Gamma$ and an open subgroup $\mathcal{O}$ in $\prod_{i=1}^k \mathrm{SL}_n(\mathbb{Z}_{p_i})$ such that every $\gamma \in x\mathcal{O} \cap \Gamma$ satisfies that $\gamma_i \in \mathrm{SL}_n(\mathbb{Z}_{p_i})$ is conjugate to a primitive element in $T_{p_i}^{[n]}$. In particular Proposition 5.6 tells us that $\mathrm{Gal}_K(P_\gamma)$ has an element of each any cycle type. It follows that $\mathrm{Gal}_K(P_\gamma) \simeq \mathrm{Sym}(n)$ and this ends the proof as $\mathcal{O}$ has finite index.

5.3. **Two corollaries.**

Corollary 5.7. *Let K be a finitely generated field of characteristic zero and let $\Gamma \leq \mathrm{SL}_n(K)$ be a finitely generated Zariski dense subgroup. Then there is an infinite subset $\{\gamma_n\}_{n\geq 1}$ of Γ such that the set $\{\lambda_i(\gamma_j) : 1 \leq i \leq n-1 \text{ and } j \geq 1\}$ is multiplicatively independent.*

Proof. We note that by (iii) of Theorem 5.1 there is an element $\gamma_1 \in \Gamma$ such that $\lambda_1(\gamma_1), \dots, \lambda_{n-1}(\gamma_1)$ are multiplicatively independent. Let $K_1 = K(\lambda_i(\gamma_1), 1 \leq i \leq n-1)$. Then K_1 is finitely generated and therefore there is $\gamma_2 \in \Gamma$ such that $\mathrm{Gal}_{K_1}(\gamma_2) \cong \mathrm{Sym}(n)$. Set $k_n = 0$ and let $k_1, \dots, k_{n-1}$ be integers such that $\lambda_1(\gamma_2)^{k_1} \cdots \lambda_{n-1}(\gamma_2)^{k_{n-1}} \in K_1$. Then for all $\sigma \in \mathrm{Sym}(n)$ it holds that

$$\lambda_1(\gamma_2)^{k_{\sigma(1)}} \cdots \lambda_{n-1}(\gamma_2)^{k_{\sigma(n-1)}} \lambda_n(\gamma_2)^{k_{\sigma(n)}} = \lambda_1(\gamma_2)^{k_1} \cdots \lambda_{n-1}(\gamma_2)^{k_{n-1}} \lambda_n(\gamma_2)^{k_n}.$$

Therefore it follows that $k_{\sigma(i)} = k_i$ for all i by multiplicative independence and hence $k_i = k_n = 0$. Iterating this construction implies the claim. □

To state a further corollary, we recall the symmetric space structure on $X = \mathrm{SL}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R})$. Indeed, we can identify X with the space of positive-definite symmetric matrices and $\mathrm{SL}_n(\mathbb{R})$ acts on X by $g \circ M = g^T M g$ for $M \in X$ and $g \in \mathrm{SL}_n(\mathbb{R})$.

We can write every element $M \in X$ as $M = k \circ a$ for $k \in \mathrm{SO}_n(\mathbb{R})$ and $a = \mathrm{diag}(a_1, \ldots, a_n)$ a diagonal element with $a_i > 0$ for $1 \leq i \leq n$. Let $x_0 = [\mathrm{Id}_n]$ be the identity coset. Then a $\mathrm{SL}_n(\mathbb{R})$-invariant metric on X is determined by

$$d(x_0, M) = d(x_0, k \circ a) = d(x_0, a) = \sqrt{\sum_{i=1}^{n} (\log a_i)^2}.$$

Let $\Gamma < \mathrm{SL}_n(\mathbb{R})$ be Zariski-dense, discrete and torsion free. Then $\Gamma \backslash X$ is a manifold and forms an example of a locally symmetric space. Each closed geodesic on $\Gamma \backslash X$ is represented by a diagonalizable element $\gamma \in \Gamma$ and its length is

$$\ell(\gamma) = d(x, \gamma x) = d(x_0, g^{-1}\gamma g x_0) = \sqrt{\sum_{i=1}^{n} (\log \lambda_i(\gamma))^2}, \tag{5.3}$$

where x is on the geodesic and written as $x = gx_0$.

Recall Schanuel's conjecture from transcendental number theory.

Conjecture 5.8. *(Schanuel) Let $z_1, \ldots, z_n$ be complex numbers that are linearly independent over $\mathbb{Q}$. Then the transcendence degree of the collection of numbers*

$$z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n}$$

is at least n.

Corollary 5.9. *Assume Schanuel's conjecture. Let $\Gamma \leq \mathrm{SL}_n(\mathbb{R})$ be a discrete, Zariski-dense and torsion free subgroup. Then $\mathbb{Q}(\ell(\gamma), \gamma \in \Gamma)$ has infinite transcendence degree.*

