Труды Москов. Матем. Общ.
Том 78 (2017), вып. 2

Trans. Moscow Math. Soc.
2017, Pages 299–314
http://dx.doi.org/10.1090/mosc/274
Article electronically published on December 1, 2017

GENERIC ELEMENTS OF A ZARISKI-DENSE SUBGROUP FORM AN OPEN SUBSET

G. PRASAD AND A. S. RAPINCHUK

Dedicated to E. B. Vinberg
on his 80th birthday

Abstract. Let G be a semisimple algebraic group over a finitely generated field K of characteristic zero, and let $\Gamma \subset G(K)$ be a finitely generated Zariski-dense subgroup. In this paper we prove that the set of *K-generic elements* of Γ (whose existence was established earlier by the authors in *Existence of irreducible $\mathbb{R}$-regular elements in Zariski-dense subgroups*, Math. Res. Lett. **10** (2003), no. 1, 21–32, is open in the profinite topology of Γ. We then extend this result to the fields of positive characteristic, and also prove the existence of generic elements in this case.

1. Introduction

This is a companion paper to [PR03] where we first proved the existence of generic elements in an arbitrary Zariski-dense subgroup of the group of points of a semi-simple algebraic group over a finitely generated field of characteristic zero. Since then generic elements have been used in a variety of situations, in particular, to resolve some long-standing problems about isospectral locally symmetric spaces [PR09] (see also [PR14] for a survey). This prompted us to try to understand the structure of the set of all generic elements in a given (finitely generated) Zariski-dense subgroup. The goal of this paper is to establish a rather surprising fact that this set is open in the profinite topology of the subgroup — see below for a more general/precise statement which applies to fields of any characteristic. We begin by recalling the relevant definitions.

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 $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, where K^{sep} is a fixed separable closure of K, on the character group $X(T)$ of T gives rise to a group homomorphism

$$\theta_T\colon \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(\Phi(G,T))$$

that factors through the Galois group $\mathrm{Gal}(K_T/K)$ of the minimal splitting field K_T of T in K^{sep} 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 $\theta_T(\mathrm{Gal}(K^{\mathrm{sep}}/K)) \supset W(G,T)$. 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 (recall that $g \in T(K)$). Some possible variations of this definition are discussed in [PR14, 9.4], but all the versions are equivalent for semi-simple 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).

2010 *Mathematics Subject Classification.* Primary 20G15, 22E20.
Key words and phrases. Zariski-dense subgroups, generic elements, profinite topology.

Now, fix a matrix K-realization $G \subset \mathrm{GL}_n$, and let R be a subring of K. Quite often, by the *congruence topology* on the group $G(R) := G(K) \cap \mathrm{GL}_n(R)$ one understands the topology having as a fundamental system of neighborhoods of the identity the family of congruence subgroups

$$G(R, \mathfrak{a}) := G(R) \cap \mathrm{GL}_n(R, \mathfrak{a}),$$

where

$$\mathrm{GL}_n(R, \mathfrak{a}) = \{X \in \mathrm{GL}_n(R) \mid X \equiv I_n \pmod{\mathfrak{a}}\},$$

in the obvious notation, for *all* nonzero ideals $\mathfrak{a}$ of R. However, in this note we reserve this term for the (generally) weaker topology defined by the congruence subgroup $G(R, \mathfrak{a})$, where $\mathfrak{a} \subset R$ is an ideal of *finite index*, that is the quotient $R/\mathfrak{a}$ is finite. Any such congruence subgroup is obviously a normal subgroup of finite index in $G(R)$, and consequently the topology induced by the congruence topology in this sense on any subgroup $\Gamma \subset G(R)$ is generally coarser than the *profinite topology* of Γ defined by *all* normal subgroups $N \subset \Gamma$ of finite index.

We can now formulate the main result.

Theorem 1. *Let G be a semisimple algebraic group defined over a finitely generated field K of any characteristic, $R \subset K$ be a finitely generated subring and let $\Gamma \subset G(R)$ be a subgroup which is Zariski-dense in G. Then the set $\Delta(\Gamma, K)$ of regular semisimple K-generic elements is open in Γ in the congruence topology defined by ideals $\mathfrak{a} \subset R$ of finite index. In particular, $\Delta(\Gamma, K)$ is open in Γ in the profinite topology.*

Corollary. *Let G be a semisimple algebraic group defined over a finitely generated field K, and let $\Gamma \subset G(K)$ be a finitely generated Zariski-dense subgroup. Then the set $\Delta(\Gamma, K)$ is open in Γ in the profinite topology.*

The proof of Theorem 1 requires a suitable generalization of Chebotarev's Density Theorem, and in § 2 we give this generalization for fields of characteristic zero — see Proposition 2.1. Then in § 3 we combine this proposition with some techniques developed earlier in [PR03] to prove Theorem 1 in characteristic zero. The argument easily extends to positive characteristic provided that one can generalize Chebotarev's Theorem to this case; we establish the required generalization in § 4.

While Theorem 1 gives the *openness* of the set $\Delta(\Gamma, K)$ of regular semi-simple K-generic elements in the profinite topology of a finitely generated Zariski-dense subgroup $\Gamma \subset G(K)$, its proof does not automatically yield the *nonemptiness* of $\Delta(\Gamma, K)$. As we already pointed out, the existence of generic elements was first established in [PR03] over fields of characteristic zero — for the reader's convenience we summarize this argument in Remark 3.2. One of its essential components is a form of weak approximation that asserts that for a finite set V of discrete valuations of K that is constructed in the proof, the closure of the image of the diagonal embedding

$$\Gamma \hookrightarrow G_V = \prod_{v \in V} G(K_v)$$

is open. In characteristic zero V is selected so that the completions K_v for $v \in V$ are the p-adic fields $\mathbb{Q}_p$ for pairwise distinct primes p, and then the required openness is an easy consequence of the Zariski-density of Γ. In characteristic $p > 0$, this property becomes significantly more delicate. If $p > 3$, then the argument from [PR03] can still be made to work using the strong approximation theorem of B. Weisfeiler [Wei84]. Additional complications in characteristics 2 and 3 come from so-called *exceptional isogenies*, whose existence render the openness statement invalid even after passing to the universal cover. For this reason, the existence of generic elements over fields of positive characteristic remained unproven until recently. J. Schwartz in his dissertation [Sch14] used the

approximation results of R. Pink [Pin98, Pin00] to prove the existence of generic elements over global fields of all characteristics. Here we will establish the following general result for all absolutely almost simple groups.

Theorem 2. *Let G be a connected absolutely almost simple algebraic group over a finitely generated field K (of any characteristic), and let Γ' be a Zariski-dense subsemigroup of $G(K)$ that contains an element of infinite order. Then Γ' contains a regular semisimple element $\gamma' \in \Gamma'$ of infinite order that is K-generic.*

We will prove Theorem 2 in § 5. The argument heavily relies on the results of Pink [Pin98] which we will briefly review below for the reader's convenience.

Notation. Given a variety X defined over a field K, and a field extension L of K, we will denote by X_L, or $(X)_L$, the L-variety obtained from X by base change $K \hookrightarrow L$. If X is an algebraic K-group, by L-torus of X, we will mean a L-torus of X_L.

