STRONG APPROXIMATION FOR ALGEBRAIC GROUPS

ANDREI S. RAPINCHUK

Contents

Main references – [26, Ch. VII], [39].

1. The notion of strong approximation

The idea of strong approximation goes back to congruences and the Chinese Remainder Theorem. To keep things simple, let us consider a family of polynomials

$$f_\alpha(x_1, \ldots, x_d) \in \mathbb{Z}[x_1, \ldots, x_d], \quad \alpha \in I,$$

and let $X \subset \mathbb{A}^d_{\mathbb{Z}}$ be the closed subscheme defined by these equations. Thus, for a $\mathbb{Z}$-algebra R we have the set of R-points

$$X(R) = \{(a_1, \ldots, a_d) \in R^d \mid f_\alpha(a_1, \ldots, a_d) = 0 \ \text{ for all } \ \alpha \in I\}.$$

For any integer $m \geqslant 1$ we have the reduction modulo m map

$$\rho_m \colon X(\mathbb{Z}) \longrightarrow X(\mathbb{Z}/m\mathbb{Z}).$$

We can then ask the following

Question. *(When) are the maps ρ_m surjective for all m?*

If all ρ_m's are surjective, we say that X has *strong approximation* – this provisional definition will soon be reformulated using adeles. Strong approximation trivially holds for $X = \mathbb{A}^d$ (no equations), but as we will see it may or may not hold in a more general situation. In fact, as we will see, there are many obstructions for this property to hold. As a result, it actually holds quite rarely, however it does hold in some important situations (particularly, for some algebraic groups and homogeneous spaces) in which case we get a number of useful consequences.

For now though let us reformulate this property in a way that will lead to the adelic formulation. Note that for $m|n$, there is a natural projection $X(\mathbb{Z}/n\mathbb{Z}) \to X(\mathbb{Z}/m\mathbb{Z})$, so we can form the inverse limit

$$\lim_{\leftarrow} X(\mathbb{Z}/m\mathbb{Z}).$$

Furthermore, this set can be identified with the set of points $X(\widehat{\mathbb{Z}})$ over the completion $\widehat{\mathbb{Z}} = \lim\limits_{\leftarrow} \mathbb{Z}/m\mathbb{Z}$. There are reduction modulo m maps

$$\widehat{\rho}_m \colon X(\widehat{\mathbb{Z}}) \longrightarrow X(\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}}) = X(\mathbb{Z}/m\mathbb{Z}),$$

and the preimages of points form a base for the natural topology on $X(\widehat{\mathbb{Z}})$ (which can be described either as the topology of the inverse limit or the topology induced by the embedding $X(\widehat{\mathbb{Z}}) \hookrightarrow \widehat{\mathbb{Z}}^d$). This leads us to the following equivalence

$$\boxed{\text{maps } \rho_m \text{ are surjective for all } m \geqslant 1} \;\Leftrightarrow\; \boxed{\text{embedding } X(\mathbb{Z}) \hookrightarrow X(\widehat{\mathbb{Z}}) \text{ is } \textit{dense}}$$

Using the Chinese Remainder Theorem, we can naturally identify $\widehat{\mathbb{Z}}$ with the product $\prod_p \mathbb{Z}_p$ (over all primes p). So, the last condition is equivalent to the fact that the embedding

$$X(\mathbb{Z}) \hookrightarrow \prod_p X(\mathbb{Z}_p)$$

is dense - the point here is that this condition easily lends itself to the generalization in terms of adeles. It also exhibits situations where X cannot possibly have strong approximation. For example, there are example where $X(\mathbb{Z}_p) \neq \emptyset$ for all p but $X(\mathbb{Z}) = \emptyset$ (in other words, X fails the Hasse principle), in which case of course it cannot possibly have "strong approximation" (the same happens when $X(\mathbb{Z})$ is "small"). In these lectures, we will be dealing with primarily with algebraic groups where the set of $\mathbb{Z}$-points is never empty, but here "strong approximation" is not automatic either as the following example shows.

Example. $\underline{\mathrm{SL}_2 \text{ vs. } \mathrm{GL}_2.}$ The groups $G_1 = \mathrm{SL}_2$ and $G_2 = \mathrm{GL}_2$ can be realized as *hypersurfaces* in the affine spaces, viz.

$$G_1 = \{(x_{11}, x_{12}, x_{21}, x_{22}) \in \mathbb{A}^4 \mid x_{11}x_{22} - x_{12}x_{21} = 1\}$$

and

$$G_2 = \{(x_{11}, x_{12}, x_{21}, x_{22}, y) \in \mathbb{A}^5 \mid (x_{11}x_{22} - x_{12}x_{21})y = 1\}.$$

One doesn't really see much of a difference between the defining equation, however G_1 has "strong approximation" but G_2 doesn't. (We should point out that the reason is *not* the fact that G_1 is defined by quadratic equations, and G_2 by cubic: the group SL_3 is defined by a single *cubic* equation but *does* have strong approximation.)

Lemma 1.1. *The reduction modulo m map*

$$\rho_m \colon \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$$

is surjective, for any $m \geqslant 1$.

Sketch of proof. We will not work with the defining equation but rather use some structural information about SL_2. The crucial observation is that any $\bar{g} \in \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ can be written in the form

$$\bar{g} = \prod_{k=1}^{\ell} e_{i_k j_k}(\bar{a}_k) \quad \text{with} \quad (i_k, j_k) \in \{(1,2),(2,1)\} \text{ and } \bar{a}_k \in \mathbb{Z}/m\mathbb{Z},$$

where $e_{ij}(a)$ denotes the elementary matrix having a as its (ij)-entry (exercise!). Suppose we are given such a $\bar{g}$, and then find a factorization as above. Then picking an integer a_k in the class $\bar{a}_k$ modulo m, we see that

$$g := \prod_{k=1}^{\ell} e_{i_k j_k}(a_k)$$

satisfies $\rho_m(g) = \bar{g}$. Thus, ρ_m is surjective. □

(This entirely elementary argument obviously extends to $\mathrm{SL}_n(\mathbb{Z})$ for any $n \geqslant 2$, but more generally shows that proving strong approximation is easy if there are unipotent elements available.)

It is even easier to see that GL_2 does not have strong approximation. In fact, already the map

$$\rho_5 \colon \mathrm{GL}_2(\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

is not surjective. Indeed, the determinant of any matrix in the image of ρ_5 is $\pm 1 (\mathrm{mod}\, 5)$, implying that, for example, the matrix $\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}$ does not lie in the image. A more conceptual way to express the reason for failure of strong approximation in this case is contained in the following statement.

Lemma 1.2. *If X as above has strong approximation as defined above (i.e. $X(\mathbb{Z})$ is dense in $\prod_p X(\mathbb{Z}_p)$) then $X(\mathbb{Z})$ is Zariski-dense in X.*

Sketch of proof. Let Y be the Zariski-closure of $X(\mathbb{Z})$, and assume that $Y \neq X$. Then one can find a point $a \in X(\bar{\mathbb{Q}}) \setminus Y(\bar{\mathbb{Q}})$ (where $\bar{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$). It follows from Chebotarev's Density Theorem (cf. Proposition 2.4) that there exist infinitely many primes p for which $a \in X(\mathbb{Z}_p)$; fix one such prime p. Then $X(\mathbb{Z}_p) \setminus Y(\mathbb{Z}_p)$ is a nonempty open set in $X(\mathbb{Z}_p)$ that has empty intersection with $X(\mathbb{Z})$. □

We note that the (nontrivial) equation $(\det x)^2 - 1$ vanishes on $\mathrm{GL}_2(\mathbb{Z})$, so it is *not* Zariski-dense in GL_2. We can fix the lack of Zariski-density by passing from $\mathbb{Z}$ to some localization, e.g. $\mathbb{Z}[1/2]$. Then $\Gamma = \mathrm{GL}_2(\mathbb{Z}[1/2])$ is already Zariski-dense in GL_2. (Exercise. Prove this. (*Hint.* Observe that the Zariski closure $\bar{\Gamma}$ contains SL_2 and has infinite image in $\mathrm{GL}_2/\mathrm{SL}_2 = \mathbb{G}_m$.)) So, one may wonder if we have the natural analog of strong approximation in this situation, viz. whether the embedding

$$\Gamma \hookrightarrow \prod_{p \neq 2} \mathrm{GL}_2(\mathbb{Z}_p)$$

is dense. As we have just seen, for the group $\mathrm{GL}_2(\mathbb{Z})$ itself, already the reduction map ρ_5 modulo 5 was not surjective. It turns out that for Γ we have $\rho_5(\Gamma) = \mathrm{GL}(\mathbb{Z}/5\mathbb{Z})$ (and in fact, Γ is dense in $\mathrm{GL}_2(\mathbb{Z}_5)$). However, $\rho_{17}(\Gamma) \neq \mathrm{GL}_2(\mathbb{Z}/17\mathbb{Z})$ (and hence Γ is *not* dense in $\mathrm{GL}_2(\mathbb{Z}_{17})$). The reason is that the determinants of matrices in Γ are all of the form $\pm 2^{\ell}$, $\ell \in \mathbb{Z}$, and since -1 and 2 are both squares modulo 17, the determinants of matrices in $\rho_{17}(\Gamma)$ are contained in $(\mathbb{Z}/17)^{\times 2} \neq (\mathbb{Z}/17)^{\times}$. The same argument shows that Γ is not dense in $\mathrm{GL}_2(\mathbb{Z}_p)$ for any prime $p \equiv 1 (\mathrm{mod}\, 8)$, implying that the closure of Γ in $\prod_{p \neq 2} \mathrm{GL}_2(\mathbb{Z}_p)$ has *infinite* index.

Let us now give an example of the opposite nature. Consider the subgroup $\Delta \subset \mathrm{SL}_2(\mathbb{Z})$ generated by the matrices

$$\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

Then Δ has infinite index in $\mathrm{SL}_2(\mathbb{Z})$ but is still Zariski-dense in SL_2. (Exercise. Prove this. (*Hint.* To prove that the index is infinite, use the fact that the matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ generated a free subgroup.)) On the other hand, repeating the argument given in the proof of Lemma 1.2, one shows that the embedding

$$\Delta \hookrightarrow \prod_{p \neq 2} \mathrm{SL}_2(\mathbb{Z}_p)$$

is dense, and in fact the closure of Δ in $\prod_p \mathrm{SL}_2(\mathbb{Z}_p) = \mathrm{SL}_2(\widehat{\mathbb{Z}})$ has finite index. One can use some advanced results to give examples of infinite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that are actually dense in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. For example, according to a result of Margulis-Soifer [17], the group $\mathrm{SL}_n(\mathbb{Z})$ for any $n \geqslant 2$ has a continuum of maximal subgroups of infinite index. Such subgroups are automatically dense in $\mathrm{SL}_n(\mathbb{Z})$ in the profinite topology, and therefore are also dense in $SL_n(\widehat{\mathbb{Z}})$. These subgroups are infinitely generated, but one can first pick a finitely generated subgroup which is Zariski-dense and then using the approximation theorems of Matthews-Vaserstein-Weisfeiler [18] and Weisfeiler [46] (cf. §6) to conclude that the closure of this finitely generated subgroup in $\mathrm{SL}_n(\widehat{\mathbb{Z}})$ has finite index. After that we can add more elements to create a finitely generated subgroup which is dense in $\mathrm{SL}_n(\widehat{\mathbb{Z}})$ (this subgroup will be contained in a subgroup of infinite index in $\mathrm{SL}_n(\mathbb{Z})$, and therefore will itself have infinite index). See Soifer-Venkataramana [43] for more sophisticated constructions (they show, in particular, that $\mathrm{SL}_n(\mathbb{Z})$ for $n \geqslant 3$ contains a finitely generated *free* subgroup that is dense in the profinite topology; we note that this construction cannot be implemented in $\mathrm{SL}_2(\mathbb{Z})$ since the latter is virtually free, and in a free group every finitely generated subgroup is closed in the profinite topology).

These two examples show that there may be situations where an arithmetic or S-arithmetic group is Zariski-dense but still fails strong approximation, and there are also situations where a Zariski-dense subgroup that has *infinite index* in an arithmetic subgroup does have strong approximation. In order to address these and other phenomena pertaining to strong approximation systematically, we will now give steer the discussion in the adelic setting.

Adeles and strong approximation. Since we are mainly interested in strong approximation for (linear) algebraic groups, we will first give the definitions in this case. Given a global field K, we let V^K denote the set of all (equivalence classes of) valuations of K, and let V_∞^K and V_f^K denote the subsets of archimedean and nonarchimedean valuations. Let G be a (linear) algebraic K-group. First, let us fix a faithful linear K-representation (matrix realization) $G \hookrightarrow \mathrm{GL}_n$ which enables us to define unambiguously the groups

$$G(\mathcal{O}_v) = G \cap \mathrm{GL}_n(\mathcal{O}_v) \ \text{ for all } \ v \in V_f^K,$$

where $\mathcal{O}_v$ is the valuation ring in the completion K_v. For a given subset $S \subset V^K$, we let $\mathbb{A}_S$ denote the ring of S-adeles of the field K, and define the group of S-adeles of G as follows:

$$G(\mathbb{A}_S) = \{g = (g_v) \in \prod_{v \in V^K \setminus S} G(K_v) \mid g_v \in G(\mathcal{O}_v) \ \text{ for almost all } \ v \notin S\}$$

("restricted direct product" of the groups $G(K_v)$ for $v \in V^K \setminus S$ with respect to the distinguished subgroups $G(\mathcal{O}_v)$ for $v \in V^K \setminus (S \cup V_\infty^K)$). The group $G(\mathbb{A}_S)$ is endowed with the natural topology ("restricted direct product" topology) which is uniquely characterized by the fact that the subgroup

$$\prod_{v \in V_\infty^K \setminus S} G(K_v) \times \prod_{v \in V_f^K \setminus S} G(\mathcal{O}_v)$$

is open and the induced adelic topology on it coincides with the the product topology. It now should be noted that while the topological group $G(\mathbb{A}_S)$ was defined using a certain *fixed* matrix realization of G, it actually is independent of the choice of this realization, viz. a different matrix realization results in a naturally isomorphic group. Furthermore, we have the diagonal embedding $G(K) \hookrightarrow G(\mathbb{A}_S)$.

Definition. *We say that the K-group G has* strong approximation *with respect to the set of places (valuations) S if $G(K)$ is dense in $G(\mathbb{A}_S)$.*

Let us now clarify how this definition of strong approximation relates to the provisional version we discussed earlier. Tke $K = \mathbb{Q}$ and $S = \{\infty\}$. Suppose G has strong approximation in the sense of the above adelic definition, i.e. $G(\mathbb{Q})$ is dense in $G(\mathbb{A}_S)$. Then, since the subgroup

$$\prod_p G(\mathbb{Z}_p) \subset G(\mathbb{A}_S)$$

is open, the intersection

$$G(\mathbb{Q}) \cap \prod_p G(\mathbb{Z}_p) = G(\mathbb{Z})$$

must be dense in $\prod_p G(\mathbb{Z}_p) = G(\widehat{\mathbb{Z}})$. Thus, strong approximation in the adelic sense implies strong approximation in the previous sense for *any* matrix realization $G \hookrightarrow \mathrm{GL}_n$.

As we stated earlier, in these lectures we are mostly interested in strong approximation for algebraic groups, but for the sake of completeness let us mention very briefly how the notion of adeles, hence that of strong approximation, generalizes to arbitrary varieties. The generalization to affine varieties is completely straightforward. Namely, for a K-defined affine variety X we first fix a closed K-embedding $X \hookrightarrow \mathbb{A}^n$ which allows us to talk unambiguously about $X(\mathcal{O}_v)$ for $v \in V_f^K$, and then define $X(\mathbb{A}_S)$

as the restricted product of $X(K_v)$ for $v \in V^K \setminus S$ relative to $X(\mathcal{O}_v)$ for $v \in V^K \setminus (S \cup V_\infty^K)$ just as above, i.e.

$$X(\mathbb{A}_S) = \{x = (x_v) \in \prod_{v \in V^K \setminus S} X(K_v) \mid x_v \in X(\mathcal{O}_v) \ \text{ for almost all } \ v \in V^K \setminus (S \cup V_\infty^K)\}.$$

One then show that $X(\mathbb{A}_S)$ is independent of the choice of a closed embedding $X \hookrightarrow \mathbb{A}^n$.

The definition of adeles for non-affine varieties is more involved (see Weil [45]). Let X be an algebraic variety defined over a global field K. Then X admits a finite covering by K-open affine subsets:

$$X = \bigcup_{i=1}^{d} X_i,$$

and for each i we fix a K-isomorphism $f_i \colon U_i \to X_i$, where U_i is a closed K-subvariety of some affine space. Then $X(K) = \bigcup f_i(U_i(K))$ and $X(K_v) = \bigcup f_i(U_i(K_v))$ for all v (in particular, $X(K_v)$ is locally compact for the natural topology that extends the usual topology on each $U_i(K_v)$). For $v \in V_f^K$ we set

$$[X, f_i, U_i](\mathcal{O}_v) = \bigcup f_i(U_i(\mathcal{O}_v)).$$

One shows that if

$$X = \bigcup_j Y_j, \quad g_j \colon W_j \to Y_j$$

is another finite open covering by K-open affine subsets with K-isomorphisms g_j, then

$$[X, f_i, U_i](\mathcal{O}_v) = [X, g_j, W_j](\mathcal{O}_v) \ \text{ for almost all } \ v \in V_f^K.$$

This means that the spaces of S-adeles

$$X(\mathbb{A}_S) := \{x = (x_v) \in \prod_{v \in V^K \setminus S} X(K_v) \mid x_v \in [X, f_i, U_i](\mathcal{O}_v) \ \text{ for almost all } v \in V^K \setminus (S \cup V_\infty^K)\}$$

does not depend on the choice of a finite open affine covering or a system of isomorphisms. See B. Conrad [9] for a discussion of various aspects this definition, and in particular of the fact that its outcome coincides with the set of points of X over $\mathbb{A}_S$ (i.e. morphisms $\mathrm{Spec}(\mathbb{A}_S) \to X$ as K-schemes) as sets and also topological spaces.