Proof. Let $(\gamma_j)_{j \geq 1}$ be as in Corollary 5.7. Assume for a contradiction that the above transcendence degree is finite. Then there is $k_0 \geq 1$ such that for every $k \geq k_0$ the number $\ell(\gamma_k)$ is algebraic over

$$L_0 = \mathbb{Q}(\log |\lambda_i(\gamma_j)|, 1 \leq i \leq n, j \leq k_0).$$

This implies that for each $k > k_0$ the transcendence degree of $L_0(\log |\lambda_i(\gamma_k)|, 1 \leq i \leq n)$ is at most $\mathrm{trdeg}(L_0) + n - 2$, which follows from the relation $\sum_{i=1}^{n} \log |\lambda_i| = 0$ and from (5.3), which gives an algebraic relation between the $\log |\lambda_i(\gamma_k)|$ over L_0. Denote

$$L_k = L_0(\log |\lambda_i(\gamma_j)|, 1 \leq i \leq n, k_0 < j \leq k)$$

and iterating the above argument it follows that $\mathrm{trdeg}(L_k) \leq (k - k_0)(n-2) + \mathrm{trdeg}(L_0)$. On the other hand, by Corollary 5.7, the collection $\log |\lambda_i(\gamma_j)|$ for $1 \leq i \leq n-1$ and $j \geq 1$ is $\mathbb{Q}$-free. Therefore by Schanuel's conjecture $\mathrm{trdeg}(L_k) \geq (k - k_0)(n-1)$, which is a contradiction for large enough k. □

5.4. **Remarks on the Profinite Topology.** If Γ is a discrete group, the profinite topology on Γ is defined to be the smallest topology that makes the map $\pi_N : \Gamma \to \Gamma/N$ continuous for all finite index normal subgroups $N \trianglelefteq \Gamma$. In particular, the set

$$\mathscr{N} = \{N : N \trianglelefteq \Gamma \text{ and } [\Gamma : N] < \infty\}$$

forms a basis of neighborhoods of the identity of this topology.

The profinite completion $\widehat{\Gamma}$ is the totally disconnected compact group defined as the inverse limit

$$\widehat{\Gamma} = \varprojlim_{N \in \mathscr{N}} \Gamma/N$$

of the direct system $\{\Gamma/N\}_{N\in\mathscr{N}}$. This means that $\widehat{\Gamma}$ is the subgroup of the direct product $\prod_{N\in\mathscr{N}}\Gamma/N$ endowed with the product topology given as

$$\widehat{\Gamma}=\left\{(\gamma_N)_{N\in\mathscr{N}}\in\prod_{N\in\mathscr{N}}\Gamma/N\,:\,\pi_M(\gamma_N)=\gamma_M \text{ for all } M\leq N\right\}.$$

In particular, every normal finite index subgroup of Γ is open and closed and a subset Σ of $\widehat{\Gamma}$ is open if for each $s\in\Sigma$ there is $N\in\mathscr{N}$ with $sN\subset\Sigma$. It is dense if is intersects every coset of every finite index normal subgroup. We refer to the book [DdSMS99] for the basics (and much more!) about profinite groups.

If K has charactersitic zero and $\Gamma<\mathrm{SL}_n(K)$ is a finitely generated subgroup, then by Theorem 5.1 the set

$$\Sigma_K=\{\gamma\in\Gamma\,:\,\mathrm{Gal}_K(P_\gamma)\cong\mathrm{Sym}(n)\} \tag{5.4}$$

of K-Galois generic elements is Zariski dense and contains a coset of a finite index subgroup of Γ. Thus means that Σ_K has non-empty interior in Γ for the profinite topology. More recently, Prasad-Rapinchuk [PR17] established that Σ_K is profinitely open in Γ. It can also be seen to be dense, although we live this as an exercise to the interested reader.

We finally mention the work of Lubotzky-Rosenzweig [LR14] and Jouve-Kowalski-Zywina [JKZ13] that is concerned with random walks on Γ. If μ is a finitely supported probability measure Γ assumed to be symmetric and with $\langle\mathrm{supp}\,\mu\rangle=\Gamma$, then they show that $\mu^{*n}(\Gamma\backslash\Sigma_K)\to 0$ exponentially fast as $n\to\infty$. This uses expander graphs and super-strong approximation, see [Bre13].

5.5. **Exercises.**

5.5.1. (suggested by Udi Hrushovski) Prove the following continuous analogue of Jordan's Lemma 5.3. Given a compact group G, let $\mathrm{Conj}(G)$ be the set of conjugacy classes of G endowed with the natural probability measure inherited from the Haar probability measure on G (i.e. a random conjugacy class is the conjugacy class of a random element in G). Suppose $H\leq G$ is a closed subgroup with the property that the natural map $\mathrm{Conj}(H)\to\mathrm{Conj}(G)$ is measure preserving. Show that $H=G$.

5.5.2. Show that primitive elements of $\mathbb{Q}_p^{(n)}$ form an open dense subset. This also holds for $T_p^{[n]}$ and $T_p^{[n]}\cap\mathrm{SL}_n(\mathbb{Q}_p)$.

5.5.3. Show that the $\mathrm{GL}_n(\mathbb{Q}_p)$-conjugacy class of $T_p^{[n]}$ is open in $\mathrm{GL}_n(\mathbb{Q}_o)$ for all $[n]$ and furthermore intersets every neighborhood of the identity in $\mathrm{GL}_n(\mathbb{Q}_p)$ and $\mathrm{SL}_n(\mathbb{Q}_p)$. Hint: Use a dimension argument with the open mapping theorem and use that $\dim_{\mathbb{Q}_p}T_p^{[n]}=n$.