2. A generalization of Chebotarev's density theorem

Proposition 2.1. *Let R be a finitely generated subring of a finitely generated field K of characteristic zero, and let L be a finite Galois extension of K with Galois group $\mathcal{G} = \mathrm{Gal}(L/K)$. Fix a conjugacy class $\mathcal{C}$ of $\mathcal{G}$. Then there exists an infinite set of primes Π such that for each $p \in \Pi$ there exists an embedding $\iota_p \colon K \hookrightarrow \mathbb{Q}_p$ with the following properties:*

(1) *$\iota_p(R) \subset \mathbb{Z}_p$,*

(2) *if v denotes the discrete valuation of K obtained by pulling back the p-adic valuation of $\mathbb{Q}_p$ (so that $K_v = \mathbb{Q}_p$), then any extension $w|v$ to L is unramified and the Frobenius automorphism of L_w/K_v belongs to $\mathcal{C}$.*

Proof. In this argument, for a (monic) polynomial $f(x) \in A[x]$ over an integral domain A we let $\delta_f \in A$ denote its discriminant. Without loss of generality, we may assume that K is the field of fractions of R. Using Noether's Normalization Theorem, we can find algebraically independent $t_1, \dots, t_r \in \mathbb{Q}R$ so that $\mathbb{Q}R$ is integral over $\mathbb{Q}[t_1, \dots, t_r]$. In fact, we may further assume $t_1, \dots, t_r \in R$ and then pick a finite set of primes S such that for $p_S := \prod_{p \in S} p$, the localization $\mathbb{Z}_S = \mathbb{Z}[p_S^{-1}]$ of $\mathbb{Z}$ away from S, we have that $\mathbb{Z}_S R$ is integral over $\mathbb{Z}_S[t_1, \dots, t_r]$. Now, set $k = \mathbb{Q}(t_1, \dots, t_r)$ and let E denote the Galois closure of L over k with Galois group $\mathcal{H} = \mathrm{Gal}(E/k)$. We can pick a primitive element α for E over k whose minimal polynomial f is of the form

$$f(x) = x^n + z_{n-1}(t_1, \dots, t_r)x^{n-1} + \cdots + z_0(t_1, \dots, t_r)$$

with $z_i(t_1, \dots, t_r) \in \mathbb{Z}[t_1, \dots, t_r]$. Now, fix $\sigma \in \mathcal{C}$, and let $\widetilde{\sigma} \in \mathcal{H}$ be an automorphism that acts trivially on K and restricts to σ on L. Pick polynomials $g_0, \dots, g_{n-1}$ and $h \in \mathbb{Z}_S[t_1, \dots, t_r]$ so that

$$\widetilde{\sigma}(\alpha) = \sum_{j=0}^{n-1} c_j \alpha^j, \quad \text{where} \quad c_j = \frac{g_j}{h}. \tag{1}$$

Using Hilbert's Irreducibility Theorem (cf. [Ser92b, Ch. 3] and references therein), we can find $(a_1^0, \dots, a_r^0) \in \mathbb{Q}^r$ such that $h(a_1^0, \dots, a_r^0) \neq 0$ and the polynomial

$$f_0(x) := x^n + z_{n-1}(a_1^0, \dots, a_r^0)x^{n-1} + \cdots + z_0(a_1^0, \dots, a_r^0) \in \mathbb{Q}[x]$$

is irreducible. Then, if we write the discriminant δ_f as a polynomial in $t_1, \dots, t_r$, we automatically have $\delta_f(a_1^0, \dots, a_r^0) \neq 0$. Let $\mathfrak{m}_0$ be the maximal ideal of $\mathbb{Q}[t_1, \dots, t_r]$ generated by $t_1 - a_1^0$, …, $t_r - a_r^0$, let A be the corresponding local ring $\mathbb{Q}[t_1, \dots, t_r]_{\mathfrak{m}_0}$ with the maximal ideal $\mathfrak{m} = \mathfrak{m}_0 A$, and let B be the integral closure of A in E. By

construction, $\alpha \in B$ and the discriminant of the basis $1, \alpha, \ldots, \alpha^{n-1}$ is a unit in A. So, a standard argument using traces shows that in fact $B = A[\alpha]$. The specialization homomorphism $\psi\colon A \to \mathbb{Q}$ with kernel $\mathfrak{m}$ that sends t_i to a_i^0 for $i = 1, \ldots, r$, extends to a homomorphism $\widetilde{\psi}\colon B \to \overline{\mathbb{Q}}$ into the algebraic closure of $\mathbb{Q}$ (see [Lan02, Ch. VII, Proposition 3.1]); note that $\mathfrak{M} := \operatorname{Ker}\widetilde{\psi}$ is a maximal ideal of B lying above $\mathfrak{m}$. Let $E_0 = \widetilde{\psi}(B) \simeq B/\mathfrak{M}$; clearly, $E_0 = \mathbb{Q}(\alpha_0)$, where $\alpha_0 = \widetilde{\psi}(\alpha)$ is a root of f_0. Since f_0 is irreducible, we have

$$[E_0 : \mathbb{Q}] = n = [E : k]. \tag{2}$$

Furthermore, by [Lan02, Ch. VII, Proposition 2.5], the extension $E_0/\mathbb{Q}$ is normal and if we let $\mathcal{H}(\mathfrak{M})$ denote the decomposition subgroup of $\mathfrak{M}$ in $\mathcal{H}$, then the reduction of automorphism modulo $\mathfrak{M}$ yields a *surjective* homomorphism

$$\rho\colon \mathcal{H}(\mathfrak{M}) \to \operatorname{Gal}(E_0/\mathbb{Q}) =: \mathcal{H}_0.$$

Since according to (2) we have $|\mathcal{H}| = |\mathcal{H}_0|$, we conclude that $\mathcal{H}(\mathfrak{M}) = \mathcal{H}$, and $\rho\colon \mathcal{H} \to \mathcal{H}_0$ is actually an isomorphism. Let $\widetilde{\sigma}_0 := \rho(\widetilde{\sigma}) \in \mathcal{H}_0$.

Enlarging S if necessary, we may assume that $a_1^0, \ldots, a_r^0 \in \mathbb{Z}_S$ and $\delta_f(a_1^0, \ldots, a_r^0)$ and $h(a_1^0, \ldots, a_r^0)$ are p-adic units for all primes $p \notin S$. Let Π be the set of all primes $p \notin S$ such that the extension $E_0/\mathbb{Q}$ is unramified at p and for a suitable extension u of the p-adic place to E_0, the Frobenius automorphism $\operatorname{Fr}(u|p)$ of $(E_0)_u/\mathbb{Q}_p$ is $\widetilde{\sigma}_0$. By Chebotarev's Density Theorem (cf. [CF10, Ch. VII, 2.4]), the set Π is infinite, and we will show that it is as required.

Let $p \in \Pi$. By our construction, we can then pick an extension of the p-adic valuation u to E_0 such that $(E_0)_u/\mathbb{Q}_p$ is unramified with the Frobenius automorphism $\operatorname{Fr}(u|p)$ equal to $\widetilde{\sigma}_0$. Then u corresponds to an embedding $\varepsilon\colon E_0 \hookrightarrow \overline{\mathbb{Q}}_p$ into the algebraic closure of $\mathbb{Q}_p$, and we set $\mathcal{E} = \mathbb{Q}_p(\varepsilon(\alpha_0))$ (clearly, $\mathcal{E}$ is naturally identified with the completion $(E_0)_u$) and let φ be the Frobenius automorphism of $\mathcal{E}/\mathbb{Q}_p$. Let $\mathcal{O}$ (resp., $\mathfrak{p}$) be the valuation ring (resp., valuation ideal) in $\mathcal{E}$.