We would like to observe for using the standard affine covering of the projective space $X = \mathbb{P}^n$, one finds that $X(\mathcal{O}_v) = X(K_v)$ for any $v \in V_f^K$. It follows that for any projective K-variety X we have $X(\mathcal{O}_v) = X(K_v)$ for almost all $v \in V_f^K$, and therefore the (topological) space of S-adeles $X(\mathbb{A}_S)$ coincides with the direct product $\prod_{v \in V^K \setminus S} X(K_v)$. This means that in this case strong approximation for S becomes identical to weak approximation for $V^K \setminus S$. For convenience, we recall the definition of weak approximation.

Definition. *Let X be an algebraic variety defined over an arbitrary field K, and let V be a set of valuations of K. We say that X has* weak approximation *with respect to V if $X(K)$ is dense in $\prod_{v \in V} X(K_v)$ for the direct product topology.*

We note that X as weak approximation with respect to V if and only if it has weak approximation with respect to every finite subset $T \subset V$. Returning now to the situation where K is a global field, we can now clarify the difference between weak and strong approximation: the former for $V^K \setminus S$ means the density in $\prod_{v \in T} X(K_v)$, for any finite subset $T \subset V^K \setminus S$, of $X(K)$, while the latter means the density in $\prod_{v \in T} X(K_v)$, for any finite subset $T \subset V^K \setminus S$ such that $S \cup T \supset V_\infty^K$, of $X(\mathcal{O}(S \cup T))$, where $\mathcal{O}(S \cup T)$ is the ring of $(S \cup T)$-integers in K. (Thus, strong approximation means the possibility to approximate the elements of $\prod_{v \in T} X(K_v)$ not only by *some* elements of $X(K)$, but in fact by those that are integral outside $S \cup T$.) Of course, this difference originates from the fact that the adelic topology on $X(\mathbb{A}_S)$ is *stronger* than the topology induced from the direct product $\prod_{v \in V^K \setminus S} X(K_v)$.

2. Necessary conditions for strong approximation

We will now discuss a bunch of necessary conditions for strong approximation. In formulating these conditions we will assume (unless we explicitly state otherwise) that the K-variety X at hand is affine and the set $S \subset V^K$ of valuations that we discard is finite. At the end of the section, we will make some remarks for some special *infinite* sets S. As we already observed, one necessary condition (for any X, not necessarily affine) is

- $X(K)$ must be Zariski-dense in X.

The next condition is absolute irreducibility.

- X must be absolutely irreducible.

Sketch of proof. Recall that the irreducible components of a K-variety are defined over its separable closure [3, AG 12.3]. So, if X is not absolutely irreducible, we can write $X = X_1 \cup X_2$ where X_1 and X_2 are proper closed subsets defined over some finite separable extension L/K. Enlarging L we may assume that $X_i(L) \neq X(L)$ for both $i = 1, 2$. It follows from Chebotarev's Density Theorem (cf. Proposition 2.4 below) that one can find $v_1, v_2 \in V^K \setminus S$ such that $L \subset K_{v_i}$ for $i = 1, 2$. Set

$$U_{v_i} = X(K_{v_i}) \setminus X_i(K_{v_i}) \quad \text{for} \quad i = 1, 2.$$

Then U_{v_i} is a nonempty open subset of $X(K_{v_i})$ and

$$X(K) \cap (U_{v_1} \times U_{v_2}) = \emptyset,$$

a contradiction. □

So, we will assume henceforth that X is absolutely irreducible.

Next, it is well-known that K is *discrete* in the ring of *full adeles* $\mathbb{A}$ (for $S = \emptyset$), cf. [1, Ch. II, §14]. It follows that if X is affine, then $X(K)$ is discrete (and closed) in $X(\mathbb{A})$ (this is typically false for X nonaffine!). So, strong approximation can never hold in the affine case for $S = \emptyset$ (unless X is a single point). Let us take this one step further. Recall the following elementary topological lemma.

Lemma 2.1. *Let C and D be Hausdorff topological spaces with C compact, and let $\pi\colon C \times D \to D$ be the projection.*

(1) *If $E \subset C \times D$ is closed then $\pi(E)$ is also closed.*

(2) *If $E \subset C \times D$ is closed and discrete then $\pi(E)$ is also closed and discrete.*

To apply this in our situation, we observe that for S finite, we have an isomorphism of topological rings

$$\mathbb{A} = K_S \times \mathbb{A}_S \quad \text{where} \quad K_S = \prod_{v \in S} K_v.$$

This yields a homeomorphism of topological spaces

$$X(\mathbb{A}) \simeq X(K_S) \times X(\mathbb{A}_S).$$

Since $X(K)$ is closed and discrete in $X(\mathbb{A})$, applying Lemma 2.1 we see that if $X(K_S)$ is compact then the image of the diagonal embedding $X(K) \hookrightarrow X(\mathbb{A}_S)$ is closed and discrete. It follows that X cannot have strong approximation in this case. We can thus point out another necessary condition for strong approximation (in the affine case).

- $X(K_S)$ must be noncompact (i.e. there should exist $v \in S$ such that $X(K_v)$ is noncompact).

To our knowledge, there is no criterion for $X(K_v)$ to be noncompact for general affine varieties but there is the following result for algebraic groups.

Theorem 2.2. (Borel-Tits [4,]) *Let $\mathcal{G}$ be a reductive algebraic group over a locally compact field $\mathcal{K}$ of characteristic zero. Then the group $\mathcal{G}(\mathcal{K})$ is compact if and only if $\mathcal{G}$ is anisotropic over $\mathcal{K}$ (i.e. contains no nontrivial $\mathcal{K}$-split torus).*

Sketch of proof. The implication

$$\mathcal{G}(\mathcal{K}) \textit{ is compact} \Rightarrow \mathcal{G} \textit{ is } \mathcal{K}\textit{-anisotropic}$$

is totally obvious as for a nontrivial $\mathcal{K}$-split torus $\mathcal{S}$ the group $\mathcal{S}(\mathcal{K})$ is noncompact. For the opposite implication, we use Chevalley's theorem to find a faithful $\mathcal{K}$-defined representation $G \hookrightarrow \mathrm{GL}(V)$ such that there exists $v \in V(K)$ for which the stabilizer of the line $V_1 = \langle v \rangle$ reduces to the trivial group $\{e\}$. Consider some $\mathcal{K}$-defined flag

$$\mathcal{F}: \quad V_1 \subset V_2 \subset \cdots \subset V_n = V, \quad \text{where} \quad \dim V_i = i.$$

Let $\mathcal{F}(V)$ be the flag variety associated with V. We then consider the orbit morphism

$$f\colon G \to \mathcal{F}(V), \quad g \mapsto g\mathcal{F}.$$

Let $Z = \overline{f(\mathcal{G})}$ be the Zariski closure of the orbit $X = f(\mathcal{G}) = \mathcal{G}\mathcal{F}$. Since $\mathcal{F}(V)$ is projective, the space $\mathcal{F}(V)(\mathcal{K})$ is compact. Since $Z(\mathcal{K})$ is closed in $\mathcal{F}(V)(\mathcal{K})$, it is also compact. Since the stabilizer of V_1, hence of $\mathcal{F}$, is trivial, f yields a $\mathcal{K}$-defined isomorphism between $\mathcal{G}$ and the Zariski $\mathcal{K}$-open set $X \subset Z$. In particular, $f_{\mathcal{K}}$ defines a homeomorphism between $\mathcal{G}(\mathcal{K})$ and $X(\mathcal{K})$. So, to prove that $\mathcal{G}(\mathcal{K})$ is compact, it is enough to prove that $X(\mathcal{K}) = Z(\mathcal{K})$, in other words, to prove the inclusion $Z(\mathcal{K}) \subset X$. Assume that there exists $\mathcal{F}' \in Z(\mathcal{K}) \setminus X$. Then the orbit $\mathcal{G}\mathcal{F}'$ has a strictly smaller dimension than X. This means that the stabilizer $\mathcal{H}$ of $\mathcal{F}'$ in $\mathcal{G}$ has positive dimension. On the other hand, $\mathcal{H}$ stabilizes the $\mathcal{K}$-flag $\mathcal{F}'$, hence is triangulizable over $\mathcal{K}$. But since $\mathcal{G}$ is $\mathcal{K}$-anisotropic, it cannot contain any such subgroups. □

Remark. Theorem 2.2 remains valid in positive characteristic. An elegant and simple proof was given by Prasad [28]. Prasad shows that if $\mathcal{G}(\mathcal{K})$ is not compact, then $\mathcal{G}(\mathcal{K})$ contains an element that has an eigenvalue which is not a unit. Without loss of generality we may suppose that this element is semi-simple (in characteristic $p > 0$ one needs to raise this element to some power to kill the unipotent part), hence lies in a $\mathcal{K}$-torus. But then this torus cannot be $\mathcal{K}$-anisotropic since for a $\mathcal{K}$-anisotropic torus $\mathcal{T}$, the group $\mathcal{T}(\mathcal{K})$ is easily shown to be compact.

A deeper necessary condition for strong approximation is the simply connectedness. We begin with the case of algebraic groups, and for simplicity we will treat only the case of number fields.

Theorem 2.3. *Let G be a connected reductive algebraic group over a number field K. If there exists a nontrivial K-defined isogeny $\pi\colon \widetilde{G} \to G$ (i.e. $\widetilde{G}$ is connected and π is surjective with finite kernel). Then G does not have strong approximation with respect to any finite set of places $S \subset V^K$.*

Before we sketch the proof, we would like to formulated one consequence of Chebotarev's Density Theorem [1, Ch. VII, 2.4] which for number fields can be proved by elementary techniques (i.e. without any use of L-functions).

Proposition 2.4. *Let L/K be a finite extension of number fields. Then there exists infinitely many $v \in V^K$ such that for any extension $w|v$ we have $L_w = K_v$.*

Exercise. Prove this. It is enough to consider the case $K = \mathbb{Q}$ and L/K a Galois extension. Write $L = \mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial of α. We may assume without loss of generality that $f(x) \in \mathbb{Z}[x]$. Assume that the assertion is false, and show that then the values $f(n)$, $n \in \mathbb{Z}$, are divisible only by finitely many primes. Show that the latter is impossible.

Sketch of proof of Theorem 2.3. Without loss of generality, we may assume that S contains the set of archimedean places V_∞^K. If G has strong approximation with respect to S, i.e. $G(K)$ is dense in $G(\mathbb{A}_S)$, then

$$G(\mathcal{O}_S) = G(K) \cap \prod_{v \in V^K \setminus S} G(\mathcal{O}_v)$$

is dense in $\prod_{v \in V^K \setminus S} G(\mathcal{O}_v)$ (where $\mathcal{O}_S$ is the ring of S-integers in K); in particular, $G(\mathcal{O}_S)$ is dense in $G(\mathcal{O}_v)$ for every $v \in V^K \setminus S$. It is known that $\Gamma := G(\mathcal{O}_S)$ is a finitely generated group [26, Theorem 5.11], say $\Gamma = \langle \gamma_1, \ldots, \gamma_r \rangle$. Given $\gamma \in G(K)$, we pick $\tilde{\gamma} \in \widetilde{G}(\bar{K})$ so that $\pi(\tilde{\gamma}) = \gamma$, and then find a finite extension $L(\gamma)/K$ for which $\tilde{\gamma} \in \widetilde{G}(L(\gamma))$. Picking such an extension for each of the generators γ_i and using the fact that $F := \ker \pi$ is finite, we can construct a finite Galois extension L/K such that $\pi^{-1}(\Gamma) \subset \widetilde{G}(L)$ (in particular, $F \subset \tilde{G}(L)$).

Next, we can find a finite subset $T \subset V^K$ containing S so that for every $v \in V^K \setminus T$ the following properties hold:

(a) π can be reduced modulo v to an isogeny $\underline{\pi}^{(v)} \colon \widetilde{\underline{G}}^{(v)} \to \underline{G}^{(v)}$ of (smooth) connected groups;

(b) F maps injectively into $\widetilde{\underline{G}}^{(v)}$;

(c) $\pi^{-1}(\Gamma) \subset \widetilde{G}(\mathcal{O}_{L_w})$ for all $w|v$.

By Proposition 2.4, we can find $v \in V^K \setminus T$ such that $L_w = K_v$ for all $w|v$. Then in view of (3) we have

$$\pi^{-1}(\Gamma) \subset \widetilde{G}(\mathcal{O}_{L_w}) \cap \widetilde{G}(K_v) = \widetilde{G}(\mathcal{O}_v),$$

and consequently $\Gamma \subset \pi(\widetilde{G}(\mathcal{O}_v))$. Since $\widetilde{G}(\mathcal{O}_v)$ is compact, the closure of Γ is also contained in $\pi(\widetilde{G}(\mathcal{O}_v))$. So, it remains to show that

$$\pi(\widetilde{G}(\mathcal{O}_v)) \neq G(\mathcal{O}_v). \tag{1}$$

Let $k(v)$ be the residue field. We then have the following commutative diagram

$$\begin{tikzcd}
\widetilde{G}(\mathcal{O}_v) \arrow[r, "\pi"] \arrow[d] & G(\mathcal{O}_v) \arrow[d] \\
\widetilde{\underline{G}}^{(v)}(k(v)) \arrow[r, "\underline{\pi}^{(v)}"] & \underline{G}^{(v)}(k(v))
\end{tikzcd}.$$

The vertical arrows, which are the reduction maps, are surjective by Hensel's lemma since the reductions are smooth. So, to prove (1), it is enough to establish

$$\underline{\pi}^{(v)}(\widetilde{\underline{G}}^{(v)}(k(v))) \neq \underline{G}^{(v)}(k(v)). \tag{2}$$

But according to Lang's Theorem, isogenous connected groups over a finite field contain the same number of points. On the other hand,

$$\left|\underline{\pi}^{(v)}(\widetilde{\underline{G}}^{(v)}(k(v)))\right| = \frac{|\widetilde{\underline{G}}^{(v)}(k(v))|}{|\underline{F}^{(v)}(k(v))|} < |\widetilde{\underline{G}}^{(v)}(k(v))|$$

because $\underline{F}^{(v)}(k(v))$ contains the image of F in $\tilde{\underline{G}}^{(v)}(k(v))$, hence nontrivial due to condition (b) above. Another way to phrase the same argument is consider the exact sequence

$$1 \to \underline{F}^{(v)} \longrightarrow \widetilde{\underline{G}}^{(v)} \longrightarrow \underline{G}^{(v)} \to 1,$$

and the corresponding cohomological sequence:

$$\widetilde{\underline{G}}^{(v)}(k(v)) \xrightarrow{\pi} \underline{G}^{(v)}(k(v)) \longrightarrow H^1(k(v), \underline{F}^{(v)}) \longrightarrow H^1(k(v), \widetilde{\underline{G}}^{(v)}).$$

Since $\widetilde{\underline{G}}^{(v)}$ is connected, $H^1(k(v), \widetilde{\underline{G}}^{(v)})$ vanishes by Lang's Theorem. On the other hand, since the absolute Galois group of $k(v)$ is $\widehat{\mathbb{Z}}$, we have

$$|H^1(k(v), \underline{F}^{(v)})| = |H^0(k(v), \underline{F}^{(v)})| = |\underline{F}^{(v)}(k(v))| > 1$$

as above, yielding (2).

(Regarding the fact, used in the proof, that for G reductive the group $G(\mathcal{O}_S)$ is finitely generated, we observe that it remains valid in positive characteristic when $\mathrm{rk}_S\, G := \sum_{v \in S} \mathrm{rk}_{K_v} \geqslant 2$, see [2], [8].)

An analog of this theorem is valid in positive characteristic but needs to be stated more carefully using *central isogenies*, cf. [3, §22].

Examples. 1. Let T be a K-torus. Then for any integer $n > 1$, the map

$$\pi_n \colon T \to T, \quad t \mapsto t^n,$$

is a nontrivial isogeny.

2. More generally, let G be a connected reductive, but not semi-simple, group. Then G is an almost direct product $G = HT$ where H is semi-simple and T is the central torus. Let $F = H \cap T$. Then $G = (H \times T)/\Delta$, where Δ is the image of the embedding

$$F \to H \times T, \quad x \mapsto (x, x^{-1}).$$

Again, for any $n > 1$ one can consider a nontrivial isogeny

$$\tilde{\pi}_n \colon H \times T \to H \times T, \quad (h,t) \mapsto (h, t^n).$$

If $n \equiv 1 (\mathrm{mod}\, |F|)$, then $\tilde{\pi}_n$ satisfies $\tilde{\pi}_n(\Delta) = \Delta$, and therefore descends to an isogeny

$$\pi_n \colon G \to G.$$

Thus, a connected reductive, but not semi-simple, group (in particular, a torus) cannot possibly have strong approximation for any *finite* S. See, however, a discussion below of strong approximation in tori for certain infinite S.

We also recall that a semi-simple group G is simply connected (i.e., does not admit a nontrivial central isogeny $\widetilde{G} \to G$) if for some (equivalently, any) maximal torus T of G, the group of characters $X(T)$ coincides with the weight lattice of the corresponding root system (equivalently, the group of co-characters $X_*(T)$ is spanned by the coroots).

Theorem 2.3 goes back to Kneser. In 1989, H. Minchev [19] observe that the simply connectedness is a necessary condition for strong approximation not only for groups but in fact for arbitrary varieties. Since his paper appeared in a little known (Belo)Russian journal, hence is practically forgotten, I would like to show you some details.

Theorem 2.5. *Let X be an absolutely irreducible variety over a number field K. If there exist a nontrivial connected unramified cover $\pi \colon Y \to X$ defined over an algebraic closure $\bar{K}$, then X does not have strong approximation with respect to any finite set of places S of K.*

Proof. We sketch the argument assuming X and Y to be affine and smooth and S to contain all archimedean places. We may assume that π is a Galois cover of degree $n > 1$, and pick a finite extension a finite extension L/K such that π is L-defined and moreover all automorphisms Y/X are L-defined. To implement the same idea as in the proof of Theorem 2.3, we need to verify two facts:

(A) there exists a finite extension E/L and a finite subset $T \subset V_f^E$ containing V_∞^E such that $\pi^{-1}(X(\mathcal{O}_S)) \subset Y(\mathcal{O}(E)_T)$, where $\mathcal{O}(E)_T$ is the ring of T-integers in E;

(B) for almost all $v \in V_f^K$ such that $L \subset K_v$ we have $\pi(Y(\mathcal{O}_v)) \neq X(\mathcal{O}_v)$.