6. Bounded generation

In this final lecture, we discuss bounded generation for linear groups and present a recent result of Corvaja, Rapinchuk, Ren and Zannier that settled the long standing open question about bounded generation of co-compact lattices in semisimple Lie groups. One of the main ingredients of the proof is the existence of Galois generic elements proved earlier in the notes.

6.1. Bounded generation of $\mathrm{SL}_n(\mathbb{Z})$.

Definition 6.1. *A discrete group Γ is said to be **boundedly generated** if there are finitely many $\gamma_1, \dots, \gamma_k \in \Gamma$ such that*

$$\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_k \rangle,$$

i.e. if there are finitely many cyclic subgroups whose product is Γ.

Every finitely generated abelian group is boundedly generated and we leave as an exercise to show that a finitely generated nilpotent group is boundedly generated. On the other hand, not every solvable group is boundedly generated. Indeed the reader may check (see exercise 6.3.3) that the Lamplighter group $\mathbb{Z} \wr \mathbb{Z} = \mathbb{Z} \ltimes \mathbb{Z}^{(\mathbb{Z})}$, where $\mathbb{Z}^{(\mathbb{Z})}$ are the finitely supported sequences of integers indexed by $\mathbb{Z}$, is not boundedly generated.

One of the first main results about bounded generation is the following theorem by Carter and Keller:

Theorem 6.2. *([CK83]) The group $\mathrm{SL}_n(\mathbb{Z})$ is boundedly generated for $n \geq 3$.*

We remark the following:

(i) Carter-Keller [CK83] proved more generally that $\mathrm{SL}_n(\mathcal{O}_K)$ for $n \geq 3$ is boundedly generated, for $\mathcal{O}_K$ the ring of integers of a number field.
(ii) A discrete group Γ is boundedly generated whenever some finite index subgroup of Γ is. (Exercise 6.3.1)
(iii) The free group F_n on $n \geq 2$ letters is not boundedly generated. Indeed since F_n is a finite index subgroup of F_2 (which can be shown by taking a degree n cover of the wedge of two circles) it suffices to show that F_2 is not boundedly generated, which follows as $\mathbb{Z} \wr \mathbb{Z}$ is 2-generated by $(1, 0)$ and $(0, (\delta_{n,0})_{n \in \mathbb{Z}})$ for $\delta_{n,0}$ the sequence that is 1 at $n = 0$ and 0 elsewhere.
(iv) Therefore $\mathrm{SL}_2(\mathbb{Z})$, which has a finite index free subgroup, is not boundedly generated. On the other hand, $\mathrm{SL}_2(\mathcal{O}_K)$ is known to be boundedly generated if the group of units $\mathcal{O}_K^\times$ of the number field K is infinite, [MRS18].
(v) Irreducible non-uniform lattices in orthogonal groups with $\mathbb{Q}$-rank at least 2 are known to be boundedly generated, [ER06].

To prove Theorem 6.2 we establish that there is a constant $c(n)$ such that every matrix in $\mathrm{SL}_n(\mathbb{Z})$ is the product of at most $c(n)$ elementary matrices, i.e. matrices of the form $I_n + zE_{ij} = (I_n + E_{ij})^z$, $z \in \mathbb{Z}$. This amounts to showing that any $A \in \mathrm{SL}_n(\mathbb{Z})$ can be reduced to the identity I_n with boundedly many row or column operations.

For matrices A and B be write $A \sim B$ if B can be obtained from A by a bounded (in terms of n) number of elementary row or column operations. In other words if $B = UAV$ for U and V a finite product (of controlled length) of elementary matrices.

Lemma 6.3. *If $n \geq 3$ and $A \in \mathrm{SL}_n(\mathbb{Z})$ then*

$$A \sim \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix}$$

for $B \in \mathrm{SL}_{n-1}(\mathbb{Z})$.

Proof. Let $(a_1, \ldots, a_n)$ be the bottom row of A. We may assume without loss of generality that $\gcd(a_1, \ldots, a_n) = 1$ so there are $\lambda_i \in \mathbb{Z}$ such that $\sum_{i=1}^n \lambda_i a_i = 1$. If one of the a_i is 0, then by at most n column operations we can replace a_i by 1 and then by $\leq n$ column operations we conclude that

$$A \sim \begin{pmatrix} B & (*) \\ 0 & 1 \end{pmatrix}$$

for $B \in \mathrm{SL}_{n-1}(\mathbb{Z})$. We then apply at most $n-1$ row operations to clear the last column and conclude the claim.

We reduce to the previous situation as follows. Denote $\delta = \gcd(a_2, \ldots, a_{n-1})$. Then we claim that there is $t \in \mathbb{Z}$ such that $\gcd(a_1 + ta_n, \delta) = 1$. Indeed, choose t such that $a_1 + ta_n \not\equiv 0 \bmod p$ for every prime $p|\delta$. This is possible if $p \nmid a_n$ and in the case $p|a_n$ then $p \nmid a_1$ since $\gcd(a_1, \ldots, a_n) = 1$. Thus by one column operation we may assume that $\gcd(a_1, \ldots, a_{n-1}) = 1$ and thus by at most n further column operations, $a_n = 0$ and hence the claim follows. □

The lemma reduces the proof to showing the Theorem in the case $n = 3$ and more precisely to show that any 3×3 matrix

$$A = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{Z})$$

satisfies $A \sim I_3$. The following argument by Nica [Nic18] simplifies the original proof by Carter-Keller [CK83].