Now, pick $a_i^1 \in a_i^0 + p\mathbb{Z}_p$ for $i = 1, \ldots, r$ so that $a_1^1, \ldots, a_r^1$ are algebraically independent over $\mathbb{Q}$, and then let

$$f_1(x) := x^n + z_{n-1}(a_1^1, \ldots, a_r^1)x^{n-1} + \cdots + z_0(a_1^1, \ldots, a_r^1) \in \mathbb{Z}_p[x].$$

Note that $f_1(x) \equiv f_0(x) \pmod{p}$, so $\delta_{f_1} \equiv \delta_{f_0} \pmod{p}$ and therefore $\delta_{f_1} \not\equiv 0 \pmod{p}$. By construction $f_0(\varepsilon(\alpha_0)) = 0$, and consequently $f_1(\varepsilon(\alpha_0)) \equiv 0 \pmod{\mathfrak{p}}$. Since $\delta_{f_1} \not\equiv 0 \pmod{p}$, we have $f_1'(\varepsilon(\alpha_0)) \not\equiv 0 \pmod{\mathfrak{p}}$, and therefore by Hensel's Lemma, there exists a root $\alpha_1 \in \mathcal{O}$ of f_1 such that $\alpha_1 \equiv \varepsilon(\alpha_0) \pmod{\mathfrak{p}}$. We note that since $\delta_{f_0} \not\equiv 0 \pmod{\mathfrak{p}}$, we have $\mathcal{O} = \mathbb{Z}_p[\varepsilon(\alpha_0)]$ (cf. [Jan96, Ch. I, Theorem 7.5]), and therefore the residue field of $\mathcal{E}$ is generated over the prime subfield $\mathbf{F}_p$ by the image $\overline{\varepsilon(\alpha_0)} = \bar{\alpha}_1$. Since $\mathcal{E}/\mathbb{Q}_p$ is unramified, it follows that $\mathcal{E} = \mathbb{Q}_p(\alpha_1)$. Since $a_1^1, \ldots, a_r^1$ are algebraically independent over $\mathbb{Q}$, there is an embedding $k \hookrightarrow \mathbb{Q}_p$ sending t_i to a_i^1 for $i = 1, \ldots, r$. This embedding extends to a (dense) embedding $\iota\colon E \hookrightarrow \mathcal{E}$ sending α to α_1.

Claim. For $a \in E$, we have $\iota(\widetilde{\sigma}(a)) = \varphi(\iota(a))$.

Indeed, it is enough to prove this for $a = \alpha$. It follows from (1) that

$$\iota(\widetilde{\sigma}(\alpha)) = \sum_{j=0}^{n-1} c_j(a_1^1, \ldots, a_r^1)(\alpha_1)^j. \tag{3}$$

Clearly, we have

$$h(a_1^1, \ldots, a_r^1) \equiv h(a_1^0, \ldots, a_r^0) \pmod{p},$$

and in particular, $h(a_1^1, \dots, a_r^1)$ is a p-adic unit. It follows that for all $j = 0, \dots, n-1$, the elements $c_j(a_1^0, \dots, a_r^0)$ and $c_j(a_1^1, \dots, a_r^1)$ both lie in $\mathbb{Z}_p$ and are congruent modulo p. Applying to (1) the specialization map ψ, we obtain that

$$\widetilde{\sigma}_0(\alpha_0) = \sum_{j=0}^{n-1} c_j(a_1^0, \dots, a_r^0)(\alpha_0)^j. \tag{4}$$

Since $\alpha_1 \equiv \varepsilon(\alpha_0) \pmod{\mathfrak{p}}$, we have

$$\varphi(\iota(\alpha)) = \varphi(\alpha_1) \equiv \varphi(\varepsilon(\alpha_0)) \pmod{\mathfrak{p}}.$$

On the other hand, since $\mathrm{Fr}(u|p) = \widetilde{\sigma}_0$, we have $\varphi(\varepsilon(\alpha_0)) = \varepsilon(\widetilde{\sigma}_0(\alpha_0))$. Combining this with (3), (4) and the fact that $\alpha_1 \equiv \varepsilon(\alpha_0) \pmod{\mathfrak{p}}$, we conclude that

$$\varphi(\iota(\alpha)) \equiv \iota(\widetilde{\sigma}(\alpha)) \pmod{\mathfrak{p}}. \tag{5}$$

Now, both $\iota(\widetilde{\sigma}(\alpha))$ and $\varphi(\iota(\alpha))$ are roots of $f_1(x)$. But since $\delta_{f_1} \not\equiv 0$, the polynomial f_1 has no multiple roots modulo $\mathfrak{p}$, so (5) implies that $\iota(\widetilde{\sigma}(\alpha)) = \varphi(\iota(\alpha))$ as required.

By construction, $\widetilde{\sigma}$ acts on K trivially. So, it follows from the above claim that $\iota(K) \subset \mathcal{E}^{\varphi} = \mathbb{Q}_p$ because φ generates the Galois group $\mathrm{Gal}(\mathcal{E}/\mathbb{Q}_p)$. Since $\iota(\mathbb{Z}_S[t_1, \dots, t_r]) \subset \mathbb{Z}_p$ and $\mathbb{Z}_S R$ is integral over $\mathbb{Z}_S[t_1, \dots, t_r]$, we conclude that $\iota(R) \subset \mathbb{Z}_p$, so for ι_p we can take the restriction of ι to K. It follows from our construction that if we let w_0 denote the pullback to L of the extension of the p-adic valuation to $\mathcal{E}$ so that the completion L_{w_0} can be identified with the compositum $\iota(L)\mathbb{Q}_p$ inside $\mathcal{E}$, then L_{w_0}/K_v is unramified and with the Frobenius automorphism $\mathrm{Fr}(w_0|v) = \sigma$. Since L/K is a Galois extension, we conclude that *any* extension $w|v$ is unramified and the Frobenius $\mathrm{Fr}(w|v)$ belongs to the conjugacy class $\mathcal{C}$. □

Remark 2.2. Proposition 2.1 can be derived from a generalization of Chebotarev's Theorem to the case of schemes of finite type over $\mathbb{Z}$ (see [Ser12, Ch. 9] and references therein). The above argument, however, shows a way to bypass this (rather technical) generalization and obtain the required proposition using only the classical form of Chebotarev's Theorem.

3. Proof of Theorem 1

Lemma 3.1. *Let G be a semisimple algebraic group over a field $\mathcal{K}$ which is complete with respect to a discrete valuation 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 by ψ on $\mathcal{K}$-points is open for the topology defined by v.

Indeed, a direct computation shows that the differential $d_{(g,t)}\psi$ is surjective for any $(g, t) \in G \times T_{\mathrm{reg}}$. So, our assertion follows from the Inverse Function Theorem (cf. [PR94, § 3.1], [Ser92a, Part II, Ch. III]).

We will now recall one construction introduced in [PR03]. Let G be a semisimple K-group, and let T_1 and T_2 be two maximal tori of G defined over some extension F/K. Then 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

$\iota_g^*\colon \mathrm{X}(T_2) \to \mathrm{X}(T_1)$ 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 $\iota_g^\natural\colon \alpha \mapsto (\iota_g^*)^{-1} \circ \alpha \circ \iota_g^*$, for $\alpha \in \mathrm{Aut}(\Phi(G,T_1))$, then the following holds: *if $g \in G(E)$, where E is an extension of F, then for any $\sigma \in \mathrm{Gal}(\bar{E}/E)$ we have*

$$\iota_g^\natural(\theta_{T_1}(\sigma)) = \theta_{T_2}(\sigma) \tag{6}$$

in the above notations.