Granting these facts, one completes the argument as follows. If X has strong approximation with respect to S, then $X(\mathcal{O}_S)$ is dense in $X(\mathcal{O}_v)$ for all $v \in V^K \setminus S$. On the other hand, using Proposition 2.4, one can find $v \in V^K \setminus S$ such that $E \subset K_v$ and v does not lie under any place in T, and also that (B) holds for this v. Then

$$X(\mathcal{O}_S) \subset \pi(Y(\mathcal{O}(E)_T)) \subset \pi(Y(\mathcal{O}_v)).$$

Since $Y(\mathcal{O}_v)$ is compact, we obtain that the closure of $X(\mathcal{O}_S)$ in $X(\mathcal{O}_v)$ is also contained in $\pi(Y(\mathcal{O}_v))$, and therefore cannot be equal to $X(\mathcal{O}_v)$ due to (B).

When proving an analog of (A) in Theorem 2.3, we relied on the fact that the group $G(\mathcal{O}_S)$ is finitely generated, so in no shape or form can this argument be extended to arbitrary varieties. Here one uses the Chevalley-Weil theorem [12, Ch. 2, Lemma 8.3], [42, 4.2]. It follows from (the local version of) this theorem that one can find a finite set $S_1 \subset V^L$ containing all extensions of the valuations in S such that for any $x \in X(\mathcal{O}_S)$, the extension $L(\pi^{-1}(x))$ generated by the coordinates of all preimages of x is unramified at all $w \in V^L \setminus S_1$. On the other hand,

$$[L(\pi^{-1}(x)) : L] \leqslant n!.$$

Invoking now Hermite's theorem [13, p. 122], we see that there are only finitely many possibilities for $L(\pi^{-1}(x))$. Taking the compositum of all these fields, we obtain a finite extension E/L such that $\pi^{-1}(X(\mathcal{O}(S))) \subset Y(E)$. To find a required finite set $T \subset V^E$, we let $x_1, \ldots x_s$ and $y_1, \ldots, y_t$ denote the affine coordinates on X and Y respectively. Since π is finite, one can find a finite subset $S_2 \subset V^L$ containing all extensions of places in S such that all $y_1, \ldots, y_t$ are integral over the ring $\mathcal{O}(L)_{S_2}[x_1, \ldots, x_s]$. Then for T one can take the set of all extensions of the valuations in S_2 to E.

To prove (B), let us pick a finite $S_3 \subset V^L$ containing the extensions of all valuations in S so that for $w \in V^L \setminus S_3$, there are smooth reductions $\underline{Y}^{(w)}$ and $\underline{X}^{(w)}$, and the reduction $\underline{\pi}^{(w)} \colon \underline{Y}^{(w)} \to \underline{X}^{(w)}$ is a Galois cover of degree n. As in the proof of Theorem 2.3, it is enough to show that

$$\underline{\pi}^{(w)}(\underline{Y}^{(w)}(\ell^{(w)})) \neq \underline{X}^{(w)}(\ell^{(w)}), \tag{3}$$

where $\ell^{(w)}$ is the residue field, for almost all w. But clearly

$$|\underline{\pi}^{(w)}(\underline{Y}^{(w)}(\ell^{(w)}))| = \frac{|\underline{Y}^{(w)}(\ell^{(w)})|}{n}. \tag{4}$$

On the other hand, by the Lang-Weil theorem [14], the sizes of both $\underline{X}^{(w)}(\ell^{(w)})$ and $\underline{Y}^{(w)}(\ell^{(w)})$ are

$$q_w^d + O(q_w^{d-1/2}),$$

where q_w is the size of $\ell^{(w)}$ and d is the common dimension of X and Y. Combining this with (4) we obtain (3) when q_w is sufficiently large (i.e., for almost all w). □

It follows in particular that a (nontrivial) K-torus T does not have strong approximation for any finite S. Nevertheless, tori can have strong approximation with respect to certain infinite (and co-infinite) sets S, which can be used for the congruence subgroup problem. The results that follow are joint with G. Prasad [34].

Definition. Let F/K be a finite Galois extension with Galois group $\mathcal{G}$, and let $\mathcal{C}$ be a conjugacy class in $\mathcal{G}$. Then the generalized arithmetic progression $\mathcal{P}(F/K, \mathcal{C})$ is the set of all $v \in V_f^K$ that are unramified in F and for which the Frobenius $\mathrm{Fr}(w|v) \in \mathcal{C}$ for some (equivalently, any) extension $w|v$.

Theorem 2.6. *For every $d, m \geq 1$ there exists an integer $n = n(d,m)$ such that given a K-torus T of dimension $\leqslant d$, a generalized arithmetic progression $\mathcal{P}(F/K, \mathcal{C})$ with $[F : K] = m$, and a finite subset $\mathcal{P}_0 \subset \mathcal{P}(F/K, \mathcal{C})$, for the set*

$$S = (\mathcal{P}(F/K, \mathcal{C}) \setminus \mathcal{P}_0) \cup V_\infty^K,$$

the index $[T(\mathbb{A}_S) : \overline{T(K)}^{(S)}]$ of the closure of $T(K)$ is finite and divides n provided that some (equivalently, every) element of $\mathcal{C}$ acts trivially on $K_T \cap F$, where K_T is the splitting field of T.

Remark. If the assumption of the theorem does not hold, then in some cases it can be shown that the group $T(\mathbb{A}_S)/\overline{T(K)}^{(S)}$ has infinite exponent (cf. [32, Proposition 4]).

Theorem 2.6 has an application to the congruence subgroup problem. Let G be an absolutely almost simple simply connected algebraic group over a number field K, and let $S \subset V^K$ be a subset that contains V_∞^K and does not contain any nonarchimedean v such that G is K_v-anisotropic. We also assume that $G(K)$ satisfies the Margulis-Platonov conjecture (if G is not of type A_ℓ, then this simply means that $G(K)$ does not have any noncentral normal subgroups - which has been established in many cases, cf. [26, Ch. IX] for the details). The goal of the congruence subgroup problem is to compute the corresponding congruence kernel $C^{(S)}(G)$ – see [33] for the relevant definitions. According to a conjecture due to Serre, the congruence kernel $C^{(S)}(G)$ is expected to be finite whenever the S-rank

$$\mathrm{rk}_S\, G := \sum_{v \in S} \mathrm{rk}_{K_v}\, G$$

is $\geqslant 2$. Then one can give a precise computation of $C^{(S)}(G)$ using the results on the metaplectic kernel [30]. These show that under some additional conditions on S, the congruence kernel $C^{(S)}(G)$ is actually trivial, which is equivalent to the fact that for the group $G(\mathcal{O}(S))$ of points over the ring of S-integers $\mathcal{O}(S)$ we have the classical *congruence subgroup property*: every normal subgroup $N \subset G(\mathcal{O}(S))$ of finite index contains the congruence subgroup $G(\mathcal{O}(S), \mathfrak{a})$ for some nonzero ideal $\mathfrak{a}$ of $\mathcal{O}(S)$. Serre's conjecture, in particular, implies that $C^{(S)}(G) = \{1\}$ whenever S is infinite. Using Theorem 2.6, we have been able to prove this in the case where S almost contains a generalized arithmetic progression.

Theorem 2.7. *In the above notations, let L/K be the minimal Galois extension over which G becomes an inner form of a split group. If S almost contains a generalized arithmetic progression $\mathcal{P}(F/K, \mathcal{C})$ where $\sigma|(F \cap L) = \mathrm{id}_{F\cap L}$ for some (equivalently, any) $\sigma \in \mathcal{C}$ (which is automatically true if G is an inner form), then $C^{(S)}(G)$ is trivial.*

3. Strong approximation theorem. Ingredients of the proof.

Let G be an algebraic group over a global field K, and let $S \neq \emptyset$ be a finite set of places of K. We already know that G can have strong approximation only if it is *connected*. So, assume that G is *connected*, and also *reductive*. In characteristic zero, the latter is not really a restriction since any connected G can be written as a semi-direct product $G = H \ltimes U$ over K where H is reductive (the Levi subgroup of G) and U is the unipotent radical of G (the maximal (connected) normal unipotent subgroup of G). It follows from the strong approximation for the field K (which is basically the Chinese remainder theorem when $S \supset V_\infty^K$) that U always strong approximation for any (nonempty) S. Moreover, G has strong approximation if and only if H does which fully reduces the problem to the reductive case (cf. [26, Proposition 7.1]). On the contrary, in positive characteristic, unipotent elements can cause a lot of trouble, which we would like to avoid in these lectures.

We have also seen that if G is reductive but not semi-simple, or semi-simple but not simply connected, then G does not have strong approximation. So, it remains to consider the case of G *semi-simple simply connected.* Then $G = G_1 \times \cdots \times G_r$ (direct product over K), where the G_i's are K-simple groups, and the strong approximation with respect to S holds for G if and only it holds for each G_i. Furthermore, each G_i is of the form

$$G_i = \mathrm{R}_{K_i/K}(H_i),$$

(restriction of scalars) where K_i/K is a finite separable extension and H_i is an absolutely almost simple simply connected K_i-group. It is not difficult to see that strong approximation for G_i with respect to S is equivalent to strong approximation for H_i with respect to $\bar{S}_i$, which consists of all extensions of places from S to K_i (cf. [26, Proposition 7.1]). Thus, we see that it is enough to investigate strong approximation for G an absolutely almost simple simply connected K-group. We then have the following.

Theorem 3.1. (Kneser [11], Platonov [24] for characteristic zero; Margulis [15], [16], Prasad [27] for positive characteristic) *Let G be an absolutely almost simple simply connected algebraic group over a field K, S be a (finite) set of places of K. Then G has strong approximation with respect to S if and only if the group $G_S = \prod_{v\in S} G(K_v)$ is noncompact.*

In other words, a K-simple group G has strong approximation with respect to S if and only if it is simply connected and the group G_S is noncompact. In the general case, a semi-simple K-group G has strong approximation if and only if it is the direct product of its K-simple components and each component has strong approximation. It should be noted that already for homogeneous spaces of absolutely almost simple groups, simply connectedness and the noncompactness of S-points is not sufficient for strong approximation – see ...

Our goal is to prove the strong approximation theorem over number fields. One of the main ingredients of the proof is the truth of the Kneser-Tits conjecture for algebraic groups over local fields, which we will discuss in detail in the next section. The other two is Cartan's theorem for p-adic Lie groups and (one consequence of) the reduction theory for S-arithmetic subgroups.

On p-adic Lie groups. Let $\mathcal{G}$ be an algebraic group defined over $\mathbb{Q}_p$. Then the group $\mathcal{G} = \mathcal{G}(\mathbb{Q}_p)$ has a natural structure of a p-adic Lie group. Recall the following fundamental fact (see [40, pp. 260-263]):

Theorem 3.2. (Cartan) *Let $\mathcal{G}$ be a Lie group over $\mathbb{R}$ or $\mathbb{Q}_p$. Then every closed subgroup of $\mathcal{G}$ is also a Lie group. Every continuous homomorphism of Lie groups is analytic.*

We will now make a couple of additional comments for the case where $\mathcal{G} = \mathcal{G}(\mathbb{Q}_p)$ where $\mathcal{G}$ is a $\mathbb{Q}_p$-defined algebraic group. Let $\mathfrak{g} = L(\mathcal{G})$ be the Lie algebra of the algebraic group $\mathcal{G}$. Then the Lie algebra $\mathfrak{g}^*$ of $\mathcal{G}$ as a p-adic Lie group can be naturally identified with $\mathfrak{g}_{\mathbb{Q}_p}$. Let $\mathcal{H} \subset \mathcal{G}$ be a subgroup closed in the p-adic topology. Then according to Theorem 3.2, $\mathcal{H}$ is also a Lie group (more precisely, $\mathcal{H}$ has a structure of a p-adic manifold, and the identity map $\mathcal{H} \hookrightarrow \mathcal{G}$ is an analytic embedding), so that we have an inclusion $\mathfrak{h}^* \subset \mathfrak{g}^*$ of the corresponding Lie algebras. We note that $\mathfrak{h}^* = \mathfrak{g}^*$ if and only if $\mathcal{H}$ is open in $\mathcal{G}$.

On the other hand, we can consider the Zariski closure B of $\mathcal{H}$ in G, so that $\mathcal{H} \subset \mathcal{B} := B(\mathbb{Q}_p)$. Let $\mathfrak{b}^*$ be the Lie algebra of $\mathcal{B}$.

Lemma 3.3. $\mathfrak{h}^*$ *is an ideal of* $\mathfrak{b}^*$.

Indeed, consider the adjoint representation $\mathrm{Ad}\colon G \to \mathrm{GL}(\mathfrak{g})$. Let $\mathbf{K}$ be the "universal domain" containing $\mathbb{Q}_p$, so that $\mathfrak{g} = \mathfrak{g}^* \otimes_{\mathbb{Q}_p} \mathbf{K}$. Then the space $\mathfrak{h} = \mathfrak{h}^* \otimes_{\mathbb{Q}_p} \mathbf{K}$ is invariant under $\mathcal{H}$, hence also under its Zariski closure B. It follows that $\mathfrak{h}^*$ is invariant under $\mathcal{B}$. Since the differential of Ad is the adjoint representation ad of the Lie algebra, we obtain that $[\mathfrak{b}^*, \mathfrak{h}^*] \subset \mathfrak{h}^*$, as required. □

Corollary 3.4. *Let $\mathcal{G}$ be an almost $\mathbb{Q}_p$-simple algebraic group, and let $\Gamma \subset \mathcal{G} = \mathcal{G}(\mathbb{Q}_p)$ be a nondiscrete Zariski-dense subgroup. Then the closure $\overline{\Gamma} \subset \mathcal{G}$ in the p-adic topology is open.*

Indeed, let $\mathcal{H} = \overline{\Gamma}$. Since Γ is nondiscrete, $\mathcal{H}$ is a Lie subgroup of $\mathcal{G}$ of positive dimension, so its Lie algebra $\mathfrak{h}^*$ is nonzero. Since Γ is Zariski-dense in $\mathcal{G}$, we obtain from Lemma 3.3 that $\mathfrak{h}^*$ is an ideal of $\mathfrak{g}^*$. But G is almost $\mathbb{Q}_p$-simple, implying that $\mathfrak{g}^*$ does not have proper nonzero ideals. Thus, $\mathfrak{h}^* = \mathfrak{g}^*$, so $\mathcal{H}$ is open in $\mathcal{G}$. □

On the reduction theory for S-arithmetic groups and its consequences. Let $G \subset \mathrm{GL}_n$ be an algebraic defined over a number field K, let $S \subset V^K$ be a finite subset containing V_∞^K, and let $\mathcal{O}_S$ be the ring of S-integers. Set

$$G(\mathcal{O}_S) = G \cap \mathrm{GL}_n(\mathcal{O}(S)).$$

Then $G(\mathcal{O}_S)$ diagonally embeds into $G_S := \prod_{v \in S} G(K_v)$ as a *discrete* subgroup; subgroups commensurable with $G(\mathcal{O}_S)$ are called *S-arithmetic.* The following theorem summarizes the main results of the reduction theory for S-arithmetic subgroups.

Theorem 3.5. (1) *For G semi-simple, the quotient $G_S/G(\mathcal{O}_S)$ has finite invariant measure.*

(2) *For G reductive, the quotient $G_S/G(\mathcal{O}_S)$ is compact if and only if G is K-anisotropic.*

(We will not actually use (2) but the following remark is in order. Strong approximation for an absolutely almost simple simply connected *K-isotropic* group can be established by using strong approximation in unipotent subgroups, so one really needs to consider only the case of K-anisotropic groups. Then by (2) the quotient $G_S/G(\mathcal{O}_S)$ is compact, (and so the quotient $G(\mathbb{A})/G(K)$). In this case, the statements from measure theory that we will use - such as Lemmas 3.7, 3.8 - become almost trivial. In other words, in treating the main case of anisotropic groups in characteristic zero, the use of measure theory can be avoided altogether.)

Proposition 3.6. (Density Theorem) *Assume that G is almost K-simple. If G_S is noncompact then $G(\mathcal{O}_S)$ is Zariski-dense in G.*

(Conversely, if G_S is compact then $G(\mathcal{O}_S)$, being a discrete subgroup thereof, is finite, hence not Zariski-dense.)

Proof. Since G_S is noncompact, its Haar measure is infinite. On the other hand, according to Theorem 3.5(1), the quotient $G_S/G(\mathcal{O}_S)$ has finite measure (which simply amounts to saying that there is a measurable subset $\Omega \subset G_S$ having finite Haar measure such that $G_S = \Omega G(\mathcal{O}_S)$). So, the group $G(\mathcal{O}_S)$ is *infinite.* Let $H = \overline{G(\mathcal{O}_S)}^\circ$ (connected component of the Zariski-closure). Then H is a K-defined subgroup of G having positive dimension. Let $g \in G(K)$. It is easy to show that the subgroups $G(\mathcal{O}_S)$ and $gG(\mathcal{O}_S)g^{-1}$ are *commensurable*, i.e. their intersection has finite index in both of them. It follows that

$$\overline{G(\mathcal{O}_S)}^\circ = \overline{G(\mathcal{O}_S) \cap gG(\mathcal{O}_S)g^{-1}}^\circ = \overline{gG(\mathcal{O}_S)g^{-1}}^\circ,$$

i.e. $H = gHg^{-1}$. Thus, H is normalized by $G(K)$, and since $G(K)$ is Zariski-dense in G (see [3, 18.3]) we see that H is a normal subgroup of G. Since G is K-simple, $H = G$, as required. □

Remark. The argument actually establishes the following stronger fact. Let $\mathcal{G} = \mathrm{R}_{K/\mathbb{Q}}(G)$. Then one can naturally identify $G(K)$ with $\mathcal{G}(\mathbb{Q})$, and we let Γ denote the image of $G(\mathcal{O}_S)$ under this identification. Then Γ is Zariski-dense in $\mathcal{G}$. Since there is a K-defined map $\mathcal{G} \to G$ taking Γ back to $G(\mathcal{O}_S)$, this assertion implies the proposition. The proof of this assertion is a slight variation of the argument given in the proof of the proposition. More precisely, we observe that for any $g \in \mathcal{G}(\mathbb{Q})$, the subgroups Γ and $g\Gamma g^{-1}$ are commensurable. So, if we let $\mathcal{H}$ denote the connected component of the Zariski-closure of Γ, then $\mathcal{H}$ is a $\mathbb{Q}$-defined normal subgroup of $\mathcal{G}$ of positive dimension. But $\mathcal{G}$ is $\mathbb{Q}$-simple. (Indeed, since G is K-simple, we may assume that $G_0 = \mathrm{R}_{L/K}(G_0)$ for some absolutely almost simple group G_0 over some finite extension L/K. Then $\mathcal{G} = \mathrm{R}_{L/\mathbb{Q}}(G_0)$, hence $\mathbb{Q}$-simple.) So, $\mathcal{H} = \mathcal{G}$, as required.