The first observation is that

$$\begin{pmatrix} 1 & c' & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ c & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+cc' & c' & 0 \\ c & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{6.1}$$

Thus if $a \equiv 1 \bmod c$, then $d \equiv 1 \bmod c$ since $ad - bc = 1$ and hence

$$A \sim \begin{pmatrix} a & b' & 0 \\ c & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which is clearly $\sim I$ by equation 6.1. We leave it to the reader to check that a similar reduction works in case $a \equiv -1 \bmod c$. The main idea of the proof is to replace A by a power of itself to place oneself in a situation where $a \equiv \pm 1 \bmod c$.

Recall that by Fermat's little theorem, since $\gcd(a, c) = 1$ as $ad - bc = 1$ it holds that $a^{\varphi(c)} \equiv 1 \bmod c$ for $\varphi(c)$ Euler's function. The main lemma is as follows.

Lemma 6.4. *If $c \in \mathbb{Z}$ is an odd prime and $c \nmid a$, then $A^{x(\frac{|c|-1}{2})} \sim I$ uniformly for all $x \in \mathbb{Z}$.*

We postpone the proof of the lemma and conclude the proof of Theorem 6.2. In particular if c and b are odd primes with $\gcd(\frac{|c|-1}{2}, \frac{|b|-1}{2}) = 1$, then there are $x, y \in \mathbb{Z}$ with $x\frac{|c|-1}{2} - y\frac{|b|-1}{2} = 1$. Therefore

$$A^{x\frac{|c|-1}{2}} \cdot A^{-y\frac{|b|-1}{2}} = A$$

and hence $A \sim I_3$ by Lemma 6.4, where we note that

$$A^{-1} = \begin{pmatrix} d & -c & 0 \\ -b & a & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and we have applied Lemma 6.4 for $-b$ instead of c.

Therefore it suffices to find such primes. To do so, we use Dirichlet's Theorem on arithmetic progressions, which says that if α and β are coprime then the set of primes $p \equiv \beta \bmod \alpha$ is infinite.

First note that a and b are coprime, so if a is even b is odd and by one column operation, we may replace a by $a + b$ and thus assume that a is odd. Therefore by the chinese remainder theorem and Dirichlet's theorem we can find infinitely many primes p with $p \equiv b \bmod a$ with $p \equiv 3 \bmod 4$. As

$$A \sim_{(C)} \begin{pmatrix} a & b + ta & 0 \\ c & d + tc & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for all $t \in \mathbb{Z}$, we may thus assume without loss of generality that b is prime and $\equiv 3 \bmod 4$. Similarly using row operations,

$$A \sim_{(R)} \begin{pmatrix} a & b & 0 \\ c + sa & d + sb & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and so we may assume that d is prime and $> b - 1$.

Finally,

$$A \sim_{(C)} \begin{pmatrix} a + tb & b & 0 \\ c + td & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and we claim there is a prime q such that q is odd, $q \equiv c \bmod d$ and $q \equiv 2 \bmod \frac{b-1}{2}$.

Indeed, we note that by construction $\frac{b-1}{2}$ is prime to d and 2 is prime to $\frac{b-1}{2}$. So by the Chinese remainder theorem there is a number n_0 prime to $d(\frac{b-1}{2})$ such that $n_0 \equiv c \bmod d$ and $n_0 \equiv 2 \bmod \frac{b-1}{2}$. Thus by Dirichlet's Theorem there is such a prime q.

It follows that $q - 1 = 1 \bmod \frac{b-1}{2}$ and so $\gcd(\frac{q-1}{2}, \frac{b-1}{2}) = 1$. This ends the proof by the previous argument and it remains to show the lemma.

Proof. (of Lemma 6.4) Recall that by Cayley-Hamilton $A^2 = (\mathrm{tr}A)A - \mathrm{Id}_2$. Therefore for all $n \in \mathbb{Z}$ there are $e, f \in \mathbb{Z}$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = eI_2 + f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} e + fa & bf \\ cf & e + df \end{pmatrix}.$$

If we consider the matrices mod c, both matrices become upper triangular and therefore $a^n \equiv e + fa \bmod c$. If c is an odd prime, then $a^{\frac{|c|-1}{2}} \equiv \pm 1 \bmod c$. Therefore if $n = x\frac{|c|-1}{2}$, it follows that $e + fa \equiv \pm 1 \bmod c$. If $f = 1$, we would be done

by the previous argument (see equation 6.1). But we can clearly reduce to this case by using the following trick due to [Nic18].

If $a \equiv d \bmod s$ and $ad - bsc = 1$, then

$$\begin{pmatrix} a & b & 0 \\ sc & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} -a & -sb & 0 \\ c & d & 0 \\ 0 & 0 & -1 \end{pmatrix} \tag{6.2}$$