Proof of Theorem 1. It is enough to show that the set $\Delta(\Gamma,K)$ of regular semisimple K-generic elements in $\Gamma = G(R)$ is open in Γ in the congruence topology defined by ideals $\mathfrak{a} \subset R$ of finite index. Let $g_0 \in \Delta(\Gamma,K)$. Then for the maximal K-torus $T_0 = Z(g_0)^\circ$ we have the inclusion

$$\bar{\theta}_{T_0}(\mathrm{Gal}(K_{T_0}/K)) \supset W(G,T_0)$$

in the above notations. Let $w_1,\dots,w_r$ be a set representative of all nontrivial conjugacy classes of $W(G,T_0)$, let $\widetilde{\sigma}_i \in \mathrm{Gal}(\bar{K}/K)$ be such that $\theta_{T_0}(\widetilde{\sigma}_i) = w_i$ for $i = 1,\dots,r$, and let σ_i be the image of $\widetilde{\sigma}_i$ in $\mathrm{Gal}(K_{T_0}/K)$ (so that $\bar{\theta}_{T_0}(\sigma_i) = w_i$). Applying Proposition 2.1 to $L = K_{T_0}$, we can find r distinct primes $p_1,\dots,p_r$ such that for each $i \in \{1,\dots,r\}$ there is an embedding $\iota_{p_i}\colon K \hookrightarrow \mathbb{Q}_{p_i}$ such that $\iota_{p_i}(R) \subset \mathbb{Z}_{p_i}$ and for a suitable extension $u_i|v_{p_i}$, where v_{p_i} is the pullback of the p_i-adic valuation on $\mathbb{Q}_{p_i}$, the extension L_{u_i} of $K_{v_{p_i}} = \mathbb{Q}_{p_i}$ is unramified with the Frobenius automorphism σ_i. According to Lemma 3.1, for each $i \in \{1,\dots,r\}$, the set

$$\mathcal{U}_{p_i} := \psi_{\mathbb{Q}_{p_i}}\big(G(\mathbb{Q}_{p_i}) \times (T_0)_{\mathrm{reg}}(\mathbb{Q}_{p_i})\big), \quad \text{where } \psi_{\mathbb{Q}_{p_i}}(g,t) = gtg^{-1}$$

is open and obviously contains g_0. So, we can find $\ell_i \geqslant 1$ such that the coset $g_0 G(\mathbb{Z}_{p_i}, p_i^{\ell_i}\mathbb{Z}_{p_i})$ of the corresponding congruence subgroup is contained in $\mathcal{U}_{p_i}$. Set

$$\mathfrak{a} = \bigcap_{i=1}^{r} \big(R \cap \iota_{p_i}^{-1}(p_i^{\ell_i}\mathbb{Z}_{p_i})\big).$$

Clearly, $\mathfrak{a}$ is an ideal of R having finite index, and to conclude the proof we will show that $g_0\Gamma(\mathfrak{a}) \subset \Delta(\Gamma,K)$. Let $g \in g_0\Gamma(\mathfrak{a})$. Then by construction $g \in \mathcal{U}_{p_i}$ for all $i = 1,\dots,r$, and in particular g is a regular semi-simple element. Furthermore, if $T = Z_G(g)^\circ$, then for each $i = 1,\dots,r$ there exists $g_i \in G(\mathbb{Q}_{p_i})$ such that $\iota_{g_i}(T_0) = T$. It follows from (6) that $\iota_{g_i}^\natural(\theta_{T_0}(\widetilde{\sigma}_i)) = \theta_T(\widetilde{\sigma}_i)$, and therefore the conjugacy class $\iota_{T_0,T}([w_i])$ of $W(G,T)$ intersects

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

This being true for each $i = 1,\dots,r$, we conclude that the subgroup

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

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

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

as required. □

Remark 3.2. We would like to indicate that the above argument is parallel to the argument developed in [PR03] in order to prove the existence of K-generic elements in any Zariski-dense subgroup (and in fact those with special properties such as $\mathbb{R}$-regularity if $K \subset \mathbb{R}$). This indicates that the construction of generic elements from [PR03] in fact enables one to obtain *all of them*. More precisely, fix a K-torus T_0 of G and as above let $[w_1],\dots,[w_r]$ be all nontrivial conjugacy classes of $W(G,T_0)$. It follows from Proposition 2.1 that one can pick r distinct primes $p_1,\dots,p_r$ such that for each $i = 1,\dots,r$

there exists an embedding $\iota_i\colon K \hookrightarrow \mathbb{Q}_{p_i}$ such that $\iota_i(R) \subset \mathbb{Z}_{p_i}$ and G splits over $\mathbb{Q}_{p_i}$. Then one shows that there is a maximal $\mathbb{Q}_{p_i}$-torus T_i of $G/\mathbb{Q}_{p_i}$ such that

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

Let

$$\mathcal{U}_{p_i} = \psi_{\mathbb{Q}_{p_i}}\big(G(\mathbb{Q}_{p_i}) \times (T_i)_{\mathrm{reg}}(\mathbb{Q}_{p_i})\big), \quad \text{where } \psi_{\mathbb{Q}_{p_i}}(g,t) = gtg^{-1}.$$

We observe that $\mathcal{U}_{p_i}$ intersects every open subgroup of $G(\mathbb{Q}_{p_i})$. Since the p_i are distinct, a standard approximation argument shows that since Γ is Zariski-dense, its closure in $\prod_{i=1}^r G(\mathbb{Q}_{p_i})$ is open, and therefore $\Gamma \cap \prod_{i=1}^r \mathcal{U}_{p_i} \neq \varnothing$. Then the argument used in the proof of the above theorem shows that any element of this intersection is generic over K.

4. Positive characteristic case: Theorem 1

The argument given in § 3 is independent of the characteristic of the base field. So, to prove Theorem 1 in positive characteristic we only need to provide a suitable analogue of Proposition 2.1. It suffices to prove the following.

Proposition 4.1. *Let R be a finitely generated subring of an infinite finitely generated field K of characteristic $p > 0$, and let L/K be a finite Galois extension with Galois group $\mathcal{G} = \mathrm{Gal}(L/K)$. Fix a conjugacy class $\mathcal{C}$ of $\mathcal{G}$. Then there exists a (nontrivial) discrete valuation v on K such that the completion K_v is locally compact, R lies in the corresponding valuation ring $\mathcal{O}_v$, and for any extension $w|v$, the Frobenius automorphism of L_w/K_v belongs to $\mathcal{C}$.*

We will only indicate the changes that need to be made in the proof of Proposition 2.1. Again, we may (and we will) assume that the field of fractions of R coincides with K, and then find in R a separable transcendence basis $t_0, \dots, t_r$ for K over the prime subfield $\mathbb{F}_p$ (which means that K is a finite separable extension of $k := \mathbb{F}_p(t_0, \dots, t_r)$). Let E denote the Galois closure of L over k with Galois group $\mathcal{H} = \mathrm{Gal}(E/k)$. Set $A = \mathbb{F}_p[t_0]$ and $k_0 = \mathbb{F}_p(t_0)$, and pick a primitive element $\alpha \in E$ over k whose minimal polynomial is of the form

$$f(x) = x^n + z_{n-1}(t_1, \dots, t_r)x^{n-1} + \cdots + z_0(t_1, \dots, t_r),$$

where $z_i(t_1, \dots, t_r) \in A[t_1, \dots, t_r]$. We can find $h_1 \in A[t_1, \dots, t_r]$ so that the extension of the corresponding localizations $R_{h_1}/A[t_1, \dots, t_r]_{h_1}$ is integral. Next, pick a representative $\sigma \in \mathcal{C}$ and let $\widetilde{\sigma} \in \mathcal{H}$ be such that $\widetilde{\sigma}|L = \sigma$. There exist $g_0, \dots, g_{n-1}$ and $h_2 \in A[t_1, \dots, t_r]$ such that

$$\widetilde{\sigma}(\alpha) = \sum_{j=0}^{n-1} c_j \alpha^j, \quad \text{where } c_j = g_j/h_2.$$