Now, let point out the following straightforward result from measure theory.

Lemma 3.7. *Let $G = G_1 \times G_2$ be the direct product of two locally compact topological groups, let $\pi_i \colon G \to G_i$ $(i = 1, 2)$ be the corresponding projection, and let $H \subset G$ be a closed subgroup for which the intersection $H \cap (G_1 \times \{e\})$ is trivial and the quotient G/H has finite invariant measure. Then $\pi_2(H)$ is nondiscrete and the quotient $G_2/\overline{\pi_2(H)}$ (where $\bar{}$ denotes the closure) has finite invariant measure.*

This follows from the following property of quotient measures: Let $H_1 \subset H_2$ be two closed subgroups of a locally compact group G; if G/H_1 has finite invariant measure then so does G/H_2 (cf. Raghunathan [36, Lemma 1.6]).

We will use the following consequence of this fact.

Lemma 3.8. *Let G be a semi-simple algebraic group over a number field K, and let $S \subset V^K$ be a finite subset such that the group G_S is noncompact. Given any finite (nonempty) subset $S_1 \subset V^K \setminus S$ such that $S \cup S_1$ contains V_∞^K, the image of $G(\mathcal{O}(S \cup S_1))$ in G_{S_1} is nondiscrete and the quotient $G_{S_1}/\overline{G(\mathcal{O}(S \cup S_1))}$ has finite invariant measure.*

This follows from the previous statement applied to $G_{S \cup S_1} = G_S \times G_{S_1}$ and $H = G(\mathcal{O}(S \cup S_1))$ taking into account Theorem 3.5(1).

4. The Kneser-Tits conjecture over local fields

Let G be an absolutely almost simple algebraic group over a field K. Assume that G is K-isotropic - recall that this means that $\mathrm{rk}_K\, G > 0$, i.e. G contains a nontrivial K-split torus, or equivalently, that G contains proper K-defined parabolics. We then let $G(K)^+$ denote the (normal) subgroup of $G(K)$ generated by the K-rational points of the unipotent radicals of K-defined parabolics (note that $G(K)^+$ is known to coincide with the subgroup generated by all unipotents in $G(K)$ if $\mathrm{char}\, K = 0$). It was proved by Tits [44] that if K contains at least 4 elements then the group $G(K)^+$ does not contain any proper noncentral (abstract) normal subgroups. In the same paper Tits, referring to a suggestion made by Kneser, formulated the following conjecture, which became known as

The Kneser-Tits conjecture. *$G(K) = G(K)^+$ for any absolutely almost simple simply connected algebraic group G over any field K.*

It is known, due to Chevalley and Steinberg, that the conjecture is true if G is split or quasi-split over K. The general case remained open until around 1978 when Platonov constructed the first counterexamples to this conjecture over general fields (cf. [26, 7.2] and references therein). What is important for strong approximation, however, is that the conjecture is actually true for all groups over local (i.e. nondiscrete locally compact) fields.

Theorem 4.1. (Platonov [24], [25]) *Let G be an absolutely almost simple simply connected isotropic algebraic group over a nonarchimedean local field K. Then $G(K)^+ = G(K)$.*

(Platonov actually handled the characteristic zero case, i.e. when K is a finite extension of $\mathbb{Q}_p$, but the result remains valid also in positive characteristic.)

Corollary 4.2. *Let G be an absolutely almost simple simply connected isotropic algebraic group over a nonarchimedean local field K. Then $G(K)$ does not have any proper subgroups of finite index.*

We will first give an outline of the ideas involved in the proof of Theorem 4.1, and then fill in some details. An important general fact is that the proof of the Kneser-Tits conjecture over a field K can generally be reduced to almost K-simple simply connected groups of K-rank 1. Such a group G is of the form $G = \mathrm{R}_{L/K}(H)$ for an absolutely almost simple simply connected group H over a finite separable extension L/K with $\mathrm{rk}_L\, H = 1$. Clearly, if the Kneser-Tits conjecture holds for H over L, then it holds for G over K. Thus, we get a reduction to absolutely almost simple simply connected groups of relative rank 1 (note that we need the Kneser-Tits conjecture to hold not only over a given field K itself but also over its finite separable extensions). A very helpful fact over nonarchimedean local fields is that all absolutely almost simple groups of relative rank one are of classical types. This follows from the classification results, but in fact we don't even need the detailed classification. There are two fundamental facts related to the classification over a nonarchimeadean local field K:

(A) $H^1(K, G) = 1$ for any semi-simple simply connected group G;

(B) if G is absolutely almost simple and K-anisotropic then G is an inner form of type A_n.

(These facts can either be derived from the Bruhat-Tits theory [7], or can be obtained through a careful case-by-case analysis [26, Ch. VI].) Since the groups of types $\mathsf{E}_8, \mathsf{F}_4, \mathsf{G}_2$ are both simply connected and adjoint, we obtain from (A) that they all are split over K. Let G be an absolutely almost simple simply connected group, and Z be its center, and $\bar{G} = G/Z$ be the corresponding adjoint group. Then we have the coboundary map

$$H^1(K, \bar{G}) \to H^2(K, Z).$$

It follows from (A) applied to G and its twists that this map is injective. On the other hand, $H^2(K, Z)$ can be easily computed in all cases. In particular, these computations show that for types${}^{3,6}\mathsf{D}_4$ and ${}^2\mathsf{E}_6$, the group $H^2(K, Z)$ vanishes. These means that all groups of these types are quasi-split (then their K-rank is $\geqslant 2$, and they satisfy the Kneser-Tits conjecture anyway). This leaves us with only types E_6 and E_7.

To handle these types, let us introduce some notations that will be used in this section systematically. Let S be a maximal K-split torus of G (thus, $\dim S = \mathrm{rk}_K G$). Pick a maximal K-torus T of G containing S, and let $\Phi = \Phi(G, T)$ be the corresponding root system. We then pick a minimal K-defined parabolic $P \subset G$ and then choose a Borel subgroup $B \subset P$. Let $\Pi \subset \Phi$ be the system of simple roots that corresponds to B. We then consider the Dynkin diagram for Φ, and call a vertex in this diagram *distinguished* (and circle it in the diagram) if the restriction of the corresponding simple root to S is nontrivial. Yet another important element is the so-called $*$-action of the Galois group $\mathrm{Gal}(\bar{K}/K)$ on the Dynkin diagram. More precisely, since T is defined over K, the Galois group acts on the group of characters $X(T)$, and this action takes roots to roots. In other words, we get a homomorphism

$$\theta \colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(\Phi(G, T)).$$

Let $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Then $\sigma(\Pi)$ is another system of simple roots in Φ, so there exists a unique $w_\sigma \in W(G, T) = W(\Phi(G, T))$ (the Weyl group of G with respect to T which is identified with the Weyl group of the root system $\Phi(G, T)$) such that

$$(w_\sigma \circ \sigma)(\Pi) = \Pi.$$

Then the action on the Dynkin diagram given by $w_\sigma \circ \sigma$ is called the $*$-action by σ. (Exercise. Check that this is indeed an action.) Recall that the $*$-action is trivial if and only if our group is an inner form of the split group. The Dynkin diagram with circled vertices and the given $*$-action is called the Tits index. When we draw the Tits index, we put the vertices that lie in the same orbit of the $*$-action close to each other. In fact, the $*$-action takes distinguished vertices to distinguished vertices, so we put a common circle on the distinguished orbits on the distinguished vertices in the same orbit of the $*$-action. Recall that the K-rank of G coincides with the number of orbits of the $*$-action on the set of distinguished vertices; in fact, the maximal K-split torus S is defined inside T by the conditions stating that all nondistinguished vertices vanish on S and all distinguished vertices in the same $*$-orbit have the same value on S.

Let $H = Z_G(S)$, and let $G_0 = [H, H]$ be the anisotropic kernel of G over K. It is a K-anisotropic semi-simple group with a maximal K-torus $T_0 := T \cap G_0$, and its Dynkin diagram is obtained from the Dynkin diagram of G by discarding all distinguished vertices (thus, the set of vertices of this diagram coincides with the set Π_0 of nondistinguished vertices).

Now, let us handle the remaining cases E_6 and E_7. For G of type E_7, the center Z has order 2. Then every element of $H^2(K, Z)$ splits over a (in fact, any) quadratic extension extension of K, so G splits over a quadratic extension of K. On the other hand, the anisotropic kernel can have only components of type A_n. Since these split over a quadratic extension, all components must be of type A_1. But it is impossible to obtain a diagram of type $\mathsf{A}_1 + \cdots + \mathsf{A}_1$ by deleting from a diagram of type E_7 only one vertex. So, $\mathrm{rk}_K\, G \geqslant 2$.

Similarly, for G of type E_6, the center Z has order 3. Arguing as above, we conclude that G splits over a cubic extension of K, and therefore all components of the anisotropic kernel must be of type A_2. But again, it is impossible to obtain a diagram of type $\mathsf{A}_2 + \cdots + \mathsf{A}_2$ from a diagram of type E_6 by deleting just one vertex. So, $\mathrm{rk}_K\, G \geqslant 2$.

Thus, it remains to establish the Kneser-Tits conjecture for classical groups of relative rank one, which one does basically case-by-case. We will discuss this later, but now I would like to give more details about this reduction to the rank-one case.

In his original argument, Platonov did not fully justify the reduction to the rank-one case (this was done later by Prasad and Raghunathan [29]), but he described a procedure that leads to a reduction to groups of smaller K-rank. His idea was the following. Let $H = Z_G(S)$, and let $U^{\pm}$ be the unipotent radicals of two opposite parabolic subgroups. Then the product map

$$U^+ \times H \times U^- \longrightarrow G$$

yields a K-defined isomorphism onto a Zariski-open subset $\Omega \subset G$. Then, assuming that K is infinite (which we always may since any semi-simple algebraic group over a finite field is split or quasi-split by Lang's theorem, cf. [3, §16]), $\Omega(K)$ generates $G(K)$. It follows that the embedding $H \hookrightarrow G$ gives an isomorphism of abstract groups:

$$H(K)/(H(K) \cap G(K)^+) \simeq G(K)/G(K)^+.$$

Thus, to prove that $G(K) = G(K)^+$, we need to prove that $H(K) \subset G(K)^+$. Platonov's idea was to find absolutely almost simple simply connected K-isotropic subgroups G_i, normalized by S, for which the Kneser-Tits is known to be true (in his argument over local fields, these were groups of classical types) and such that for $H_i = (G_i \cap H)^\circ$ the subgroups $H_i(K)$ generate $H(K)$. Then

$$H(K) = \langle H_i(K) \rangle \subset \langle G_i(K)^+ \rangle \subset G(K)^+.$$

In 1985, Prasad and Raghunathan showed that the most natural choice of the G_i's works in the general case. More precisely, let Π_0 be the set of nondistinguished vertices, and let $\Theta_1, \ldots, \Theta_r$ be the orbits of the $*$-action on $\Pi \setminus \Pi_0$. For a $*$-invariant subset $\Theta \subset \Pi$ containing Π_0 we let

$$T(\Theta) = \left(\bigcap_{\theta \in \Theta} \ker \theta \right)^\circ \quad , \quad H(\Theta) = Z_G(T(\Theta)) \quad , \quad G(\Theta) = [H(\Theta), H(\Theta)].$$

(So, for $\Theta = \Pi_0$, the group $H(\Pi_0)$ coincides with $H = Z_G(S)$, and $G(\Pi_0)$ coincides with G_0, the anisotropic kernel.) For any Θ as above, the group $G(\Theta)$ is a semi-simple (but not necessarily absolutely or even K-simple group) simply connected group. Furthermore, for any orbit Θ_i the group $G(\Theta_i \cup \Pi_0)$ has K-rank one, hence has a unique K-simple K-isotropic factor G_i.

Theorem 4.3. (Prasad-Raghunathan [29]) *Assume that* $\mathrm{rk}_K G \geqslant 2$. *Then the group* $H(K)$ *is generated by the subgroups* $H_i(K)$ *for* $i = 1, \ldots, r$. *Consequently, if the Kneser-Tits conjecture is true for* G_i *then it is also true for* G.

Note that this result is for *general* fields. It is derived from the following cohomological statement.

Theorem 4.4. *Let* $\Pi_1, \ldots, \Pi_d$ *be* $*$*-invariant subsets of* $\Pi \setminus \Pi_0$ *such that* $\bigcap_{i=1}^d \Pi_i = \emptyset$. *Then the map*

$$H^1(K, G_0) \longrightarrow \prod_{i=1}^{d} H^1(K, G(\Pi_i \cup \Pi_0))$$

has trivial kernel.

This result becomes trivial over nonarchimedean local fields since H^1 vanishes for any simply connected group (see (A) above). So, we will make no comments on the proof of Theorem 4.4, and show only how it implies Theorem 4.3.

Let Π_i denote the complement of Θ_i in $\Pi \setminus \Pi_0$, i.e. $\Pi_i = \bigcup_{j \neq i} \Theta_i$. We begin with the following.

Lemma 4.5. *The natural map*

$$H(\Pi_0)/G(\Pi_0) \to \prod_{i=1}^{r} H(\Pi_i \cup \Pi_0)/G(\Pi_i \cup \Pi_0).$$

induced by inclusions, is an isomorphism.

Proof. For $\alpha \in \Phi$, we let G_α denote the corresponding 3-dimensional subgroup and let $T_\alpha = T \cap G_\alpha$. It is well-known that since G is simply connected, we have

$$T = \prod_{\alpha \in \Pi} T_\alpha.$$

Note that $G_\alpha = [H(\alpha), H(\alpha)]$ where $H(\alpha) = Z_G(T(\alpha))$ and $T(\alpha) = (\ker \alpha)^\circ$. It follows that for any subset $\Theta \subset \Pi$, the group $G(\Theta)$ contains $T_\Theta = \prod_{\alpha \in \Theta} T_\alpha$. So,

$$\dim T_\Theta = |\Theta| \leqslant \mathrm{rk}\, G(\Theta) \leqslant \dim T - \dim T(\Theta) = |\Theta|,$$

and therefore all inequalities are actually equalities, and T_Θ is a maximal torus of $G(\Theta)$. It follows that $(T \cap G(\Theta))^\circ = T_\Theta$, and consequently $G(\Theta) \cap T_{\Pi \setminus \Theta} = \{1\}$. On the other hand,

$$H(\Theta) = G(\Theta)T = G(\Theta)T_{\Pi \setminus \Theta},$$

showing that $H(\Theta)$ is a semi-direct product of $G(\Theta)$ and $T_{\Pi \setminus \Theta}$. Now, consider the following commutative diagram induced by embeddings:

$$\begin{tikzcd}
H(\Pi_0)/G(\Pi_0) \arrow[r] & \prod_{i=1}^{r} H(\Pi_i \cup \Pi_0)/G(\Pi_i \cup \Pi_0) \\
T_{\Pi \setminus \Pi_0} \arrow[u] \arrow[r] & \prod_{i=1}^{r} T_{\Theta_i} \arrow[u]
\end{tikzcd}.$$

All maps in this diagram, except possibly for the top one, are bijection. So, the top one is a bijection as well, proving our claim. □

To simplify notations, we set $C_i = H(\Pi_i \cup \Pi_0)$ and $D_i = G(\Pi_i \cup \Pi_0)$. We then have the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & G_0 \arrow[r] \arrow[d] & H \arrow[r] \arrow[d] & H/G_0 \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \prod_{i=1}^{r} D_i \arrow[r] & \prod_{i=1}^{r} C_i \arrow[r] & \prod_{i=1}^{r}(C_i/D_i) \arrow[r] & 1
\end{tikzcd}.$$

It induces the following commutative cohomological diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & G_0(K) \arrow[r] \arrow[d] & H(K) \arrow[r] \arrow[d] & (H/G_0)(K) \arrow[r] \arrow[d, "\alpha"] & H^1(K, G_0) \arrow[d, "\beta"] \\
1 \arrow[r] & \prod_{i=1}^{r} D_i(K) \arrow[r] & \prod_{i=1}^{r} C_i(K) \arrow[r] & \prod_{i=1}^{r}(C_i/D_i)(K) \arrow[r] & \prod_{i=1}^{r} H^1(K, D_i)
\end{tikzcd}.$$

Since $\cap_{i=1}^r \Pi_i = \emptyset$, we obtain from Theorem 4.4 that β has trivial kernel. It follows from the lemma that α is an isomorphism. Then a simple diagram chase shows that the homomorphism

$$H(K)/G_0(K) \longrightarrow \prod_{i=1}^{r} C_i(K)/D_i(K)$$

is an isomorphism. It follows that $H(K)$ is generated by the subgroups

$$F_i := H(K) \bigcap \left(\bigcap_{j \neq i} D_j(K) \right) = \left(H \bigcap G(\Theta_i \cup \Pi_0) \right)(K).$$

We have

$$H \bigcap G(\Theta_i \cup \Pi_0) = A_i \times H_i,$$

where A_i is the product of K-anisotropic factors of $G(\Theta_i \cup \Pi_0)$. Then $F_i = A_i(K)H_i(K)$. It remains to observe that $A_i \subset G_0$ for every i. Since the Tits index is connected, every component of G_0 lies in some G_i, hence in H_i. This completes the proof of Theorem 4.3. □

Thus, we have reduced the proof of Theorem 4.1 to groups of K-rank one and also established that (for a nonarchimedean locally compact field K) all such groups belong to classical types. Here is the list of such groups (over the the fields in question):

(1) $G = \mathrm{SL}_{2,D}$ where D is a central division algebra over K;
(2) $G = \mathrm{SU}_n(L/K, h)$ where h is a hermitian form over a quadratic extension L/K of Witt index 1;
(3) $G = \mathrm{Spin}_n(q)$ where q is a quadratic form of Witt index 1;
(4) $G = \widetilde{SU}_3(D, h)$, the universal cover of the unitary group of a skew-hermitian h over a quaternion algebra D with the canonical involution, having Witt index 1.