To show (6.2), note that by taking determinants mod s, $ad \equiv 1 \bmod s$ however by assumption $a \equiv d \bmod s$ and therefore $a^2 \equiv 1 \bmod s$. Write $s = s_1 s_2$ with $a = 1 + k_1 s_1 = k_2 s_1 - 1$ for some s_1, s_2 and k_1, k_2. Then we observe the following calculation, where the subscript indicates the number of column (C) or row (R) moves:

$$\begin{pmatrix} a & b & 0 \\ sc & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim_{(C)} \begin{pmatrix} a & b & 0 \\ sc & d & 0 \\ s_1 & 0 & 1 \end{pmatrix} \sim_{(2R)} \begin{pmatrix} 1 & b & -k_1 \\ 0 & d & -s_2 c \\ s_1 & 0 & 1 \end{pmatrix} \sim_{(R)} \begin{pmatrix} 1 & b & -k_1 \\ 0 & d & -s_2 c \\ 0 & -s_1 b & a \end{pmatrix}$$
$$\sim_{(2C)} \begin{pmatrix} 1 & 0 & s_2 \\ 0 & d & -cs_2 \\ 0 & -bs_2 & a \end{pmatrix} \sim_{(2R)} \begin{pmatrix} 1 & 0 & s_2 \\ c & d & 0 \\ -k_2 & -s_1 b & -1 \end{pmatrix}$$
$$\sim_{(2R)} \begin{pmatrix} -a & -sb & 0 \\ c & d & 0 \\ -k_2 & -s_1 b & -1 \end{pmatrix} \sim_{(2C)} \begin{pmatrix} -a & -sb & 0 \\ c & d & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

□

The proof is quantitative and we note that the current record is 37 for the number of elementary subgroups needed to express $\mathrm{SL}_3(\mathbb{Z})$ as a product, [Nic18].

We furthermore point out that there is a more conceptual approach to the problem using non-standard analysis that leads to proofs of bounded generation of $\mathrm{SL}_n(A)$, where A is a more general commutative ring. Indeed, it is easy to see that bounded generation of $\mathrm{SL}_n(A)$ is equivalent to **generation** of $\mathrm{SL}_n(A^*)$ by elementary subgroups of matrices with coefficients in A^*, where A^* is an ultrapower of A. This is related to K-theory and to the solution to the congruence subgroup problem, see [WM07].

6.2. **Non-uniform lattices.** In the previous section we showed that there are many examples of non-uniform lattices in higher rank Lie groups that are boundedly generated. Therefore the following recent result came as a surprise.

Theorem 6.5. *(*[CRRZ22]*) If K is a field of characteristic zero and let $\Gamma < \mathrm{GL}_n(K)$ be a subgroup with $n \geq 2$. Assume there are semisimple elements $\gamma_1, \ldots, \gamma_s \in \Gamma$ such that $\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_s \rangle$. Then Γ is virtually solvable.*

We remark in even more recent work [CDR+22] the conclusion is improved to Γ virtually abelian, and $(\overline{\Gamma}^Z)^\circ$ is shown to be a torus.

Corollary 6.6. *A uniform lattice in a semisimple Lie group is never boundedly generated.*

Proof. This follows since such groups only consist of semisimple elements. □

Without loss of generality we may assume that Γ is Zariski-connected since $[\Gamma : \Gamma^\circ] < \infty$. In these notes we furthermore reduce to the case that $K = \overline{\mathbb{Q}}$ and

$\overline{\Gamma}^Z = \mathrm{SL}_n$. For the analogous general case we refer to [CRRZ22]. The following is the main proposition. Recall the definition of Galois-generic elements from (5.4).

Proposition 6.7. *Let L be the field generated by the eigenvalues of $\gamma_1, \dots, \gamma_s$ and let $\gamma \in \Gamma$ be a Galois generic element over L. Then $\langle \gamma \rangle \cap \langle \gamma_1 \rangle \cdots \langle \gamma_s \rangle$ is finite.*

The proposition implies the theorem, because we know from the main result of Prasad-Rapinchuk proved in the previous lecture, Theorem 5.1, that there exist L-Galois generic elements in Γ and that they have infinite order as their eigenvalues are multiplicatively independent. We first show the following lemma.

Lemma 6.8. *If γ is L-Galois generic, then $A(\gamma) \cap L = \{1\}$, where $A(\gamma) \leq \mathbb{C}^\times$ is the multiplicative subgroup generated by the eigenvalues of γ.*

Proof. Recall that being L-Galois generic implies that the eigenvalues $\lambda_1(\gamma), \dots, \lambda_{n-1}(\gamma)$ are multiplicatively independent and $\mathrm{Gal}_L(P_\gamma) \cong \mathrm{Sym}(n)$. Therefore if $\lambda_1^{k_1} \cdots \lambda_n^{k_n} \in L$ for some $k_1, \dots, k_n \in \mathbb{Z}$ then $\lambda_1^{k_{\sigma(1)}} \cdots \lambda_n^{k_{\sigma(n)}} = \lambda_1^{k_1} \cdots \lambda_n^{k_n}$, which implies that all k_i's conincide by multiplicative independence. Thus $\lambda_1^{k_1} \cdots \lambda_n^{k_n} = (\lambda_1 \cdots \lambda_n)^{k_1} = 1$, implying the claim. □

The other key ingredient in the proof is Laurent's theorem.

Theorem 6.9. *(Laurent's theorem* [Lau84]*) Suppose $H \leq (\mathbb{G}_m(\overline{\mathbb{Q}}))^N$ is a finitely generated multiplicative subgroup and $\Sigma \subset H$ is any subset. Then $\overline{\Sigma}^Z$ is a finite union of cosets of subtori $T_i \leq (\mathbb{G}_m)^N$.*

The same statement holds if H is replaced by the torsion subgroup

$$H = \{(\omega_1, \dots, \omega_N) \in (\mathbb{G}_m)^N \text{ all } \omega_i \text{ are roots of unity}\}.$$

Indeed this is the so-called Manin-Mumford conjecture for $(\mathbb{G}_m)^N$. The general Manin-Mumford conjecture was proved by Raynaud [Ray83]. Laurent proved an even more general result, when H is an arbitrary subgroup of $(\mathbb{G}_m(\mathbb{C}))^N$ which is finitely generated modulo the torsion subgroup. This had been conjectured by S. Lang, who proved a special case [Lan83].