Set $h = h_1h_2$. By Hilbert's Irreducibility Theorem, one can find $(a_1^0, \dots, a_r^0) \in (k_0)^r$ such that $h(a_1^0, \dots, a_r^0) \cdot \delta_f(a_1^0, \dots, a_r^0) \neq 0$, where $\delta_f \in A[t_1, \dots, t_r]$ is the discriminant of f, and the polynomial

$$f_0(x) = x^n + z_{n-1}(a_1^0, \dots, a_r^0)x^{n-1} + \cdots + z_0(a_1^0, \dots, a_r^0) \in k_0[x]$$

is irreducible. We can find a finite set of places S of k_0, that includes the place at infinity, such that for any place $v \notin S$ and the corresponding valuation ring $\mathcal{O}_{k_0,v}$, we have the inclusions

$$a_1^0, \dots, a_r^0 \in \mathcal{O}_{k_0,v} \quad \text{and} \quad h(a_1^0, \dots, a_r^0),\ \delta_f(a_1^0, \dots, a_r^0) \in \mathcal{O}_{k_0,v}^\times.$$

We then consider the extension $E_0 = k_0(\alpha_0)$, where α_0 is a root of f_0. As in the proof of Proposition 2.1, we see that E_0/k_0 is a Galois extension such that the specialization $t_i \mapsto a_i^0$ for $i = 1, \dots, r$ yields a natural isomorphism between $\mathcal{H}$ and the Galois group

$\mathcal{H}_0 = \mathrm{Gal}(E_0/k_0)$. We let $\widetilde{\sigma}_0 \in \mathrm{Gal}(E_0/k_0)$ denote the automorphism corresponding to $\widetilde{\sigma}$ under this isomorphism. Applying Chebotarev's Density Theorem, we find a place $v_0 \notin S$ of k_0 which is unramified in E_0 and such that for a suitable extension w_0, the Frobenius automorphism $\mathrm{Fr}(w_0|v_0)$ is $\widetilde{\sigma}_0$. The valuation w_0 corresponds to an embedding $\varepsilon\colon E_0 \hookrightarrow ((k_0)_{v_0})^{\mathrm{sep}}$ into the separable closure of the completion $(k_0)_{v_0}$, and we set $\mathcal{E} = (k_0)_{v_0}(\varepsilon(\alpha_0))$ observing that it is naturally identified with the completion $(E_0)_{w_0}$.

Let $\mathcal{O}_0$ be the valuation ring in $(k_0)_{v_0}$, and let $\mathfrak{p}_0$ be its maximal ideal. Since the latter is uncountable, we can find $a_i^1 \in a_i^0 + \mathfrak{p}_0$ for $i = 1, \dots, r$ so that the elements $t_0, a_1^1, \dots, a_r^1 \in (k_0)_{v_0}$ are algebraically independent over $\mathbb{F}_p$. Then there is an embedding $\iota_0\colon k \hookrightarrow (k_0)_{v_0}$ that sends t_0 to t_0 and t_i to a_i^1 for $i = 1, \dots, r$. Consider the polynomial

$$f_1(x) := x^n + z_{n-1}(a_1^1, \dots, a_r^1)x^{n-1} + \dots + z_0(a_1^1, \dots, a_r^1) \in \mathcal{O}_0[x].$$

Applying Hensel's Lemma as in the proof of Proposition 2.1, we see that there is a root α_1 of f_1 in the valuation ring $\mathcal{O}(\mathcal{E})$ of $\mathcal{E}$ which is congruent to $\varepsilon(\alpha_0)$ modulo the corresponding valuation ideal. Then ι_0 extends to a dense embedding $\widetilde{\iota}\colon E \hookrightarrow \mathcal{E}$ that sends α to α_1. Let ι be the restriction of $\widetilde{\iota}$ to K, and let v be the pullback of w_0 to K. Then the completion K_v can be identified with the compositum $\iota(K)(k_0)_{v_0}$ inside $\mathcal{E}$, hence it is locally compact. It follows from our construction that $\iota(A[t_1, \dots, t_r]) \subset \mathcal{O}_v$ (= the valuation ring of K_v) and $h_1(a_1^1, \dots, a_r^1) \in \mathcal{O}_v^\times$. Since the ring extension $R_{h_1}/A[t_1, \dots, t_r]_{h_1}$ is integral, we conclude that $\iota(R) \subset \mathcal{O}_v$. Finally, repeating verbatim the argument given in the proof of Proposition 2.1, we see that if w is the pullback to L of the valuation on $\mathcal{E}$ with respect to the restriction $\widetilde{\iota}|L$, then L_w/K_v is unramified and the Frobenius automorphism $\mathrm{Fr}(w|v)$ is σ. Now, the fact that L/K is a Galois extension implies that *any* extension $w|v$ is unramified with $\mathrm{Fr}(w|v)$ belonging to the conjugacy class $\mathcal{C}$, as required.

Remark 4.2. The proof of Proposition 4.1 actually gives an infinite number of inequivalent valuations v having the properties indicated in the statement.

5. Positive characteristic: Existence of generic elements

The goal of this section is to prove Theorem 2 (of the introduction). The argument relies heavily on the results of Pink [Pin98] which we briefly summarize below. But first we would like to reduce the proof to the case where Γ' is finitely generated. We recall that an abstract semigroup is called *locally finite* if every finitely generated subsemigroup of it is finite.

Lemma 5.1. *Let G be an absolutely almost simple algebraic K-group, and let Γ' be a Zariski-dense subsemigroup of $G(K)$. If Γ' is not locally finite, then it contains a finitely generated Zariski-dense subsemigroup Δ'.*

Proof. Pick a finitely generated subsemigroup $\Delta' \subset \Gamma'$ for which the Zariski closure $H = \overline{\Delta'}$ has maximum possible dimension. We note that the Zariski closure of a subsemigroup is actually a subgroup, and since Γ' is not locally finite, H is of positive dimension. Take any $\gamma' \in \Gamma'$, and let H' be the Zariski closure of the subsemigroup generated by Δ' and γ'. By construction, $\dim H = \dim H'$, and therefore the connected components H° and $(H')^\circ$ coincide. It follows that γ' normalizes H°. Since $\gamma' \in \Gamma'$ is arbitrary, H° is normalized by all of Γ', hence by $\overline{\Gamma'} = G$. Now, since $\dim H^\circ > 0$, the fact that G is absolutely almost simple implies that $H^\circ = G$, so Δ' is Zariski-dense. □

Since a semigroup containing an element of infinite order is not locally finite, it follows from the lemma that Γ' as in Theorem 2 always contains a finitely generated subsemigroup Δ' which is Zariski-dense in G. Then it is enough to establish the existence of K-generic semisimple elements of infinite order in Δ'. *Thus, we may (and we will)*

henceforth assume that Γ' *is finitely generated and will denote by* Γ *the subgroup of* $G(K)$ *generated by* Γ'.

Before we proceed with the proof of the theorem, we would like to point out that a theorem due to Schur (cf. [Lam01, Theorem 9.9]) implies that the condition that Γ' is not locally finite is in fact equivalent to the condition that it contains an element of infinite order. (Technically, Schur's theorem treats linear *groups*, so we note that a semigroup consisting of elements of finite order is automatically a group.)