One shows that for any of the groups in (2)-(4), the Kneser-Tits conjecture holds over *any* field. We will demonstrate this by considering the case of spinor groups of isotropic quadratic forms (the fact that the Witt index is one does not play any role).

Proposition 4.6. *Let q be a nondegenerate* isotropic *quadratic form over a field K of characteristic $\neq 2$. Then the Kneser-Tits conjecture holds for $G = \mathrm{Spin}_n(q)$.*

(We note that this follows also from the geometric approach (Gille [10]) since $\mathrm{Spin}_n(q)$ is known to be a rational variety if q is isotropic.)

Proof. It is well-known that for $n = 3$, the group G is isomorphic to SL_2 (for example, because the corresponding (even) Clifford algebra is isomorphic to the matrix algebra M_2), and in this case our assertion is well-known. The general case is considered by induction on $n \geqslant 4$.

We will view q as a quadratic form on $V = K^n$, and assume that in the standard basis $e_1, \ldots, e_n$ of V the form q looks as follows:

$$q(x_1e_1 + \cdots x_ne_n) = x_1x_2 + a_3x_3^2 + \cdots + a_nx_n^2$$

(in other words, the space $\langle e_1, e_2\rangle$ is a hyperbolic plane). We consider the standard action of $\mathcal{G} = G(K)$ on V (this action factors through the usual action of $\mathrm{SO}_n(q)(K)$). Set $a = e_{n-1}$, $b = e_n$. To implement induction, it is enough to show that

$$\mathcal{G} = \mathcal{G}(a)\mathcal{G}(b)\mathcal{G}(a), \tag{5}$$

where $\mathcal{G}(a)$ and $\mathcal{G}(b)$ are the stabilizers of the corresponding vectors (indeed, these stabilizers are the spinor groups of isotropic forms of dimension $n-1$ and, on the other hand, $G(a)(K)^+, G(b)(K)^+ \subset G(K)^+$; so $G(a)(K) = G(a)(K)^+$ and $G(b)(K) = G(b)(K)^+$ in conjunction with (5) implies $G(K) = G(K)^+$). Let $(\,|\,)$ denote the bilinear form on V associated with q. Since the space $\langle a, b\rangle^{\perp} = \langle e_1, e_2, \ldots, e_{n-2}\rangle$ is isotropic, we have

$$q(\langle a, b\rangle^{\perp}) = K.$$

It follows that for a given $g \in \mathcal{G}$ we can find $v \in V$ that satisfies

$$(v|a) = (g(a)|a)\ ,\ (v|b) = (a|b) = 0\ ,\ q(v) = q(a).$$

Then the spaces $\langle a, v\rangle$ and $\langle a, g(a)\rangle$ are isometric by an isometry that takes $a \to a$, $v \to g(a)$. By Witt's theorem, one can find $\bar{g}_1 \in \mathrm{O}_n(q)(K)$ such that

$$\bar{g}_1(a) = a\ \ ,\ \ \bar{g}_1(v) = g(a).$$

Changing $\bar{g}_1$ by a reflection with respect to an anisotropic vector in $\langle v, a\rangle^{\perp}$, we can assume that $\bar{g}_1 \in \mathrm{SO}_n(q)(K)$. Similarly, we can find $\bar{g}_2 \in \mathrm{SO}_n(q)(K)$ such that

$$\bar{g}_2(a) = v\ ,\ \bar{g}_2(b) = b.$$

Then for $\bar{g}_3 := (\bar{g}_1\bar{g}_2)^{-1}\bar{g}$, where $\bar{g}$ is the image of g in $\mathrm{SO}_n(q)(K)$, we have

$$\bar{g}_3(a) = (\bar{g}_2^{-1}\bar{g}_1^{-1}\bar{g})(a) = \bar{g}_2^{-1}(v) = a.$$

Thus, $\bar{g} = \bar{g}_1\bar{g}_2\bar{g}_3$ with $\bar{g}_1, \bar{g}_2, \bar{g}_3 \in \mathrm{SO}_n(q)(K)$, with $\bar{g}_1, \bar{g}_3$ fixing a and $\bar{g}_2$ fixing b. Now, we need to lift this factorization to the spinor group, for which we need to make sure that the spinor norm of the factors is 1. For this we observe that we can replace $\bar{g}_1, \bar{g}_2$ with $\bar{g}_1h, h^{-1}\bar{g}_2$ for any $h \in \mathrm{SO}_{n-2}(q)(a,b)(K)$. Since the space $\langle a, b\rangle^{\perp}$ is isotropic, the spinor norm maps $\mathrm{SO}_{n-2}(q)(a,b)(K)$ surjectively onto $K^{\times}/{K^{\times}}^2$. So, we can make the spinor norm of $\bar{g}_1$ to be 1. Similarly, replacing $\bar{g}_2, \bar{g}_3$ with $\bar{g}_2h, h^{-1}\bar{g}_3$, we can make the spinor norm of $\bar{g}_2$ to be 1. Now, we lift $\bar{g}_1, \bar{g}_2$ to $g_1, g_2 \in \mathcal{G}$, and set $g_3 = (g_1g_2)^{-1}g$. Then

$$g = g_1g_2g_3,$$

and the images of g_1, g_2, g_3 in $SO_n(g)$ are $\bar{g}_1, \bar{g}_2, \bar{g}_3$. This implies that $g_1, g_3 \in \mathcal{G}(a)$ and $g_2 \in \mathcal{G}(b)$, as required. □

To complete the proof of Theorem 4.1, it remains to consider the groups $G = \mathrm{SL}_{2,D}$; the argument actually works for $G = \mathrm{SL}_{m,D}$ for any $m \geqslant 2$. Here some reduction steps in the argument work over arbitrary fields, but the crucial step uses the following special property of nonarchimedean local fields: the reduced norm $\mathrm{Nrd}_{D/K}\colon D^{\times} \to K^{\times}$ is surjective. Since the complete argument is quite long, we will only indicate the main steps.

First, one uses the Dieudonné determinant to show that for $G = \mathrm{SL}_{m,D}$ where $m \geqslant 2$ and D a finite-dimensional central division algebra over any field that

$$G(K)/G(K)^+ \simeq SL(1,D)/[D^{\times}, D^{\times}]\ \text{ where }\ SL(1,D) = \{x \in D^{\times} \,|\, \mathrm{Nrd}_{D/K}(x) = 1\}.$$

The quotient $SL(1,D)/[D^{\times}, D^{\times}]$ is usually called the *reduced Whitehead group* of D and denoted $SK_1(D)$ (similarly, one defines the group SK_1 of any finite-dimensional central simple algebra). So, what we need to prove is the following.

Theorem 4.7. *Let D be a finite-dimensional central division algebra over a nonarchimedean local field K. Then $SK_1(D) = 1$.*

First, one uses properties of the Dieudonné determinant to prove the following.

Lemma 4.8. *Let $a \in SL(1, D)$. If*

$$a \in [(D \otimes_K B)^\times, (D \otimes_K B)^\times]$$

where B is some associative K-algebra with 1 of dimension m then $a^m \in [D^\times, D^\times]$.

This lemma has two important consequences.

Corollary 4.9. *If D has degree n (i.e. $\dim_K D = n^2$) then $SK_1(D)$ is a group of exponent n.*

Indeed, if L is a maximal subfield of D then $D \otimes_K L \simeq M_n(L)$, and it is known that $SL_n(L) = [GL_n(L), GL_n(L)]$.

Next, it is known that if $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ then $D = D_1 \otimes_K \cdots \otimes_K D_r$ where D_i has degree $p_i^{\alpha_i}$.

Corollary 4.10. $SK_1(D) \simeq SK_1(D_1) \times \cdots \times SK_1(D_r)$.

Thus, it is enough to prove that $SK_1(D)$ is trivial assuming that D has degree p^d for some prime p (we note that this reduction is valid over any field). This case is treated by induction on d. The following statement (which again is valid over any field) handles the base case $d = 1$.

Proposition 4.11. *Let D be a central division algebra over an arbitrary field K of a prime degree p. Then $SK_1(D) = 1$.*

Proof. Let $a \in D^\times$ with $\mathrm{Nrd}_{D/K}(a) = 1$, and let L be a maximal subfield of D containing a. Then

$$\mathrm{N}_{L/K}(a) = \mathrm{Nrd}_{D/K}(a) = 1.$$

If L/K is (purely) inseparable (which is possible only if $p = \mathrm{char}\, K$), then $a = 1$, and there is nothing to prove. So, we may assume that L/K is separable. Let M be the Galois closure of L with Galois group $\mathcal{G} = \mathrm{Gal}(M/K)$. Let $\mathcal{G}_p$ be the Sylow p-subgroup of $\mathcal{G}$, and let $P = M^{\mathcal{G}_p}$ be the corresponding fixed field. Then the degree $m = [P : K]$ is prime to p. On the other hand, since $\mathcal{G}$ is contained in the symmetric group S_p, the subgroup $\mathcal{G}_p$ has order p. It follows that $L \otimes_K P = LP = M$ and M/P is a cyclic Galois extension of degree p. We have

$$N_{M/P}(a) = N_{L/K}(a) = 1.$$

It follows from Hilbert 90 that $a = \sigma(b)/b$ for some $b \in M^\times$, where σ is a generator of $\mathrm{Gal}(M/P)$. On the other hand, by the Skolem-Noether Theorem, there exists $t \in (D \otimes_K P)^\times$ such that $\sigma(b) = tbt^{-1}$. Thus,

$$a = tbt^{-1}b^{-1}$$

is a commutator in $(D \otimes_K P)^\times$. Invoking Lemma 4.8, we conclude that $a^m \in [D^\times, D^\times]$. On the other hand, by Corollary 4.9, $a^p \in [D^\times, D^\times]$. Since m and p are relatively prime, we see that $a \in [D^\times, D^\times]$, as required. □

Conclusion of the proof of Theorem 4.7. We will now assume that the group SK_1 is trivial for all central division algebras of degree p^{d-1} over nonarchimedean local fields, and prove that it is then trivial for all algebras of degree p^d over such fields. The argument here is a beefed up version of the proof of Proposition 4.11. So, let D be a central division algebra of degree p^d over a nonarchimedean local field K, let $a \in SL(1, D)$, and let L be a maximal subfield of D containing a. We will only consider the case where L/K is separable; the general case differs by some minor technical details. Let M be the Galois closure of L with Galois group $\mathcal{G} = \mathrm{Gal}(M/K)$. Pick a Sylow p-subgroup $\mathcal{G}_p \subset \mathcal{G}$, and set $P = M^{\mathcal{G}_p}$. Let $\mathcal{H} \subset \mathcal{G}_p$ be the subgroup corresponding to the subfield $LP \subset M$. Then one can find a normal subgroup $\mathcal{N} \subset \mathcal{G}_p$ of index p containing $\mathcal{H}$. Then $E := M^{\mathcal{N}}$ is a cyclic extension of P contained in $LP = L \otimes_K P$. As above, it is enough to show that

$$a \in [(D \otimes_K P)^\times, (D \otimes_K P)^\times].$$

We have

$$\mathrm{N}_{LP/P}(a) = \mathrm{Nrd}_{D/K}(a) = 1 = \mathrm{N}_{E/P}\left(\mathrm{N}_{LP/E}(a)\right).$$

Applying Hilbert's 90, we conclude that there exists $b \in E$ such that

$$\mathrm{N}_{LP/E}(a) = \sigma(b)b^{-1}, \tag{6}$$

where σ is a generator of $\mathrm{Gal}(E/P)$. Now, let Δ be the centralizer of E in $D \otimes_K P$; according to the Double Centralizer Theorem, Δ is a central division algebra over E of degree p^{d-1}. The crucial for us property is

$$\mathrm{Nrd}_{\Delta/E}(\Delta^\times) = E^\times;$$

this property holds because E is a nonarchimedean local field and is equivalent to the fact that $H^1(E, \mathrm{SL}_{1,\Delta}) = 1$, cf. (A) above. Thus, we can pick $t \in \Delta$ so that $\mathrm{Nrd}_{\Delta/E}(t) = b$. Furthermore, by the Skolem-Noether Theorem, one can find $s \in (D \otimes_K P)^\times$ such that the inner automorphism $x \mapsto sxs^{-1}$ induces σ on E. Then s normalizes Δ, and for $[s,t] = sts^{-1}t^{-1} \in \Delta$ we have

$$\mathrm{Nrd}_{\Delta/E}([s,t]) = \sigma(b)b^{-1}.$$

Comparing with (6)), we obtain

$$\mathrm{Nrd}_{\Delta/E}(a[s,t]^{-1}) = 1.$$

By induction, we conclude that $a[s,t]^{-1} \in [\Delta^\times, \Delta^\times]$, and therefore $a \in [(D \otimes_K P)^\times, (D \otimes_K P)^\times]$, as required. □

For completeness, let us also discuss the archimedean situation. A semi-simple group G over $\mathbb{C}$ splits, so $G(\mathbb{C})^+ = G(\mathbb{C})$ and $G(\mathbb{C})$ is connected. The following statement treats real algebraic groups.

Proposition 4.12. (Cartan) *Let G be an absolutely almost simple simply connected $\mathbb{R}$-group. Then $G(\mathbb{R})$ does not have any proper noncentral normal subgroups. In particular, $G(\mathbb{R})$ is connected, and if G is $\mathbb{R}$-isotropic then $G(\mathbb{R})^+ = G(\mathbb{R})$.*

Proof. First, let G be an arbitrary reductive $\mathbb{R}$-anisotropic group, i.e. $G(\mathbb{R})$ is compact. Then every element of $g \in G(\mathbb{R})$ is semi-simple, hence lies in some maximal $\mathbb{R}$-torus T. Since T splits over $\mathbb{C}$ and is anisotropic over $\mathbb{R}$, we have

$$T \simeq (\mathrm{R}^{(1)}_{\mathbb{C}/\mathbb{R}}(G_m))^d, \quad d = \dim T.$$

Then $T(\mathbb{R}) \simeq \mathbb{U}^d$, where $\mathbb{U} = \{z \in \mathbb{C}^\times \mid |z| = 1\}$, hence connected. It follows that $G(\mathbb{R})$ is connected. Now, let G be in addition $\mathbb{R}$-simple. Then using the Implicit Function Theorem, it is easy to show that every noncentral normal subgroup of $G(\mathbb{R})$ is open [26, Theorem 3.3], and therefore must coincide with $G(\mathbb{R})$ since this group is connected.

Now, let G be an almost simple simply connected $\mathbb{R}$-isotropic group. Being a normal subgroup of $G(\mathbb{R})$ the group $G(\mathbb{R})^+$ is open in $G(\mathbb{R})$. Furthermore, since the group of real points of a unipotent subgroup is connected, the group $G(\mathbb{R})^+$ is also connected. So, we just need to prove that

$$G(\mathbb{R})^+ = G(\mathbb{R}).$$

Let S be a maximal $\mathbb{R}$-split torus of G, and let $H = Z_G(S)$. As we remarked earlier, it is enough to show that $H(\mathbb{R}) \subset G(\mathbb{R})^+$. Write H as an almost direct product $H = B \cdot S$ where B is a reductive $\mathbb{R}$-anisotropic group. Then $H(\mathbb{R}) = B(\mathbb{R}) \cdot S(\mathbb{R})$. Indeed, we have the following commutative diagram

$$\begin{tikzcd} H \arrow[r] & H/S \\ B \arrow[u] \arrow[r, "\alpha"] & B/(B \cap S) \arrow[u, "="'] \end{tikzcd} .$$

Then $B/(B \cap S)$ is a reductive $\mathbb{R}$-anisotropic group, so $(B/(B \cap S))(\mathbb{R})$ is connected as we have just seen above. On the other hand, it follows from the Implicit Function Theorem that $\alpha(B(\mathbb{R}))$ is open in $(B/(B \cap S))(\mathbb{R})$. Thus,

$$\alpha(B(\mathbb{R})) = (B/(B \cap S))(\mathbb{R}).$$

Then a simple diagram chase shows that $H(\mathbb{R}) = B(\mathbb{R}) \cdot S(\mathbb{R})$. Now, since $B(\mathbb{R})$ is connected and $G(\mathbb{R})^+$ is open in $G(\mathbb{R})$, we conclude that $B(\mathbb{R})$. On the other hand, it was shown by Borel and Tits [4, 7.2] and [5, 4.6] that S is contained in a simply connected $\mathbb{R}$-split subgroup of G, implying that $S(\mathbb{R}) \subset G(\mathbb{R})^+$. Thus, $H(\mathbb{R}) \subset G(\mathbb{R})^+$, as required. □

5. Proof of strong approximation

Let G be an absolutely almost simple simply connected algebraic group over a number field K, and let $S \subset V^K$ be a finite subset such that the group G_S is noncompact. We wish to show that $G(K)$ is dense in $G(\mathbb{A}_S)$. Any open subset $\Omega \subset G(\mathbb{A}_S)$ looks as follows:

$$\Omega = \mathcal{U} \times \prod_{v \notin S \cup S_1} G(\mathcal{O}_v)$$

for some finite set $S_1 \subset V^K \setminus S$ such that $S \cup S_1$ contains V_∞^K and some open set $\mathcal{U} \subset G_{S_1}$. Then $G(K) \cap \Omega \neq \emptyset$ is equivalent to $G(\mathcal{O}(S \cup S_1)) \cap \mathcal{U} \neq \emptyset$. Thus, the density of $G(K)$ in $G(\mathbb{A}_S)$ is equivalent to the density of $G(\mathcal{O}(S \cup S_1))$ in G_{S_1}, for any finite $S_1 \subset V^K \setminus S$ (and one can assume without loss of generality that $S \cup S_1 \supset V_\infty^K$). To prove the latter, we will be using repeatedly the following elementary statement.