We note that Laurent's theorem over $\overline{\mathbb{Q}}$ is a rather simple consequence of Schmidt's subspace theorem, or rather its S-adic version due to Schlickewei. We refer to [BG06, Theorem 7.4.7] for the proof.

Proof. (of Proposition 6.7) Assume that $m \in \mathbb{Z}$ satisfies $\gamma^m \in \langle \gamma_1 \rangle \cdots \langle \gamma_s \rangle$. Then there are $a_1(m), \dots, a_s(m) \in \mathbb{Z}$ such that

$$\gamma^m = \gamma_1^{a_1(m)} \cdots \gamma_s^{a_s(m)}.$$

The element γ and the γ_i are diagonalizable, in particular in some basis of $(\overline{\mathbb{Q}})^n$, the $(1,1)$ entry satisfies

$$(\gamma^m)_{1,1} = \lambda_1(\gamma)^m = \left(\prod_{j=1}^{s} g_j D_j^{a_j(m)} g_j^{-1} \right)_{1,1}$$

for $D_i = \mathrm{diag}(\lambda_1(\gamma_1), \dots, \gamma_n(\gamma_i))$ and $g_i \in \mathrm{GL}_n(\overline{\mathbb{Q}})$. The right hand side has the form of a linear combination of monomials in $(\lambda_i(\gamma_j)^{a_j(m)})_{i,j}$, i.e. there is a polynomial $P \in \overline{\mathbb{Q}}[(x_{ij})_{ij}]$ such that

$$\lambda_1(\gamma)^m = P((\lambda_i(\gamma_j)^{a_j(m)})_{i,j}).$$

Take H to be the multiplicative subgroup of $\mathbb{C}^\times$ generated by $\lambda_1(\gamma)$ and the $\lambda_i(\gamma_j)$ and apply Laurent's theorem to $\Sigma = \{(x_m)_{m\in\mathbb{Z}}\}$ in $(\mathbb{G}_m)^N$, where $N = 1 + ns$ and

$$x_m = (\lambda_1(\gamma)^m, (\lambda_i(\gamma_j))^{a_j(m)}).$$

We conclude that $\overline{\Sigma}^Z = \bigcup x_i T_i$ for T_i tori. On the other hand $\overline{\Sigma}^Z$ is contained in the algebraic set $\{(y, (x_{ij})), y = P((x_{ij}))\}$.

If $\dim T_i > 0$, there are infinitely many m such that $x_m \in x_i T_i$ and hence there are distinct m and m' such that $x_m x_{m'}^{-1} \in T_i$. Yet T_i is a torus, so $T_i = \bigcap_\chi \ker \chi$ for a family of characters χ of $(\mathbb{G}_m)^N$ with $\chi(y, (x_{ij})_{i,j}) = y^{k_0} \prod_{i,j} x_{ij}^{k_{ij}}$ with $k_0, k_{ij} \in \mathbb{Z}$. So it follows that

$$\lambda_1(\gamma)^{(m-m')k_0} \prod_{i,j} \lambda_i(\gamma_j)^{(a_j(m)-a_j(m'))k_{i,j}} = 1.$$

Applying the lemma, since $\prod_{i,j} \lambda_i(\gamma_j)^{(a_j(m)-a_j(m'))k_{i,j}} \in L$, it follows that $k_0 = 0$. So T_i is invariant under multiplication by the first coordinate, i.e.

$$T_i = (y, 1)T_i$$

for all $y \in \overline{\mathbb{Q}}^\times$. Yet if $x_m \in x_i T_i$ then $\lambda_1(\gamma)^m = P(\lambda_i(\gamma_j)^{a_j(m)})$ so it can't be that $y\lambda_1(\gamma)^m = P(\lambda_i(\gamma_j)^{a_j(m)})$ for all y. This shows that $\dim T_i$ must be zero and therefore Σ is finite. □

We note that the above argument works just as well without assuming that Γ has algebraic entries, if we use instead the general version of Laurent's theorem (valid over $\mathbb{C}$).

We note that in [CDR+22], it is shown that any set of the form

$$\Sigma = \{(f_1(n), \dots, f_N(n)), n \in \mathbb{Z}^n\},$$

where each f_i is a purely exponential polynomial, i.e. $f_i(n)$ is a linear combination in $\overline{\mathbb{Q}}$ of monomials of the form $\mu_1^{n_1} \cdots \mu_r^{n_r}$ with $\mu_i \in \overline{\mathbb{Q}}^\times$ has the property that

$$\{n \in \mathbb{Z}^n, H(f(n)) \le H\} = O((\log H)^{O(1)}),$$

where $H(\cdot)$ is the height. This easily implies that boundedly generated groups with semisimple elements have polynomial growth, and then that the connected component of their Zariski closure is a torus.

6.3. **Exercises.**

6.3.1. A discrete group Γ is boundedly generated if and only if some (any) finite index subgroup of Γ is boundedly generated.