On Pinks' approximation results. In this subsection, we will review the notions involved in the results of Pink [Pin98, Pin00] and then give a precise statement of his main result in [Pin98] in the form needed for our purpose. For $i = 1, \dots, r$, let G_i be a connected absolutely simple adjoint group over a local (i.e. nondiscrete locally compact) field F_i. Let G denote the group scheme over the commutative semisimple ring $F = \prod_{i=1}^{r} F_i$ with fibers G_i so that $G(F) = \prod_{i=1}^{r} G_i(F_i)$. Let $\Gamma \subset G(F)$ be a subgroup with compact closure and with Zariski-dense projections in all factors. Following Pink [Pin98], we say that a triple (E, H, φ) consisting of a closed semisimple subring $E \subset F$ such that F is a module of finite type over E, a group scheme H over E whose fibers over factor fields of E are connected absolutely simple adjoint groups, and an isogeny $\varphi\colon H \times_E F \to G$ such that $\Gamma \subset \varphi(H(E))$, is a *weak quasi-model* of the triple (F, G, Γ). If in addition the derivative of φ does not vanish on any fiber, the triple (E, H, φ) is called a *quasi-model*. The triple (F, G, Γ) is called *minimal* if for any quasi-model (E, H, φ) we necessarily have $E = F$ and φ is an isomorphism. Now, if (E, H, φ) is a quasi-model then the fact that the fibers of H over factor fields of E are adjoint makes the isogeny φ purely inseparable. It follows that the induced map $H(E) \to G(F)$ is injective, which enables us to identify Γ with its pre-image in $H(E)$. Then the triple (E, H, Γ) satisfies the same assumptions as (F, G, Γ). A (weak) quasi-model (E, H, φ) is said to be *minimal* if the triple (E, H, Γ) is minimal in the above sense. Pink [Pin98, Theorem 3.6] proves that every triple (F, G, Γ) has a minimal quasi-model (E, H, φ); the subring E in this model is unique, and H and φ are determined up to unique isomorphism.

Now, let (E, H, φ) be a minimal model of (F, G, Γ), and view Γ as a subgroup of $H(E)$. Let $\widetilde{H}$ be the universal cover of H (it is the direct product of the universal covers of the factors of H). Then the commutator morphism of $\widetilde{H}$ factors through a unique morphism $[\ ,\ ]^{\sim}\colon H \times H \to \widetilde{H}$. Let $\widetilde{\Gamma}$ be the subgroup of $\widetilde{H}(E)$ generated by $[\Gamma, \Gamma]^{\sim}$.

Theorem 3 ([Pin98, Main Theorem 0.2])**.** *The closure of* $\widetilde{\Gamma}$ *in* $\widetilde{H}(E)$ *is open.*

We can now state the key proposition that leads to the existence of generic elements. In the rest of this paper G will denote a connected absolutely simple adjoint group defined over a finitely generated field K and $\Gamma \subset G(K)$ a Zariski-dense subgroup that contains an element of infinite order. For a discrete valuation v of K such that the completion K_v is locally compact and Γ has compact closure in $G(K_v)$, we let (E_v, H_v, φ_v) denote a minimal quasi-model of (K_v, G, Γ). Let r be the number of conjugacy classes in the Weyl group of (a maximal torus of) G.

Proposition 5.2. *Assume that there exist a subfield* $K' \subset K$ *such that* K/K' *is a purely inseparable extension and valuations* $v_1, \dots, v_r$ *of* K *satisfying the following properties.*

(0) *Each completion* K_{v_i} *is locally compact and* Γ *has compact closure in* $G(K_{v_i})$.

(1) *For each* $i \in \{1, \dots, r\}$, *the group* H_{v_i} *is* E_{v_i}*-split and* E_{v_i} *contains* K'.

(2) *Set* $V = \{v_1, \dots, v_r\}$, $K_V = \prod_{v \in V} K_v$, $E_V = \prod_{v \in V} E_v\ (\subset K_V)$, $H_V = \prod_{v \in V} H_v$, *and* $\varphi_V = \prod_{v \in V} \varphi_v$; *then* (E_V, H_V, φ_V) *is a minimal quasi-model of* (K_V, G, Γ) (*here* Γ *is diagonally embedded into* $G(K_V) = \prod_{v \in V} G(K_v)$).

Then $\Gamma'\ (\subset \Gamma)$ *contains regular semisimple elements of infinite order that are generic over* K.

Proof. For $v \in V$, we let $\varpi_v\colon \widetilde{H}_v \to H_v$ denote the universal E_v-cover, and set $\pi_v = \varphi_v \circ (\varpi_v)_{K_v}$. Since H_v is E_v-split, $\widetilde{H}_v$ is also E_v-split. As above, we can unambiguously identify Γ with a subgroup of

$$H_V(E_V) = \prod_{v\in V} H_v(E_v).$$

Furthermore, for each $v \in V$, let $[\ ,\ ]_v^{\sim}\colon H_v \times H_v \to \widetilde{H}_v$ be the E_v-morphism obtained from the commutator map, and let

$$[\ ,\ ]^{\sim} = \prod_{v\in V} [\ ,\ ]_v^{\sim}$$

be the product of these morphisms regarded either as a morphism of E_V-schemes

$$H_V \times H_V \to \widetilde{H}_V := \prod_{v\in V} \widetilde{H}_v,$$

or simply as a map

$$H_V(E_V) \times H_V(E_V) \to \widetilde{H}_V(E_V) = \prod_{v\in V} \widetilde{H}_v(E_v).$$

Let $\widetilde{\Gamma}$ be the subgroup of $\widetilde{H}_V(E_V)$ generated by $[\Gamma,\Gamma]^{\sim}$. Since by our assumption (E_V, H_V, φ_V) is a minimal quasi-model of (K_V, G, Γ), the approximation theorem of Pink stated above tells us that the closure of $\widetilde{\Gamma}$ in $\widetilde{H}_V(E_V)$ is open.

Now, for $i \leqslant r$, let $\widetilde{T}_i$ be a maximal E_{v_i}-split torus of $\widetilde{H}_{v_i}$, and let $S_i = \pi_{v_i}((\widetilde{T}_i)_{K_{v_i}})$ be the corresponding maximal K_{v_i}-torus of G. We extend the associated comorphism

$$\pi_i^*\colon \mathrm{X}(S_i) \to \mathrm{X}(\widetilde{T}_i)$$

of the character groups to an isomorphism of vector spaces

$$\tau_i\colon V_i := \mathrm{X}(S_i) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{X}(\widetilde{T}_i) \otimes_{\mathbb{Z}} \mathbb{Q} =: \widetilde{V}_i.$$

We consider the automorphism groups of the root systems $\Phi(\widetilde{H}_{v_i}, \widetilde{T}_i)$ and $\Phi(G, S_i)$ as subgroups of $\mathrm{GL}(\widetilde{V}_i)$ and $\mathrm{GL}(V_i)$, respectively. Then by [Che85, Prop. 4], the isomorphism

$$\lambda_i\colon \mathrm{GL}(\widetilde{V}_i) \to \mathrm{GL}(V_i),\ g \mapsto \tau_i^{-1} \circ g \circ \tau_i$$

induces an isomorphism $W(\widetilde{H}_{v_i}, \widetilde{T}_i) \to W(G, S_i)$ of the Weyl groups.