Lemma 5.1. ([26, Lemma 7.4]) *Let Γ be a subgroup of the direct product $B = B_1 \times B_2$ of topological groups B_1 and B_2, and let $\pi_i \colon B \to B_i$ be the canonical projection for $i = 1, 2$. Assume that*

(1) $\pi_1(\Gamma)$ *is dense in B_1;*

(2) *B_1 has a fundamental systems of neighborhoods of the identity $\mathcal{U} = \{U\}$ consisting of subgroups such that for every $U \in \mathcal{U}$ the projection $\pi_2(\Gamma \cap (U \times B_2))$ is dense in B_2.*

Then Γ is dense in B.

We will first consider the case where S contains V_∞^K and also all those nonarchimedean v for which G is K_v-anisotropic (i.e. $G(K_v)$ is compact) - recall that such places can exist only if G is of type A_n. Let $S_1 \subset V^K \setminus S$ be a finite subset. We need to show that $\Gamma = G(\mathcal{O}(S \cup S_1))$ is dense in G_{S_1}. Assume the contrary, and let $S_2 \subset S_1$ be a maximal (possibly, empty) subset such that (the image of the diagonal embedding of Γ is dense in G_{S_2}. By our assumption, $S_2 \neq S_1$, so we pick some $v \in S_1 \setminus S_2$ and set $S_3 = S_2 \cup \{v\}$. Since Γ is *not* dense in $G_{S_3} = G_{S_2} \times G(K_v)$ and G_{S_2} has a fundamental system of neighborhoods of the identity consisting of subgroups, it follows from Lemma 5.1 that there exists an open subgroup $U \subset G_{S_2}$ such that $\Gamma \cap U$ is not dense $G(K_v)$. We may assume without loss of generality that U is a finite index subgroup of $\prod_{v \in S_2} G(\mathcal{O}_v)$. It follows that $\Gamma \cap U$ contains some finite index subgroup of $G(\mathcal{O}(S \cup \{v\}))$. But according to Corollary 4.2, the group $G(K_v)$ does not have proper subgroups subgroups of finite index, so to obtain a contradiction it is enough to prove the following.

Proposition 5.2. *For any $v \in V^K \setminus S$, the group $\Delta = G(\mathcal{O}(S \cup \{v\}))$ is dense in $G(K_v)$.*

Proof. First, it follows from Lemma 3.8 that Δ is nondiscrete in $G(K_v)$ and the quotient $G(K_v)/\overline{\Delta}$ by the closure of Δ has finite invariant measure. Next, consider the groups $\mathcal{G}_0 = \mathrm{R}_{K/\mathbb{Q}}(G)$ and $\mathcal{G} = \mathrm{R}_{K_v/\mathbb{Q}_p}(G)$, where p is chosen so that $\mathbb{Q}_p \subset K_v$ and note that there is a $\mathbb{Q}_p$-defined epimorphism $\mathcal{G}_0 \to \mathcal{G}$. According to the remark made after Proposition 3.6, the group Δ is Zariski-dense in $\mathcal{G}_0$, hence in $\mathcal{G}$. On the other hand, as we have already mentioned, Δ is not discrete in $G(K_v) \simeq \mathcal{G}(\mathbb{Q}_p)$. So, applying Corollary 3.4, we obtain that $\bar{\Delta}$ is open. Now, the fact that $G(K_v)/\bar{\Delta}$ has finite measure tells us that $\bar{\Delta}$ is a subgroup of finite index in $G(K_v)$. But again according to Corollary 4.2, the group $G(K_v)$ does not have any proper subgroups of finite index. So, $\bar{\Delta} = G(K_v)$, as required. □

We will now drop the assumption that S contains

$$S_{\mathrm{an}} := \{v \in V_f^K \mid G \text{ is } K_v\text{-anisotropic}\}.$$

We will need to use *weak approximation* for simply connected groups.

Proposition 5.3. *Let G be a semi-simple simply connected group over a number field K. Then G has weak approximation with respect to any finite subset $T \subset V^K$, i.e. $G(K)$ is dense in $G_T = \prod_{v \in T} G(K_v)$.*

Proof. It is well-known that the variety of G is unirational over K, i.e. there exists a K-defined dominant map $f\colon W \to G$ of some Zariski-open subset $W \subset \mathbb{A}^d$ of the affine space (cf. [3, 18.2]). The weak approximation theorem for the field K implies the weak approximation property for W; in other words, $W(K)$ is dense in $W_T = \prod_{v \in T} W(K_v)$. Applying f, we obtain that the closure of $G(K)$ in G_T contains $\prod_{v \in T} f(W(K_v))$. But using the Implicit Function Theorem, one shows that $f(W(K_v))$ contains an open subset of $G(K_v)$ (cf. [26, Cor. 1 in §3.1]), which implies that the closure $\overline{G(K)}$ is always open in G_T; in other words, the quotient $G_T/\overline{G(K)}$ is discrete. On the other hand, according the reduction theory for the groups of adeles, the quotient $G(\mathbb{A})/G(K)$ has finite invariant volume [26, Theorem 5.5]. Writing $G(\mathbb{A}) = G(\mathbb{A}_T) \times G_T$ and using Lemma 3.7, we see that $G_T/\overline{G(K)}$ has finite invariant measure, and therefore is in fact finite. If G is not of type A_n, then $G(K_v)$ does not have proper subgroups of finite index (indeed, if v is nonarchimedean then G is K_v-isotropic and required fact is Corollary 4.2; for v archimedean it is Proposition 4.12). Then the same is true for G_T, and we obtain $\overline{G(K)} = G_T$, as required.

Let now G be of type A_n. Then according to classification G is either $\mathrm{SL}_{m,D}$ (inner form) or $\mathrm{SU}_m(h, D)$ (outer form) where h is a hermitian form over a division algebra D with an involution of the second kind. We then let H respectively be $\mathrm{GL}_{m,D}$ and $\mathrm{U}_m(h, D)$. (A group G of type A_1 can be viewed as both, inner or outer form, but then we use the first option for H, i.e. we view G as an inner form.) In either case, the variety of H is rational over K, and therefore H has weak approximation, i.e. $H(K)$ is dense in H_T (cf. [26, 7.1]). Clearly, $[H(F), H(F)] \subset G(F)$ for any field extension F/K, and in fact

$$[H(K_v), H(K_v)] = G(K_v)$$

for any v. This follows from Theorem 4.1 when v is nonarchimedean and G is K_v-isotropic, and from Proposition 4.12 for v archimedean. It remains to consider the case where v is nonarchimedean and G is K_v-anisotropic. But then $G \simeq \mathrm{SL}_{1,\mathcal{D}}$ and $H \simeq \mathrm{GL}_{1,\mathcal{D}}$ for some central division algebra $\mathcal{D}$ over K_v (see (B) in §4), and our claim is equivalent to the fact that $SK_1(\mathcal{D}) = 1$ which was established in Theorem 4.7. But then already $[H(K), H(K)] \subset G(K)$ is dense in G_T. □

Returning now to the proof of strong approximation, we recall that the set S_{an} is finite and that strong approximation for $S \cup S_{\mathrm{an}}$ has already been established. Set $S_0 = S_{\mathrm{an}} \setminus S$ so that $S \cup S_{\mathrm{an}} = S \cup S_0$ and

$$G(\mathbb{A}_S) = G_{S_0} \times G(\mathbb{A}_{S \cup S_0})$$

Since all places in S_0 are nonarchimedean, G_{S_0} has a fundamental system of neighborhoods of the identity consisting of open subgroups $U \subset G_{S_0}$. Moreover, since G_{S_0} is compact, $[G_{S_0} : U] < \infty$. By Proposition 5.3, $G(K)$ is dense in G_{S_0}. So, in order to apply Lemma 5.1, we need to show that $G(K) \cap U$ is dense in $G(\mathbb{A}_{S \cup S_0})$. But we already know that $G(K)$ is dense in $G(\mathbb{A}_{S \cup S_0})$, so it remains to show that the latter does not have proper closed subgroups of finite index. Let H be such a subgroup. For every $v \notin S \cup S_0$, the group G is K_v-isotropic, so the group $G(K_v)$ does not have any proper subgroups of finite index, and therefore is contained in H. We conclude that H contains G_{S_2} for any finite $S_2 \subset V^K \setminus (S \cup S_0)$. But it easily follows from the definition of the adelic topology that the union $\bigcup_{S_2} G_{S_2}$ over all such S_2's is dense in $G(\mathbb{A}_{S \cup S_0})$. So, $H = G(\mathbb{A}_{S \cup S_0})$, as claimed.

Finally, let us get rid of the assumption that S contains V_∞^K. Set $S_1 = V_\infty^K \setminus (V_\infty^K \cap S)$ and $S_2 = S \cup S_1$ so that

$$G(\mathbb{A}_S) = G(\mathbb{A}_{S_2}) \times G_{S_1}.$$

We already know that $G(K)$ is dense in $G(\mathbb{A}_{S_2})$. Furthermore, the latter has a basis of neighborhoods of the identity consisting of open subgroups $U \subset G(\mathbb{A}_{S_2})$, and we need to show that for any such subgroup the intersection $G(K) \cap U$ is dense in G_{S_1}. Without loss of generality we may assume that $U \subset \prod_{v \notin S_2} G(\mathcal{O}_v)$, and then $G(K) \cap U$ is a finite index subgroup of $G(\mathcal{O}(S_2))$. It follows from Proposition 4.12 and the preceding remarks that for each $v \in S_1$ the group $G(K_v)$ is connected, so the group G_{S_1} is connected as well. So, in order to prove that $G(K) \cap U$ is dense in G_{S_1} for every U, it is enough to prove that $G(\mathcal{O}(S_2))$ is dense in G_{S_1}. Let Λ denote the connected component of the closure of $G(\mathcal{O}(S_2))$ in G_{S_1}. We claim that Λ is a normal subgroup of G_{S_1}. Indeed, for any $g \in G(K)$

the subgroups $G(\mathcal{O}(S_2))$ and $gG(\mathcal{O}(S_2))g^{-1}$ are commensurable, which implies that $\Lambda = g\Lambda g^{-1}$. But $G(K)$ is dense in G_{S_1} by Proposition 5.3, so Λ is normal in G_{S_1}. Thus, $\Lambda = G_{S_3}$ for some $S_3 \subset S_1$ and it remains to show that actually $S_3 = S_1$. Assume the contrary, i.e. $S_4 := S_1 \setminus S_3 \neq \emptyset$, and let $\pi \colon G_{S_1} \to G_{S_4}$ be the canonical projection. Since $\ker \pi = G_{S_3}$ is contained in the closure of $G(\mathcal{O}(S_2))$, the connected component of the closure $\Phi = \overline{G(\mathcal{O}(S_2))}$ in G_{S_4} coincides with $\pi(\Lambda) = 1$. If we consider G_{S_4} as a real Lie group, then by Cartan's theorem Φ is also a Lie group. So, since its connected component is trivial, it is actually discrete. But $G(\mathcal{O}(S_2))$ is a discrete subgroup of G_{S_2} such that the quotient $G_{S_2}/G(\mathcal{O}(S_2))$ has finite invariant measure. Writing $G_{S_2} = G_{S_2 \setminus S_4} \times G_{S_4}$ and observing that $S_2 \setminus S_4$ contains S, making $G_{S_2 \setminus S_4}$ noncompact, we obtain from Lemma 3.7 that $G(\mathcal{O}(S_2))$ in nondiscrete in G_{S_4}, a contradiction. □

The above proof of Theorem 3.1 for characteristic zero breaks down in positive characteristic, first and foremost, because Cartan's Theorem 3.2 is valid only in characteristic zero. It should be mentioned that eventually Pink [21] proved a result which in some sense can be viewed as an analog (or replacement) of Cartan's theorem. The precise statement in the general case is too technical for us to discuss here, so we will only indicate what it yields in one particular case (see [21, Theorem 0.7]): *Let G be an absolutely simple connected adjoint group over a nondiscrete locally compact field F, and assume that the adjoint representation of G is irreducible. If $\Gamma \subset G(F)$ is a compact Zariski-dense subgroup, then there exists a closed subfield $E \subset F$ and a model H of G over E such that Γ is open in $H(E)$.* Results of this kind can be used to prove Theorem 3.1 in positive characteristic (cf. [22]), but the original argument given simultaneously by Margulis [15] and Prasad [27], was different. They derived strong approximation (arguing along the lines indicated above) from the following statement:

> *Let G be a connected semisimple algebraic group over a local field F, and let H be a nondiscrete closed subgroup such that $G(F)/H$ carries a finite invariant Borel measure. Then $H \supset G(F)^+$.*

Their arguments (which were different) used ergodic considerations and representation theory. More than 25 years later, Pink [23] used his results from [21] to give a purely algebraic proof of this theorem, hence of strong approximation.

Strong approximation in homogeneous spaces. The results on strong approximation in homogeneous were obtained in [6] and [37] (a detailed exposition of the results of the latter was given in [38]). The fact that only connected simply connected varieties have a chance to possess strong approximation, by and large, forces us to focus our attention on homogeneous spaces of the form $X = G/H$ where G is a semi-simple simply connected algebraic K-group, and H is a K-defined connected reductive subgroup (any such variety is affine and simply connected). Furthermore, given $S \subset V^K$, it is not difficult to show that for such X, the space $X_S = \prod_{v \in S} X(K_v)$ is noncompact if and only if G_S is noncompact. Assuming that G is actually absolutely almost simple, we conclude from Theorem 3.1 that G has strong approximation with respect to S (for a general semi-simple group G one needs to consider the K-simple components). Then using Galois cohomology one investigates when strong approximation for G implies strong approximation for $X = G/H$. Here is one easy result in this direction.

Proposition 5.4. ([37]) *Let $X = G/H$ be the quotient of a connected absolutely almost simple simply connected algebraic group G defined over a number field K by a connected semi-simple simply connected K-subgroup H. Then X has strong approximation with respect to a finite set S of places of K is and only if the space X_S is noncompact.*

Example. Let $q = q(x_1, \dots, x_n)$ be a nondegenerate quadratic form over K in $n \geqslant 3$ variables. Consider the quadric $X \subset \mathbb{A}^n$ given by the equation $q(x_1, \dots, x_n) = a$ for some $a \in K^{\times}$. Assuming that $X(K) \neq \emptyset$, fix $x \in X(K)$. Then X can be identified with the homogeneous space G/H where $G = \mathrm{Spin}_n(q)$ and $H = G(x)$ (the stabilizer of x); note that $H \simeq \mathrm{Spin}_{n-1}(q')$, where q' is the restriction of q to the orthogonal complement of x. So, it follows from Proposition 5.4 that for $n \geqslant 5$, the quadric

X has strong approximation with respect to S if and only if there exists $v \in S$ such that q is K_v-isotropic. The same result remains valid for $n = 4$ even though in this case G is not absolutely almost simple. (Incidentally, this result applies to the defining equation for SL_2 we considered in §1, yielding thereby another proof of strong approximation for this group; cf. Lemma 4.5.)

Exercise. Work out explicit conditions for strong approximation in "spheres" defined by other types of forms.

The case $n = 3$ in the above example is different as here $H = G(x)$ is a torus. This case can also be treated rather explicitly using the results of Nakayama-Tate on the Galois cohomology of tori. More precisely, let T be a K-torus, and let L be the splitting field of T. As usual, given a module M over the Galois group $\mathrm{Gal}(L/K)$, we let $H^i(L/K, M)$ denote the Galois cohomology group $H^1(\mathrm{Gal}(L/K), M)$. Given a finite set S of places of K, we let $\bar{S}$ denote the set of all extensions of places in S to L, and let $\mathbb{A}_L$ and $\mathbb{A}_{L,\bar{S}}$ denote the rings of adeles and $\bar{S}$-adeles of L. Finally, let $c_L(T) = T(\mathbb{A}_L)/T(L)$ be the adele class group of T over L, and let

$$\delta\colon H^1(L/K, T(\mathbb{A}_L)) \longrightarrow H^1(L/K, c_L(T))$$

be the corresponding map on cohomology. Then, viewing $T_{\bar{S}}$ and $T(\mathbb{A}_{L,\bar{S}})$ as subgroups of $T(\mathbb{A}_L)$, we have the following statement.

Proposition 5.5. ([37]) *Let $X = G/T$, where G is an absolutely almost simple simply connected K-group and $T \subset G$ is a K-torus. Then X has strong approximation with respect to a finite set S of places of K if and only if X_S is noncompact and*

$$\delta\left(H^1(L/K, T(\mathbb{A}_{L,\bar{S}}))\right) \subset \delta\left(\ker(H^1(L/K, T_{\bar{S}}) \to H^1(L/K, G_{\bar{S}}))\right),$$

where L is the splitting field of T and $\bar{S}$ consists of all extensions of places in S to L.

Example (continuation) Using Proposition 5.5, we can now consider the case $n = 3$ and complete thereby the analysis of strong approximation in quadrics. So, let

$$q(x, y, z) = ax^2 + by^2 + cz^2$$

be a nondegenerate ternary quadratic form over a number field K, and let $X \subset \mathbb{A}^3$ be a quadric given by the equation $q(x, y, z) = a$. Set $q'(y, z) = by^2 + cz^2$. Let S be a finite set of places of K such that X_S is noncompact. Then X has strong approximation with respect to S if and only if one of the following two conditions holds:

- q' is K-isotropic, or
- q' is K-anisotropic and there exists $v \in S$ such that q' remains anisotropic over K_v and either v is nonarchimedean or q is K_v-isotropic.

It follows that the quadric X over $\mathbb{Q}$ defined by the equation

$$x^2 + y^2 - 2z^2 = 1$$

(which is simply connected) does *not* have strong approximation with respect to $S = \{\infty\}$.

Another consequence of Proposition 5.5 is that for $X = G/T$, one can find a finite set of places S_0 (depending on T) such that X has strong approximation with respect to S whenever $S \supset S_0$. It turns out that this qualitative statement remains valid for quotients by arbitrary connected reductive subgroups. More precisely, using some ideas that eventually led him to theorems of the Nakayama-Tate type for Galois cohomology of arbitrary connected groups, Borovoi proved the following.