6.3.2. Every finitely generated nilpotent group is boundedly generated. Hint: Induct on the nilpotency step.

6.3.3. Show that the lamplighter group $\mathbb{Z} \wr \mathbb{Z}$ is not boundedly generated. Hint: Establish that $\mathbb{Z} \wr \mathbb{Z}$ is linear:

$$\begin{aligned}\mathbb{Z} \wr \mathbb{Z} &= \{(p, (a_n)_{n\in\mathbb{Z}}) \,:\, p \in \mathbb{Z} \text{ and } (a_n)_{n\in\mathbb{Z}} \in \mathbb{Z}^{(\mathbb{Z})}\} \\ &\cong \left\{ \begin{pmatrix} X^n & P(X) \\ 0 & 1 \end{pmatrix} \,:\, n \in \mathbb{Z} \text{ and } P \in \mathbb{Z}[X, X^{-1}] \right\}.\end{aligned}$$

6.3.4. Complete the proof of Lemma 6.4.

References

[AMS95] H. Abels, G. A. Margulis, and G. A. Soĭfer, *Semigroups containing proximal linear maps*, Israel J. Math. **91** (1995), no. 1-3, 1–30.

[BB21] V. Bharathram and J. Birman, *On the Burau representation of B_4*, Involve **14** (2021), no. 1, 143–154.

[BB90] N. L. Biggs and A. G. Boshier, *Note on the girth of Ramanujan graphs*, J. Combin. Theory Ser. B **49** (1990), no. 2, 190–194.

[Ben97] Y. Benoist, *Propriétés asymptotiques des groupes linéaires*, Geom. Funct. Anal. **7** (1997), no. 1, 1–47.

[BG03] E. Breuillard and T. Gelander, *On dense free subgroups of Lie groups*, J. Algebra **261** (2003), no. 2, 448–467.

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[BG07] E. Breuillard and T. Gelander, *A topological Tits alternative*, Ann. of Math. (2) **166** (2007), no. 2, 427–474.

[Big02] S. Bigelow, *Does the Jones polynomial detect the unknot?*, 2002, pp. 493–505. Knots 2000 Korea, Vol. 2 (Yongpyong).

[Bir74] J. S. Birman, *Braids, links, and mapping class groups*, Annals of Mathematics Studies, No. 82, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1974. MR0375281

[BL93] Y. Benoist and F. Labourie, *Sur les difféomorphismes d'Anosov affines à feuilletages stable et instable différentiables*, Invent. Math. **111** (1993), no. 2, 285–308.

[Bli17] H. F. Blichfeldt, *Finite collineation groups*, Monograph. The University of Chicago Press, 194 pp (1917). (1917), 194pp.

[Bor91] A. Borel, *Linear algebraic groups*, Graduate Texts in Mathematics, Springer New York, NY, 1991.

[Bre13] E. Breuillard, *Approximate subgroups and super-strong approximation*, Proceedings of Group St. Andrews Conference (2013).

[Cas76] J. W. S. Cassels, *An embedding theorem for fields*, Bull. Austral. Math. Soc. **14** (1976), no. 3, 479–480.

[Cas86] ———, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986.

[CDR+22] P. Corvaja, J. L. Demeio, A. S. Rapinchuk, J. Ren, and U. M. Zannier, *Bounded generation by semi-simple elements: quantitative results*, C. R. Math. Acad. Sci. Paris **360** (2022), 1249–1255.

[CK83] D. Carter and G. Keller, *Bounded elementary generation of* $\mathrm{SL}_n(O)$, Amer. J. Math. **105** (1983), no. 3, 673–687.

[Col07] M. J. Collins, *On Jordan's theorem for complex linear groups*, J. Group Theory **10** (2007), no. 4, 411–423.

[CRRZ22] P. Corvaja, A. S. Rapinchuk, J. Ren, and U. M. Zannier, *Non-virtually abelian anisotropic linear groups are not boundedly generated*, Invent. Math. **227** (2022), no. 1, 1–26.

[DdSMS99] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, Second, Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, Cambridge, 1999.

[ER06] I. V. Erovenko and A. S. Rapinchuk, *Bounded generation of S-arithmetic subgroups of isotropic orthogonal groups over number fields*, J. Number Theory **119** (2006), no. 1, 28–48.

[Fei64] W. Feit, *Groups which have a faithful representation of degree less than p*1, Trans. Amer. Math. Soc. **112** (1964), 287–303.

[GdM89] I. Ya. Gol′ dsheĭd and G. A. Margulis, *Lyapunov exponents of a product of random matrices*, Uspekhi Mat. Nauk **44** (1989), no. 5(269), 13–60.

[Gil08] J. Gilman, *The structure of two-parabolic space: parabolic dust and iteration*, Geom. Dedicata **131** (2008), 27–48.

[Gri80] R. I. Grigorčuk, *On Burnside's problem on periodic groups*, Funktsional. Anal. i Prilozhen. **14** (1980), no. 1, 53–54.

[Hum75] J. E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, No. 21, Springer-Verlag, New York-Heidelberg, 1975. MR0396773

[Isa76] M. Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, 1976.

[Ito15] T. Ito, *A kernel of a braid group representation yields a knot with trivial knot polynomials*, Math. Z. **280** (2015), no. 1-2, 347–353.

[JKZ13] F. Jouve, E. Kowalski, and D. Zywina, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, Israel J. Math. **193** (2013), no. 1, 263–307.