We fix a maximal K-torus S of G and let $[w_1], \dots, [w_r]$ be the distinct nontrivial conjugacy classes in the Weyl group $W(G,S)$. We use $\iota_{S_i,S}$ to identify conjugacy classes in the Weyl group $W(G,S_i)$ with conjugacy classes in $W(G,S)$. For $i \leqslant r$, we pick $\widetilde{w}_i \in W(\widetilde{H}_{v_i}, \widetilde{T}_i)$ so that $[\lambda_i(\widetilde{w}_i)] = [w_i]$. Since $\widetilde{H}_{v_i}$ is E_{v_i}-split for all i, the argument used in [PR03] to prove Lemma 1 (this argument works in all characteristics) shows that for $i \leqslant r$, one can find a maximal E_{v_i}-torus $\widetilde{\mathcal{T}}_i$ of $\widetilde{H}_{v_i}$ such that

$$\theta_{\widetilde{\mathcal{T}}_i}(\mathrm{Gal}(E_{v_i}^{\mathrm{sep}}/E_{v_i})) \cap \iota_{\widetilde{T}_i, \widetilde{\mathcal{T}}_i}([\widetilde{w}_i]) \neq \varnothing. \tag{7}$$

Let $\mathcal{S}_i = \pi_{v_i}((\widetilde{\mathcal{T}}_i)_{K_{v_i}})$. Then $\mathcal{S}_i$ is a maximal K_{v_i}-torus of G. Let

$$\widetilde{\mathcal{U}}_i = \widetilde{\psi}_i\big(\widetilde{H}_{v_i}(E_{v_i}) \times (\widetilde{\mathcal{T}}_i)_{\mathrm{reg}}(E_{v_i})\big),$$

where

$$\widetilde{\psi}_i\colon \widetilde{H}_{v_i} \times \widetilde{\mathcal{T}}_i \to \widetilde{H}_{v_i},\ (\widetilde{h}, \widetilde{t}\,) \mapsto \widetilde{h}\,\widetilde{t}\,\widetilde{h}^{-1},$$

and

$$\mathcal{U}_i = \psi_i\big(G(K_{v_i}) \times (\mathcal{S}_i)_{\mathrm{reg}}(K_{v_i})\big),$$

where

$$\psi_i\colon G \times \mathcal{S}_i \to G,\ (g,s) \mapsto gsg^{-1}.$$

Observe that by the Open Mapping Theorem, $\widetilde{\mathcal{U}}_i$ and $\mathcal{U}_i$ are open in $\widetilde{H}_{v_i}(E_{v_i})$ and $G(K_{v_i})$, respectively, and they clearly intersect every open subgroup of the respective ambient groups. Let Ω be a compact-open subgroup of

$$G(K_V) := \prod_{v\in V} G(K_v)$$

that does not contain any element whose v-component, for some $v \in V$, is of finite order but not unipotent. Let $\widetilde{\Omega}$ be a compact-open subgroup of $\widetilde{H}_V(E_V)$ that is contained in the inverse image of Ω under the continuous homomorphism $\widetilde{H}_V(K_V) \to G(K_V)$ induced by $\pi_V := \prod_{v\in V} \pi_v$. Since the closure of $\widetilde{\Gamma}$ is an open subgroup of $\widetilde{H}_V(E_V)$, we see that

$$\widetilde{\Gamma} \cap \left(\widetilde{\Omega} \cap \prod_{i=1}^{r} \widetilde{\mathcal{U}}_i\right) \neq \varnothing.$$

Let $\widetilde{\gamma}$ be an element of this intersection, and let $\gamma\,(\in \Omega \cap \prod_{i=1}^{r} \mathcal{U}_i)$ be the corresponding element of Γ. We note that as the subsemigroup Γ' generates Γ, and the closure of the latter in $G(K_V)$ is a compact subgroup, the closure of Γ' in $G(K_V)$ is a subgroup and so it contains Γ. Now since $\Omega \cap \prod_{i=1}^{r} \mathcal{U}_i$ is an open neighborhood of $\gamma\,(\in \Gamma)$ in $G(K_V)$,

$$\Gamma' \cap \left(\Omega \cap \prod_{i=1}^{r} \mathcal{U}_i\right) \neq \varnothing.$$

Let $\gamma' = (\gamma'_1, \ldots, \gamma'_r)$, with $\gamma'_i \in \mathcal{U}_i$, be an element of this intersection. This element is clearly of infinite order; we will now show that it is generic. Let $\mathcal{S} = Z_G(\gamma')^\circ$; this is a maximal K-torus of G. Let $\mathcal{S}_i = Z_G(\gamma'_i)^\circ$. Then $\mathcal{S}_i$ is conjugate to $\mathcal{S}_i$ by an element of $G(K_{v_i})$, and moreover, $\mathcal{S}_{K_{v_i}} = \mathcal{S}_i$.

Since $K' \subset E_{v_i}$, K/K' is purely inseparable, $\mathcal{S}_{K_{v_i}} = \mathcal{S}_i$ is conjugate to $\mathcal{S}_i$ by an element of $G(K_{v_i})$ and $\pi_{v_i}((\widetilde{\mathcal{T}}_i)_{K_{v_i}}) = \mathcal{S}_i$, it follows from (7) by applying π_{v_i} that

$$\theta_{\mathcal{S}_{K_{v_i}}}(\mathrm{Gal}(K_{v_i}^{\mathrm{sep}}/K_{v_i})) \cap \iota_{S_i,\,\mathcal{S}_{K_{v_i}}}([w_i]) \neq \varnothing. \tag{8}$$

Thus, the image $\theta_{\mathcal{S}}(\mathrm{Gal}(K^{\mathrm{sep}}/K))\,(\subset \mathrm{Aut}\,\Phi(G,\mathcal{S}))$ intersects every conjugacy class of $W(G,\mathcal{S})$, and therefore it contains $W(G,\mathcal{S})$. So, γ' is generic, as required. □

In applying the preceding proposition, condition (0) is easy to achieve while conditions (1) and (2) require more work. The subtlety of condition (1) is that while it is easy to construct valuations v such that G is split over K_v, this may not imply automatically that H_v is E_v-split. More precisely, given a K-isogeny $\pi\colon H \to G$ of connected absolutely almost simple algebraic groups over a field K of positive characteristic, H need not be K-split when G is unless π is a central isogeny.[1] We note that over nondiscrete locally compact fields all groups of type F_4 and G_2 are split, so in our situation this problem can arise only for isogenies between groups of types B_n and C_n over fields of characteristic two. However, treating just this case does not appear to be simpler then treating the general case, which is what we are going to do. We begin with two simple lemmas.

Lemma 5.3 (cf. Vinberg [Vin71, Lemmas 2 and 3]). *Let $\Delta \subset M_n(K)$ be an absolutely irreducible multiplicative semigroup, and let E be a subfield of K such that $\mathrm{tr}\,\delta \in E$ for all $\delta \in \Delta$. Then the characteristic polynomial of every $\delta \in \Delta$ has coefficients in E.*

[1] To construct an example, let q be a "nondegenerate" quadratic form of defect 1 on a $(2n+1)$-dimensional vector space V over a field k of characteristic 2. Then the induced bilinear form on $V/\mathrm{Rad}(q)$ is a nondegenerate alternating form in $2n$ variables which is invariant under $\mathrm{SO}(q)$. Thus we get the isogeny $\mathrm{SO}(q) \to \mathrm{Sp}(2n)$. Now, over a locally compact field k, the form q can be chosen to be of Witt index $n-1$, so $\mathrm{SO}(q)$ is not k-split, but $\mathrm{Sp}(2n)$ is k-split.

Note that if the absolute root system of G is simply-laced then π is a central isogeny.

(In characteristic zero this, of course, immediately follows from Newton's formulas.)