Proposition 5.6. ([6]) *Let $X = G/H$ be the quotient of a connected absolutely almost simple algebraic group G over a number field K by its connected reductive subgroup H. There exists a finite set S_0 of places of K such that X has strong approximation with respect to S_0 (and then, of course, it also has strong approximation with respect to any $S \supset S_0$).*

6. Strong approximation for Zariski-dense subgroups

Strong approximation for algebraic group G over a number field K with respect to a set of places S gives us the density of $G(\mathcal{O}(S))$ in $\prod_{v \notin S} G(\mathcal{O}_v)$, and in particular, the openness of $\overline{G(\mathcal{O}(S))}$ in $G(\mathbb{A}_S)$, which, by and large, is the most essential part of the strong approximation theorem. It turned out, however, this property (i.e. the openness of the closure) holds not only for S-arithmetic groups but in fact in a much more general situation. For example, slightly generalizing our discussion in §1, one shows that the subgroup

$$\Delta_m = \left\langle \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \right\rangle \subset \mathrm{SL}_2(\mathbb{Z}),$$

which for $m > 2$ has *infinite* index in $\mathrm{SL}_2(\mathbb{Z})$, the closure $\overline{\Delta_m}$ is open in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, i.e. has *finite* index. We will see that actually the only feature of a subgroup needed to ensure the openness of the closure is its *Zariski-density.* To avoid technical complications, I will explain this for $K = \mathbb{Q}$ (this is, in fact how these results emerged historically), and in the end state a theorem for the general case. The following lemma, the proof of which requires only the techniques that we have already used in the proof of the strong approximation theorem, shows one immediate consequence of Zariski-density.

Lemma 6.1. *Let G be an absolutely almost simple algebraic $\mathbb{Q}$-group, and let $\Gamma \subset G(\mathbb{Z})$ be a Zariski-dense subgroup. Then for any* finite *set of primes P, the closure of Γ in $\prod_{p \in P} G(\mathbb{Z}_p)$ is open.*

Proof. We first consider the case where $P = \{p\}$ consists of a single prime. Let $\mathfrak{g} = L(G)$ be the Lie algebra of G as an algebraic group, so that $\mathfrak{g}^* = \mathfrak{g}_{\mathbb{Q}_p}$ is the Lie algebra of $G(\mathbb{Z}_p)$ as a p-adic Lie group. Since $G(\mathbb{Z}_p)$ is compact, Γ is not discrete there. So, it follows from Cartan's theorem that $\Delta := \overline{\Gamma}$ is a p-adic Lie group of *positive* dimension. Then the Lie algebra $\mathfrak{h}^*$ of Δ is a nonzero subalgebra of $\mathfrak{g}^*$. Furthermore, since Γ is Zariski-dense in G, the algebra $\mathfrak{h}^*$ is an ideal of $\mathfrak{g}^*$ (Lemma 3.3). Since G is absolutely almost simple, $\mathfrak{g}^*$ does not have any proper nonzero ideals, so $\mathfrak{h}^* = \mathfrak{g}^*$, and we conclude that Δ is open in $G(\mathbb{Z}_p)$, as required (cf. Corollary 3.4).

Now, let $P = \{p_1, \ldots, p_r\}$. We already know that the closure Δ_i of Γ in $G(\mathbb{Z}_{p_i})$ is open for each $i = 1, \ldots, r$. But $G(\mathbb{Z}_{p_i})$ is an almost pro-p_i group. So, the Sylow pro-p_i subgroup $\Delta_i(p_i)$ is also open in $G(\mathbb{Z}_{p_i})$. Let Δ be the closure of Γ in $\mathcal{G} = \prod_{i=1}^r G(\mathbb{Z}_{p_i})$, and let $\Delta(p_i)$ be the Sylow pro-p_i subgroup of Δ. Then for the projection $\pi_i \colon \mathcal{G} \to G(\mathbb{Z}_{p_i})$ we have $\pi_i(\Delta(p_i)) = \Delta_i(p_i)$. But $\Delta(p_i)$ has an open subgroup $\Delta'(p_i)$ which is contained in the factor $G(\mathbb{Z}_{p_i})$ of $\mathcal{G}$, and note that $\Delta'(p_i)$ is open in $G(\mathbb{Z}_{p_i})$. Thus, Δ contains the product $\prod_{i=1}^r \Delta'(p_i)$, and our assertion follows. □

While this assertion (and particularly its proof) is quite useful (e.g. it is used in the proof of the existence of generic elements in arbitrary Zariski-dense subgroups, cf. ..), it falls short of proving that the closure $\widehat{\Gamma}$ of Γ in $G(\widehat{\mathbb{Z}}) = \prod_p G(\mathbb{Z}_p)$ is open. Indeed, all it gives is that $\widehat{\Gamma}$ contains a subgroup of the form $\prod_p W_p$, where $W_p \subset G(\mathbb{Z}_p)$ is an open subgroup; to prove the openness however we need to show that one can take $W_p = G(\mathbb{Z}_p)$ for almost all p. Nevertheless, we have the following.

Theorem 6.2. (Matthews, Vaserstein, Weisfeiler [18]) *Let G be a connected absolutely almost simple simply connected algebraic group over $\mathbb{Q}$.*

(1) *If $\Gamma \subset G(\mathbb{Z})$ is a Zariski-dense then the closure $\widehat{\Gamma} \subset G(\widehat{\mathbb{Z}})$ is open.*

(2) *If $\Gamma \subset G(\mathbb{Q})$ is a finitely generated Zariski-dense subgroup then for some finite subset $S \subset V^{\mathbb{Q}}$ containing ∞ such that the closure of Γ in $G(\mathbb{A}_S)$ is open.*

The paper of Matthews et al. appeared in 1984, but the interest in this sort of results arose some 20 years earlier in connection with the study of Galois representations on torsion points of elliptic curves. In fact, Serre in his book on ℓ-adic representations [41] pretty much had this theorem for SL_2 (at least all the ingredients were there).

The argument for parts (1) and (2) is very much parallel. Let us sketch if for part (1) which requires less notations. The main point is to show that if we let $\overline{\Gamma}^{(p)}$ denote the closure of Γ in $G(\mathbb{Z}_p)$ then

$$\overline{\Gamma}^{(p)} = G(\mathbb{Z}_p) \tag{7}$$

for almost all p. If this fact is granted, then the proof of the fact $\widehat{\Gamma}$ is open in $G(\widehat{\mathbb{Z}})$ is obtained by a relatively straightforward group-theoretic argument. The idea is revealed in the following

Exercise. Let $F_1, \ldots, F_r$ are pairwise nonisomorphic nonabelian finite simple groups. If E is a subgroup of the direct product $F = F_1 \times \cdots F_r$ that projects surjectively onto each factor, then $E = F$.

In our situation, for almost all primes p, the group G has good reduction $\underline{G}^{(p)}$, and the finite almost simple groups $\underline{G}^{(p)}(\mathbb{F}_p)$ are pairwise nonisomorphic. Using this, one can find a finite set P of "bad" primes such that if Ψ is a closed subgroup of $\Theta = \prod_{p \notin P} G(\mathbb{Z}_p)$ that projects surjectively onto each factor, then $\Psi = \Theta$ (cf. the above exercise). This, in conjunction with with (7) and Lemma 6.1, yields the openness of $\hat{\Gamma}$.

Thus, it remains to establish (7) for almost all p. For this one uses the following statement, which can also be used to facilitate the above reduction. Let $\rho_p \colon G(\mathbb{Z}_p) \to \underline{G}^{(p)}(\mathbb{F}_p)$ be the reduction mod p map.

Proposition 6.3. *For almost all p, if $\Delta \subset G(\mathbb{Z}_p)$ is a closed subgroup such that $\rho_p(\Delta) = G(\mathbb{Z}_p)$ then $\Delta = G(\mathbb{Z}_p)$.*

To give an idea of the proof we will give a complete argument in the case $G = \mathrm{SL}_2$ which was considered by Serre.

Lemma 6.4. *Let $\Delta \subset \mathrm{SL}_2(\mathbb{Z}_p)$, where $p > 3$, such that for the reduction map $\rho_p \colon \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$ we have $\rho_p(\Delta) = \mathrm{SL}_2(\mathbb{F}_p)$. Then $\Delta = \mathrm{SL}_2(\mathbb{Z}_p)$.*

Proof. By assumption, there exists $g \in \Delta$ such that

$$g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + ps, \quad \text{with} \quad s \in M_2(\mathbb{Z}_p).$$

Using that $p > 3$, one shows that

$$g^p = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} + p^2 t, \quad \text{with} \quad t \in M_2(\mathbb{Z}_p).$$

Let $\mathrm{SL}_2(\mathbb{Z}_p, p^i)$ denote the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ modulo $p^i\mathbb{Z}_p$. It is well-known that there exists an isomorphism of abelian groups

$$\mathrm{SL}_2(\mathbb{Z}_p, p)/\mathrm{SL}_2(\mathbb{Z}_p, p^2) \simeq \mathfrak{sl}_2(\mathbb{F}_p),$$

where $\mathfrak{sl}_2$ is the Lie algebra of SL_2 (i.e., 2×2-matrices with trace zero). Our previous computation shows that the image of Φ of the intersection $\Delta \cap \mathrm{SL}_2(\mathbb{Z}_p, p)$ in this quotient is *nontrivial.* On the other hand, Φ is obviously invariant under the adjoint action of Δ, and since $\rho_p(\Delta) = \mathrm{SL}_2(\mathbb{F}_p)$, we conclude that Φ is actually invariant under $\mathrm{SL}_2(\mathbb{F}_p)$. But since $p \neq 2$, the group $\mathrm{SL}_2(\mathbb{F}_p)$ acts on $\mathfrak{sl}_2(\mathbb{F}_p)$ irreducibly, implying that $\Delta \cap \mathrm{SL}_2(\mathbb{Z}_p, p)$ surjects onto $\mathrm{SL}_2(\mathbb{Z}_p, p)/\mathrm{SL}_2(\mathbb{Z}_p, p^2)$. However, $\mathrm{SL}_2(\mathbb{Z}_p, p^2)$ is in fact the Frattini subgroup of the pro-p group $\mathrm{SL}_2(\mathbb{Z}_p, p)$, so the latter fact implies that $\Delta \cap \mathrm{SL}_2(\mathbb{Z}_p, p) = \mathrm{SL}_2(\mathbb{Z}_p, p)$, and our claim follows. □

So, to complete the proof of (both parts of) Theorem 6.2, one needs to prove the following.

Theorem 6.5. *Let G be a connected absolutely almost simple simply connected algebraic group over $\mathbb{Q}$, and let $\Gamma \subset G(\mathbb{Q})$ be a finitely generated Zariski-dense subgroup. Then there exists a finite set of primes $\Pi = \{p_1, \ldots, p_r\}$ such that*

(1) *$\Gamma \subset G(\mathbb{Z}_\Pi)$, where $\mathbb{Z}_\Pi = \mathbb{Z}[1/p_1, \ldots, 1/p_r]$;*

(2) *for $p \in \Pi$, there is a smooth reduction $\underline{G}^{(p)}$;*

(3) *if $p \notin \Pi$ and $\rho_p \colon G(\mathbb{Z}_p) \to \underline{G}^{(p)}(\mathbb{F}_p)$ is the corresponding reduction map, then $\rho_p(\Gamma) = \underline{G}^{(p)}(\mathbb{F}_p)$.*

Conditions (1) and (2) are routine (in fact, (1) holds automatically for any Π if $\Gamma \subset G(\mathbb{Z})$), so the main point is to ensure condition (3). The general idea is the following. Let $\mathfrak{g}$ and $\underline{\mathfrak{g}}^{(p)}$ be the Lie algebras of G and $\underline{G}^{(p)}$. Since Γ is Zariski-dense in G, the group $\mathrm{Ad}\,\Gamma$ acts on $\mathfrak{g}_{\mathbb{Q}}$ absolutely irreducibly. By Burnside's theorem, this means that $\mathrm{Ad}\,\Gamma$ spans $\mathrm{End}_{\mathbb{Q}}\,\mathfrak{g}_{\mathbb{Q}}$ as a $\mathbb{Q}$-vector space. Excluding finitely many primes, we can achieve that for any of the remaining primes p, the group $\mathrm{Ad}\,\rho_p(\Gamma)$ acts on $\underline{\mathfrak{g}}^{(p)}_{\mathbb{F}_p}$ absolutely irreducibly. This *eventually* implies that for almost all p we have

$$\rho_p(\Gamma) = \underline{G}^{(p)}(\mathbb{F}_p).$$

This implication would be obvious if we knew that $\rho_p(\Gamma)$ is necessarily of the form $H(\mathbb{F}_p)$, where $H \subset \underline{G}^{(p)}$ is some connected algebraic $\mathbb{F}_p$ subgroup. (Indeed, then the Lie algebra $\mathfrak{h}$ of would be a nonzero $\rho_p(\Gamma)$ invariant subspace of $\underline{\mathfrak{g}}^{(p)}$, so $\mathfrak{h} = \underline{\mathfrak{g}}^{(p)}$ and $H = \underline{G}^{(p)}$ as $\underline{G}^{(p)}$ is connected for almost all p, yielding the required fact.) Of course, such an a priori description of $\rho_p(\Gamma)$ is too much to hope for, but important information along these lines, which is sufficient for the proof of Theorem 6.5, is contained in a theorem of Nori.

Nori's Theorem. Let H be an *arbitrary subgroup* of $\mathrm{GL}_n(\mathbb{F}_p)$. Set

$$X = \{x \in H \mid x^p = 1\}.$$

Assume that $p > n$. Then the condition $x^p = 1$ is equivalent to the condition $(x-1)^n = 0$, hence characterizes precisely the unipotent elements. For $x \in X$, we can define the "truncated" logarithm

$$\log x := -\sum_{i=1}^{p-1} \frac{(1-x)^i}{i}.$$

Furthermore, observing that $(\log x)^n = 0$, we see that for any $t \in \overline{\mathbb{F}_p}$ (an algebraic closure of $\mathbb{F}_p$) one can define the "truncated" exponential

$$x(t) := \exp(t \cdot \log x), \quad \text{where} \quad \exp z = \sum_{i=0}^{p-1} \frac{z^i}{i!}.$$

(Note that $x(1) = x$.) We regard $x(t)$ as a one-parameter subgroup $\mathbb{G}_a \to \mathrm{GL}_n$. Set

$$H^+ = \langle X \rangle \subset H,$$

and let $\widetilde{H}$ denote the connected $\mathbb{F}_p$-subgroup of GL_n generated by the 1-parameter subgroups $x(t)$ for all $x \in X$.

Theorem 6.6. (Nori [20]) *If p is large enough (for a give n), then H^+ coincides with $\widetilde{H}(\mathbb{F}_p)^+$, the subgroup of $\widetilde{H}(\mathbb{F}_p)$ generated by all unipotents contained in it.*

Exercise. Prove Nori's theorem for $n = 2$. More precisely, show that for any subgroup $H \subset \mathrm{GL}_2(\mathbb{F}_p)$, we have the following three possibilities: (1) $H^+ = \{1\}$; (2) H^+ is conjugate to $U = \left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p\right\}$; (3) $H^+ = \mathrm{SL}_2(\mathbb{F}_p)$. (*Hint.* Use the Bruhat decomposition in $\mathrm{GL}_2(\mathbb{F}_p)$.)

Proof of Theorem 6.5. Recall the famous theorem of Jordan:

> *There exists a function $\mathbf{j}(n)$ on positive integers such that if $\mathcal{G} \subset \mathrm{GL}_n(\mathcal{K})$ is a finite linear group over a field $\mathcal{K}$ of characteristic zero, then $\mathcal{G}$ contains an abelian normal subgroup $\mathcal{N}$ such that the index $[\mathcal{G} : \mathcal{N}]$ divides $\mathbf{j}(n)$.*

For the proof of Theorem 6.5 we need to observe that the assertion of Jordan's theorem remains valid (with the same $\mathbf{j}(n)$) for any subgroup $\mathcal{G} \subset \mathrm{GL}_n(\mathbb{F}_p)$ of order prime to p (this is proved by lifting $\mathcal{G}$ to a subgroup $\tilde{G} \subset \mathrm{GL}_n(\mathbb{Z}_p)$).

Now, suppose that $G \subset \mathrm{GL}_n$. Let $j = \mathbf{j}(n)$ be the value of the Jordan function for this n. Set

$$\Gamma^{(j)} = \langle \gamma^j \mid \gamma \in \Gamma \rangle,$$

and let $\Phi = [\Gamma^{(j)}, \Gamma^{(j)}]$. It is easy to see that Φ is Zariski-dense in G, in particular, nontrivial. Then, by expanding Π, which initially needs to be chosen to satisfy conditions (1) and (2) of the theorem, we may assume that for all $p \notin \Pi$ we have $\rho_p(\Phi) \neq \{1\}$. In addition, by expanding Π further, we may assume that for $p \notin \Pi$, the group $\mathrm{Ad}\, \rho_p(\Phi)$ acts on $\underline{\mathfrak{g}}^{(p)}$ absolutely irreducibly, and also that Nori's theorem applies to $\mathrm{GL}_n(\mathbb{F}_p)$. We will now show that the resulting Π is as required.

Let $p \notin \Pi$, and set $H = \rho_p(\Gamma) \subset \mathrm{GL}_n(\mathbb{F}_p)$. First, we observe that the order of H is divisible by p. Indeed, otherwise by the version of Jordan's theorem mentioned above, there would exist an abelian normal subgroup $N \subset H$ of index dividing j. Then $\rho_p(\Gamma^{(j)}) \subset N$, and therefore $\rho_p(\Phi) = \{1\}$; a contradiction. This means that if we define H^+ and $\widetilde{H}$ as in Nori's theorem, then $\widetilde{H} \neq \{1\}$, hence the Lie algebra $\widetilde{\mathfrak{h}}$ of $\widetilde{H}$ is a nonzero subspace of $\underline{\mathfrak{g}}^{(p)}$. On the other hand, by our construction $\tilde{H}$ is normalized by $\rho_p(\Gamma)$, so the space $\widetilde{\mathfrak{h}}$ is $\mathrm{Ad}\, \rho_p(\Gamma)$-invariant. Combining this with the absolute irreducibility of the latter, we obtain that $\tilde{\mathfrak{h}} = \underline{\mathfrak{g}}^{(p)}$, i.e. $\tilde{H} = \underline{G}^{(p)}$. Furthermore, since G is simply connected, so is $\underline{G}^{(p)}$, and therefore by the affirmative answer to the Kneser-Tits conjecture over finite fields, we have

$$\underline{G}^{(p)}(\mathbb{F}_p) = \underline{G}^{(p)}(\mathbb{F}_p)^+.$$

Invoking Nori's theorem, we obtain

$$H = \widetilde{H}(\mathbb{F}_p)^+ = \underline{G}^{(p)}(\mathbb{F}_p)^+ = \underline{G}^{(p)}(\mathbb{F}_p),$$

as required.