[JM13] K. Juschenko and N. Monod, *Cantor systems, piecewise translations and simple amenable groups*, Ann. of Math. (2) **178** (2013), no. 2, 775–787.

[Jor78] C. Jordan, *Mémoire sur les équations différentielles linéaires à intégrale algébrique*, J. Reine Angew. Math. **84** (1878), 89–215.

[KK22] S.-H. Kim and T. Koberda, *Non-freeness of groups generated by two parabolic elements with small rational parameters* (2022). `https://arxiv.org/pdf/1901.06375.pdf`.

[Kna02] A. W. Knapp, *Lie groups beyond an introduction*, Second, Progress in Mathematics, vol. 140, Birkhäuser Boston, Inc., Boston, MA, 2002. MR1920389

[Kur49] M. Kuranishi, *Two elements generations on semi-simple Lie groups*, Kodai Math. Sem. Rep. **1** (1949), no. 5-6, 9–10. {Volume numbers not printed on issues until Vol. **7**, (1955)}.

[Lan12] S. Lang, *Algebra*, Graduate Texts in Mathematics, Springer New York, NY, 2012.

[Lan83] ———, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983.

[Lau84] M. Laurent, *Équations diophantiennes exponentielles*, Invent. Math. **78** (1984), no. 2, 299–327.

[LP11] M. J. Larsen and R. Pink, *Finite subgroups of algebraic groups*, J. Amer. Math. Soc. **24** (2011), no. 4, 1105–1158.

[LPS86] A. Lubotzky, R. Phillips, and P. Sarnak, *Hecke operators and distributing points on the sphere. I*, 1986, pp. S149–S186. Frontiers of the mathematical sciences: 1985 (New York, 1985). MR861487

[LPS87] ———, *Hecke operators and distributing points on S^2. II*, Comm. Pure Appl. Math. **40** (1987), no. 4, 401–420. MR890171

[LPS88] ———, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277. MR963118

[LR14] A. Lubotzky and L. Rosenzweig, *The Galois group of random elements of linear groups*, Amer. J. Math. **136** (2014), no. 5, 1347–1383.

[LU69] R. C. Lyndon and J. L. Ullman, *Groups generated by two parabolic linear fractional transformations*, Canadian J. Math. **21** (1969), 1388–1403.

[Mar84] G. A. Margulis, *Arithmeticity of the irreducible lattices in the semisimple groups of rank greater than* 1, Invent. Math. **76** (1984), no. 1, 93–120. MR739627

[Mas65] B. Maskit, *On Klein's combination theorem*, Trans. Amer. Math. Soc. **120** (1965), 499–509.

[MRS18] A. V. Morgan, A. S. Rapinchuk, and B. Sury, *Bounded generation of SL_2 over rings of S-integers with infinitely many units*, Algebra Number Theory **12** (2018), no. 8, 1949–1974.

[Nic18] B. Nica, *On bounded elementary generation for SL_n over polynomial rings*, Israel J. Math. **225** (2018), no. 1, 403–410.

[Oš80] A. Ju. Ol′ šanskiĭ, *An infinite group with subgroups of prime orders*, Izv. Akad. Nauk SSSR Ser. Mat. **44** (1980), no. 2, 309–321, 479.

[OV80] A. Onishchick and E. Vinberg, *Lie groups and algebraic groups*, Springer New York, NY, 1980.

[PR03] G. Prasad and A. S. Rapinchuk, *Existence of irreducible $\mathbb{R}$-regular elements in Zariski-dense subgroups*, Math. Res. Lett. **10** (2003), no. 1, 21–32.

[PR05] ———, *Zariski-dense subgroups and transcendental number theory*, Math. Res. Lett. **12** (2005), no. 2-3, 239–249.

[PR17] G. Prasad and A. S. Rapinchuk, *Generic elements of a Zariski-dense subgroup form an open subset*, Trans. Moscow Math. Soc. **78** (2017), 299–314.

[PR94] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

[Pra94] G. Prasad, **R**-*regular elements in Zariski-dense subgroups*, Quart. J. Math. Oxford Ser. (2) **45** (1994), no. 180, 541–545.

[Rag72] M. S. Raghunathan, *Discrete subgroups of Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 68, Springer-Verlag, New York-Heidelberg, 1972.

[Ray83] M. Raynaud, *Sous-variétés d'une variété abélienne et points de torsion*, Arithmetic and geometry, Vol. I, 1983, pp. 327–352.

[Rob] G. Robinson, *Finite subgroups of* U(2). URL:https://mathoverflow.net/q/389807 (version: 2021-04-11).

[Sel60] A. Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*, Contributions to function theory (Internat. Colloq. Function Theory, Bombay, 1960), 1960, pp. 147–164.

[Tit72] J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.

[Wag85] S. Wagon, *The Banach-Tarski paradox*, Encyclopedia of Mathematics and its Applications, vol. 24, Cambridge University Press, Cambridge, 1985. With a foreword by Jan Mycielski. MR803509

[Wed34] J. Wedderburn, *Lectures on matrices*, American Mathematical Society Providence, Rhode Island, 1934.

[WM07] D. Witte Morris, *Bounded generation of* $\mathrm{SL}(n, A)$ *(after D. Carter, G. Keller, and E. Paige)*, New York J. Math. **13** (2007), 383–421.