A far-reaching generalization of Theorem 6.2 was given by B. Weisfeiler. We will state it using the original notation.

Theorem 6.7. *Let k be an algebraically closed field of characteristic $\neq 2, 3$, and let G be an almost simple, connected and simply connected algebraic group defined over k. Let Γ be a Zariski-dense finitely generated subgroup of $G(k)$, and let A be the subring of k generated by the traces* $\mathrm{tr}\, \mathrm{Ad}\, \gamma$ *for $\gamma \in \Gamma$. Then there exists a nonzero $b \in A$, a subgroup $\Gamma' \subset \Gamma$ of finite index, and a structure G_{A_b} of a group scheme over A_b on G such that $\Gamma' \subset G_{A_b}(A_b)$ and Γ' is dense in $G_{A_b}(\widehat{A_b})$.*

(Here A_b denotes the localization of A with respect to b, and $\widehat{A_b}$ the profinite completion of the ring A_b, i.e. the profinite completion with respect to the topology given by all ideals of finite index.

7. Applications and generalizations

Double cosets of the adele groups

Generic elements Let G be a semi-simple algebraic group over a field K. Fix a maximal K-torus T of G, and let $\Phi(G,T)$ and $W(G,T)$ denote the corresponding root system and the Weyl group. The natural action of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$, where $\overline{K}$ is a fixed separable closure of K, on the character group $X(T)$ gives rise to a group homomorphism

$$\theta_T \colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(\Phi(G,T))$$

that factors through the Galois group $\mathrm{Gal}(K_T/K)$ of the minimal splitting field K_T of T in $\overline{K}$ inducing an *injective* homomorphism $\bar{\theta}_T \colon \mathrm{Gal}(K_T/K) \to \mathrm{Aut}(\Phi(G,T))$. We say that T is *generic* over K if

$$\theta(\mathrm{Gal}(\overline{K}/K)) \supset W(G,T).$$

Furthermore, a regular semi-simple element $g \in G(K)$ is called K-*generic* if the K-torus $T = Z_G(g)^\circ$ (the connected component of the centralizer of g) is generic over K.

Theorem 7.1. ([31], [35]) *Let G be an absolutely almost simple algebraic group over a finitely generated field K. Then any finitely generated Zariski-dense subgroup $\Gamma \subset G(K)$ contains a generic element of infinite order.*

In [31], we considered the case of an arbitrary semi-simple algebraic group G over a finitely generated field K, and proved the existence, in an arbitrary finitely generated Zariski-dense subgroup $\Gamma \subset G(K)$, of generic elements without components of finite order (where the components are understood in terms of the decomposition $G = G_1 \cdots G_d$ as an almost direct product of absolutely almost simple groups). The argument that we will sketch below, assuming G to be absolutely almost simple, used the approximation considerations in the spirit of Lemma 6.1. In [35] this argument was extend to an absolutely almost simple group G over a finitely generated field K of positive characteristic using the results of Pink [21], [22]. We note that it was also shown in [35] that if $g \in \Gamma$ is a generic element then there exists a finite index subgroup $\Delta \subset \Gamma$ such that the whole coset $g\Delta$ consists entirely of generic elements.

Sketch of proof of Theorem 7.1. Let G be an absolutely almost simple simply connected algebraic group over a finitely generated field K of characteristic zero. Given two maximal tori of G defined over some extension F/K, there exists $g \in G(\overline{F})$ such that $T_2 = \iota_g(T_1)$ where $\iota_g(x) = gxg^{-1}$. Then ι_g induces an isomorphism between the Weyl groups $W(G, T_1)$ and $W(G, T_2)$. A different choice of g will change this isomorphism by an inner automorphism of the Weyl group, implying that there is a *canonical bijection* between the sets $[W(G, T_1)]$ and $[W(G, T_2)]$ of conjugacy classes in the respective groups; we will denote this bijection by ι_{T_1,T_2}. Moreover, if we let $\iota_g^*\colon X(T_2) \to X(T_1)$ denote the corresponding isomorphism of the character groups, then ι_g^* takes $\Phi(G, T_2)$ to $\Phi(G, T_1)$, and if we identify $\mathrm{Aut}(\Phi(G, T_1))$ with $\mathrm{Aut}(\Phi(G, T_2))$ using

$$\iota_g^{\natural}\colon \alpha \mapsto (\iota_g^*)^{-1} \circ \alpha \circ \iota_g^* \quad \text{for} \quad \alpha \in \mathrm{Aut}(\Phi(G, T_1)),$$

then the following holds: *if $g \in G(E)$, where E is an extension of F, then for any $\sigma \in \mathrm{Gal}(\overline{E}/E)$ we have*

$$\iota_g^{\natural}(\theta_{T_1}(\sigma)) = \theta_{T_2}(\sigma) \tag{8}$$

in the above notations.

Next, we will the following result that enables us to embed a given finitely generated field of characteristic zero into p-adic fields.

Proposition 7.2. ([31, Proposition 1]) *Let $\mathcal{K}$ be a finitely generated field of characteristic zero, and let $\mathcal{R} \subset \mathcal{K}$ be a finitely generated subring. Then there exists an infinite set of primes Π such that for each $p \in \Pi$ there exists an embedding $\varepsilon\colon \mathcal{K} \hookrightarrow \mathbb{Q}_p$ with the property $\varepsilon_p(\mathcal{R}) \subset \mathbb{Z}_p$.*

We will also need the following immediate consequence of the Inverse Function Theorem.

Lemma 7.3. ([35, Lemma 3.1]) *Let G be a semi-simple algebraic group over a field $\mathcal{K}$ which is complete with respect to a discrete valuations v. Fix a maximal $\mathcal{K}$-torus T of G, let T_{reg} denote the Zariski-open set of regular elements, and consider the regular map*

$$\psi\colon G \times T_{\mathrm{reg}} \to G, \quad (g, t) \mapsto gtg^{-1}.$$

Then the map

$$\psi_{\mathcal{K}}\colon G(\mathcal{K}) \times T_{\mathrm{reg}}(\mathcal{K}) \to G(\mathcal{K})$$

induced on $\mathcal{K}$-points is open for the topology defined by v.

The final preparation step is contained in the following.

Lemma 7.4. *Let G be an absolutely almost simple simply connected* split *group over $\mathbb{Q}_p$, let T_0 be a maximal $\mathbb{Q}_p$-torus of G, and let $[w_0]$ be a conjugacy class in $W(G, T_0)$. Then there exists a maximal $\mathbb{Q}_p$-torus T of G such that $\iota_{T_0,T}([w_0])$ intersects $\theta_T(\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p))$*

Indeed, by our assumption there exists a maximal torus T_1 of G that splits over $\mathbb{Q}_p$, and we let $[w_1] = \iota_{T_0,T_1}([w_0])$. Since T_1 splits, we can pick a representative n_1 for w_1 in the normalizer $N_G(T_1)(\mathbb{Q}_p)$. The Galois group $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p)$ of the maximal unramified extension is isomorphic to $\widehat{\mathbb{Z}}$ by the map that sends the Frobenius automorphism φ to $1 \in \widehat{\mathbb{Z}}$. So, there exists a (continuous) homomorphism $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \to N_G(T_1)(\mathbb{Q}_p)$ that send φ to n_1. Lift this homomorphism to a homorphism $\xi\colon \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to N_G(T_1)(\mathbb{Q}_p)$. One can view ξ as a Galois cocycle with values in G, and since $H^1(\mathbb{Q}_p, G) = 1$ there exists $h \in G(\overline{Q_p})$ such that

$$\xi(\sigma) = h^{-1}\sigma(h) \quad \text{for all} \quad \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p).$$

Then a direct computation shows that the maximal torus $T := hT_1h^{-1}$ is defined over $\mathbb{Q}_p$ and for any lift $\tilde{\varphi} \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ of the Frobenius we have

$$\theta_T(\tilde{\varphi}) \in \iota_{T_1,T}([w_1]) = \iota_{T_0,T}([w_0]),$$

giving our claim. □

We are now in a position to complete the proof of Theorem 7.1. Without loss of generality we may assume G to be simply connected. Fix a maximal K-torus T_0 of G, and let $[w_1], \ldots, [w_r]$ denote all nontrivial conjugacy classes of $W(G, T_0)$. Let $\mathcal{K}$ be a finite extension of K over which G splits. Fix a matrix realization $G \subset \mathrm{GL}_n$. Since Γ is finitely generated, we can find a finitely generated subring $\mathcal{R} \subset \mathcal{K}$ such that $\Gamma \subset \mathrm{GL}_n(\mathcal{R})$. Using Proposition 7.2, we can find r primes $p_1, \ldots, p_r$ such that for each $i = 1, \ldots, r$ there exists an embedding $\varepsilon_{p_i}\colon \mathcal{K} \hookrightarrow \mathbb{Q}_{p_i}$ with the property $\varepsilon_{p_i}(\mathcal{R}) \subset \mathbb{Z}_{p_i}$. Then, in particular, Γ is not discrete in $G(\mathbb{Q}_{p_i})$, and then the proof of Lemma 6.1 shows that the closure $\overline{\Gamma}$ of the image of the diagonal embedding

$$\Gamma \hookrightarrow \prod_{i=1}^{r} G(\mathbb{Q}_{p_i})$$

is open. Now, using Lemma 7.4, for each $i = 1, \ldots, r$ we can a maximal $\mathbb{Q}_p$-torus T_i such that

$$\theta_{T_i}(\mathrm{Gal}(\overline{\mathbb{Q}_{p_i}}/\mathbb{Q}_{p_i})) \cap \iota_{T_0,T_i}([w_i]) \neq \emptyset. \tag{9}$$

By Lemma 7.3, for $\psi^{(i)}\colon G \times T_{i\,\mathrm{reg}} \to G$, $(g, t) \mapsto gtg^{-1}$, the set

$$U_i := \psi^{(i)}_{\mathbb{Q}_{p_i}}(G(\mathbb{Q}_{p_i}) \times T_{i\,\mathrm{reg}}(\mathbb{Q}_{p_i}))$$

is open and obviously intersects every open subgroup in $G(\mathbb{Q}_{p_i})$. It follows that $\prod_{i=1}^r U_i$ intersects $\overline{\Gamma}$, hence also Γ. We claim that any

$$g \in \Gamma \bigcap \prod_{i=1}^{r} U_i$$

(which can be chosen to have infinite order) is K-generic. Indeed, let $T = Z_G(g)^\circ$. Applying (8) and (9), we see that the conjugacy class $\iota_{T_0,T}([w_i])$ of $W(G, T)$ intersects

$$\theta_T(\mathrm{Gal}(\overline{\mathbb{Q}_{p_i}}/\mathbb{Q}_{p_i})) \subset \theta_T(\mathrm{Gal}(\overline{K}/K)),$$

for each $i = 1, \ldots, r$. Thus, the subgroup

$$\theta_T(\mathrm{Gal}(\overline{K}/K)) \cap W(G, T)$$

intersects *every* conjugacy class of $W(G, T)$. Applying an elementary fact (Jordan's theorem) from group theory, we obtain that

$$\theta_T(\mathrm{Gal}(\overline{K}/K)) \supset W(G, T),$$

as required. □

Strong approximation over fields other than global.

References

1. *Algebraic Number Theory*, ed. J.W.S. Cassels, A. Fröhlich, 2nd edition, London Math. Soc., 2010.
2. H. Behr, *Arithmetic groups over function fields. I. A complete characterization of finitely generated and finitely presented arithmetic subgroups of reductive algebraic groups*, J. Reine Angew. Math. **495**(1998), 79-118.
3. A. Borel, *Linear Algebraic Groups*, 2nd edition, GTM 126, Springer, 1991.
4. A. Borel, J. Tits, *Groupes réductifs*, Publ. math. IHES **27**(1965), 55-150.
5. A. Borel, J. Tits, *Compléments à l'article: "Groupes réductifs"*, Publ. math. IHES **41**(1972), 253-276.
6. M.V. Borovoi, *Strong approximation for homogeneous spaces*, Dokl. Akad. Nauk BSSR **33**(1989), no. 4, 293-296.
7. F. Bruhat, J. Tits, *Groupes algébriques sur un corps local. Chapitre III. Compléments et applications à la cohomologie galoisienne*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **34**(1987), no. 3, 671-698.
8. K.-U. Bux, R. Köhl, S. Witzel, *Higher finiteness properties of reductive arithmetic groups in positive characteristic: the rank theorem*, Ann. of Math. **177**(2013), no. 1, 311-366.
9. B. Conrad, *Weil and Grothendieck approaches to adelic points*, Enseign. Math. (2) **58**(2012), no. 1-2, 61-97.
10. P. Gille, *Le problème de Kneser-Tits*, Séminaire Bourbaki, exp. 983(2007/2008), Astérisque No. 326(2009), 39-81.
11. M. Kneser, *Starke Approximation in algebraischen Gruppen. I*, J. Reine Angew. Math. **218**(1965), 190-203.
12. S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.
13. S. Lang, *Algebraic Number Theory*, 2nd edition, GTM 110, Springer, 1994.
14. S. Lang, A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76**(1954), 819-827.
15. G.A. Margulis, *Cobounded subgroups in algebraic groups over local fields*, Funct. Anal. Appl. **11**(1977), no. 2, 119-132.
16. G.A. Margulis, *Discrete subgroups of semisimple Lie groups*, Springer, 1991.
17. G.A. Margulis, G.A. Soifer, *Maximal subgroups of infinite index in finitely generated linear groups*, J. Algebra **69**(1981), no. 1, 1-23.
18. C.R. Matthews, L.N. Vaserstein, and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups I*, Proc. London Math. Soc. **48**, no. 3, 514-532.
19. H. Minchev, *Strong approximation for varieties over an algebraic number field*, Dokl. Akad. Nauk BSSR **33**(1989), no. 1, 5-8.
20. M.V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. math. **88**(1987), no. 2, 257-275.
21. R. Pink, *Compact subgroups of linear algebraic groups*, J. Algebra **206**(1998), no. 2, 438-504.
22. R. Pink, *Strong approximation for Zariski dense subgroups over arbitrary global fields*, Comment. math. Helv. **75**(2000), no. 4, 608-643.
23. R. Pink, *On Weil restriction of reductive groups and a theorem of Prasad*, Math. Z. **248**(2004), no. 3, 449-457.
24. V.P. Platonov, *The problem of strong approximation and the Kneser-Tits hypothesis for algebraic groups*, Math. USSR Izv. **3**(1969), 1139-1147.
25. V.P. Platonov, *A supplement to the paper "The problem of strong approximation and the Kneser-Tits hypothesis for algebraic groups"*, Math. USSR Izv. **4**(1970), no. 4, 784-786.
26. V.P. Platonov, A.S. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, 1994.
27. G. Prasad, *Strong approximation for semi-simple groups over function fields*, Ann. math. **105**(1977), 553-572.
28. G. Prasad, *Elementary proof of a theorem of Bruhat-Tits-Rousseau and of a theorem of Tits*, Bull. Soc. Math. France **110**(1982), no. 2, 197-202.
29. G. Prasad, M.S. Raghunathan, *On the Kneser-Tits problem*, Comment. math. Helv. **60**(1985), no. 1, 107-121.
30. G. Prasad, A.S. Rapinchuk, *Computation of the metaplectic kernel*, Publ. math. IHES **84**(1996), 91-187.
31. G. Prasad, A.S. Rapinchuk, *Existence of irreducible* $\mathbb{R}$*-regular elements in Zariski-dense subgroups*, Math. Res. Lett. **10**(2003), no. 1, 21-32.
32. G. Prasad, A.S. Rapinchuk, *Irreducible Tori in Semisimple Groups*, IMRN, 2001, No. 23.
33. G. Prasad, A.S. Rapinchuk, *Developments on the congruence subgroup problem after the work of Bass, Milnor, and Serre*, in Collected papers of John Milnor, vol. V "Algebra," 307-326, AMS, 2010.
34. G. Prasad, A.S. Rapinchuk, *On the congruence kernel for simple algebraic groups*, Proc. Steklov Inst. Math. **292**(2016), 216-246.
35. G. Prasad, A.S. Rapinchuk, *Generic elements of a Zariski-dense subgroup form an open set*, Trans. Moscow Math. Soc. **78**(2017), 299-314.
36. M.S. Raghunathan, *Discrete subgroups of Lie groups*, Springer, 1972.
37. A.S. Rapinchuk, *The congruence subgroup problem for algebraic groups and strong approximation in affine varieties*, Dokl. Akad. Nauk BSSR **32**(1988), no. 7, 581-584.
38. A.S. Rapinchuk, *The congruence subgroup problem for algebraic groups*, Habilitationsschrift, Institute of Mathematics of the Academy of Sciences of the BSSR, Minsk, 1990.
39. A.S. Rapinchuk, *Strong approximation for algebraic groups*, Thin Groups and Superstrong Approximation, MSRI Publications **61**, Cambridge Univ. Press, 2014.
40. J.-P. Serre, *Lie Algebras and Lie Groups*, Benjamin, 1965.
41. J.-P. Serre, *Abelian* ℓ*-adic representations and elliptic curves*, Benjamin, 1968.
42. J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Vieweg, Braunschweig, 1997.

43. G.A. Soifer, T.N. Venkataramana, *Finitely generated profinitely dense free groups in higher rank semi-simple groups*, Transform. Groups **5**(2000), no. 1, 93-100.

44. J. Tits, *Algebraic and abstract simple groups*, Ann. math. **80**(1964), 313-329.

45. A. Weil, *Adeles and Algebraic Groups*, Birkhäuser, 1982.

46. B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Ann. math. **120**(1984), no. 2, 271-315.