Proof. Let A be the E-span of Δ; clearly, A is an E-algebra. We will first show that A is an E-form of $M_n(K)$, i.e. $A \otimes_E K \simeq M_n(K)$. Indeed, since Δ is absolutely irreducible, by Burnside's Theorem, we can pick $\delta_1, \dots, \delta_{n^2} \in \Delta$ that are linearly independent over K. Set

$$B = \sum_{i=1}^{n^2} E\delta_i.$$

Clearly, the map

$$\tau\colon M_n(K) \to K^{n^2},\ a \mapsto (\mathrm{tr}(a\delta_1), \dots, \mathrm{tr}(a\delta_{n^2})),$$

is an isomorphism of K-vector spaces. Since E contains the traces of all elements of Δ, we obtain that $\tau(\Delta) \subset E^{n^2}$ and the matrix of the trace form in the basis $\delta_1, \dots, \delta_{n^2}$ has entries in E. It follows that $\Delta \subset B$, and therefore $A = B$; in particular, $\dim_E A = n^2$. Then the natural homomorphism $A \otimes_E K \to M_n(K)$ is clearly an isomorphism, implying that A is a central simple E-algebra. So, the characteristic polynomial of $\delta \in \Delta \subset A$ can be viewed as its reduced polynomial, and therefore has coefficients in E. □

To formulate the next lemma, we need to introduce one additional technical notion. Let $\gamma \in G(K)$ be a regular semisimple element, and $T = Z_G(\gamma)^\circ$ be the corresponding maximal torus. We say that γ is *super-regular* if the values $a(\gamma)$, for $a \in \Phi(G,T)$, are all distinct. We note that the set of super-regular elements is Zariski-open.

Lemma 5.4. *Let H be an absolutely almost simple algebraic group over a field $E\,(\subset K)$, and let $\varphi\colon H_K \to G\,(\subset \mathrm{GL}_n)$ be an isogeny. Let $\gamma \in H(E)$ be a semisimple element such that $\varphi(\gamma)$ is super-regular and has eigenvalues in E. Then γ is regular and the corresponding torus $T = Z_H(\gamma)^\circ$ is E-split; in particular, H splits over E.*

Proof. Let T be a maximal E-torus of H containing γ, and let $S = \varphi(T_K)$. We let $\Phi = \Phi(G,S)$ and $\Phi' = \Phi(H,T)$ denote the corresponding root systems. Set $p = 1$ if $\mathrm{char}\, E = 0$, and $p = \mathrm{char}\, E$ otherwise. Chevalley [Che85, p. 5] proves that there exists a bijection $\psi\colon \Phi \to \Phi'$ such that

$$\varphi^*(a) = p^{d(a)}\psi(a) \quad \text{for all } a \in \Phi, \tag{9}$$

where $d(a)$ is an integer $\geqslant 0$. Since

$$\varphi^*(a)(\gamma) = a(\varphi(\gamma)) \quad \text{for any } a \in \Phi,$$

and $\varphi(\gamma)$ is regular, it follows from (9) that, first, for all $b \in \Phi'$, $b(\gamma) \neq 1$, and hence γ is regular. Moreover, since $d(a)$ is the same integer for all roots a of a given length (which follows from the fact that the Weyl group acts transitively on the roots of the same length), we see that the values $b(\gamma)$, for $b \in \Phi'_{\mathrm{short}}$, are all distinct (we set $\Phi'_{\mathrm{short}} = \Phi'$ if all roots have the same length). Second, $b(\gamma) \in E^{1/p^\infty}$. At the same time, $b(\gamma)$ lies in a separable closure E^{sep} of E, so in fact $b(\gamma) \in E$ for all $b \in \Phi'$. Then for any $\sigma \in \mathcal{G} := \mathrm{Gal}(E^{\mathrm{sep}}/E)$ we have

$$(\sigma(b))(\gamma) = \sigma(b(\sigma^{-1}(\gamma))) = b(\gamma).$$

It follows that $\sigma(b) = b$ for all $b \in \Phi'_{\mathrm{short}}$ and all $\sigma \in \mathcal{G}$. Since Φ'_{short} span $\mathrm{X}(T)$, we obtain that $\mathcal{G}$ acts on $\mathrm{X}(T)$ trivially, i.e., T is E-split. □

We will use the above two lemmas in the proof of Theorem 2 to verify condition (1) in Proposition 5.2. We will now address condition (2) in this proposition.

Proposition 5.5. *Let $V = \{v_1, \dots, v_r\}$ be a finite set of discrete valuations of K with locally compact completions, and for each $v \in V$ let (E_v, H_v, φ_v) be a minimal quasi-model of (K_v, G, Γ). As above, let $K_V = \prod_{v\in V} K_v$, $E_V = \prod_{v\in V} E_v$, $H_V = \prod_{v\in V} H_v$, and $\varphi_V = \prod_{v\in V} \varphi_v$. If the fields E_v are pairwise nonisomorphic as topological fields then (E_V, H_V, φ_V) is a minimal quasi-model of (K_V, G, Γ).*

Proof. Let (E, H, φ) be a quasi-model of (E_V, H_V, Γ), where Γ is identified with its lift via φ_V. We need to show that $E = E_V$ and φ is an isomorphism. Write $E = \prod_{i=1}^d E_{v_i}$ and $H = \prod_{i=1}^d H_i$, where E_i is a local field and H_i is a connected absolutely simple adjoint E_i-group. It is enough to show that $d = r$. Indeed, then, by analyzing idempotents, we see that after a possible reindexing of the E_i's we may assume that $E_i \subset E_{v_i}$. In this case, for each $i \in \{1, \dots, r\}$, the triple (E_i, H_i, φ_i), where φ_i is the restriction of φ, is a quasi-model of $(E_{v_i}, H_{v_i}, \Gamma)$. So, the minimality of the latter implies that $E_i = E_{v_i}$ and φ_i is an isomorphism, hence the required result.

Now, if $d < r$, then some E_{i_0} has nontrivial projections to E_{v_i} and E_{v_j} for some $i, j \in \{1, \dots, r\}$, $i \neq j$. So, $(E_{i_0}, H_{i_0}, \Gamma)$ is a model of both $(E_{v_i}, H_{v_i}, \Gamma)$ and $(E_{v_j}, H_{v_j}, \Gamma)$. Since these models are minimal, we have $E_{v_i} = E_{i_0} = E_{v_j}$, contradicting our assumption. □

The final preparatory step for the proof of Theorem 2 provides a construction of valuations with the required properties.

Lemma 5.6. *Let K be a finitely generated field, F an infinite subfield of K, and $R \subset K$ be a finitely generated subring. Then there exists a subfield $K' \subset K$ containing F such that the extension K/K' is purely inseparable and for any $r \geqslant 1$ one can find r discrete valuations $v_1, \dots, v_r$ of K such that:*

(1) *for each $i = 1, \dots, r$, the completion K_{v_i} is locally compact, the ring R is contained in the valuation ring $\mathcal{O}(K_{v_i})$, and the completions of F and K' with respect to the restrictions of v_i (i.e. the closures of F and K' in K_{v_i}) coincide;*

(2) *for $i \neq j$, the residue fields of K_{v_i} and K_{v_j} have different sizes.*

Proof. We only need to consider the case where K has characteristic $p > 0$. Pick a separable transcendence basis $s_0, \dots, s_a$ of F over the prime subfield $\mathbb{F}_p$ ($a \geqslant 0$ since F is infinite), and let $t_1, \dots, t_b$ be any transcendence basis of K/F. We then let K' denote the separable closure of $F(t_1, \dots, t_b)$ in K. Then K' is a finite separable extension of $L = \mathbb{F}_p(s_0, \dots, s_a, t_1, \dots, t_b)$, and K/K' is a finite purely inseparable extension. Since R is finitely generated, we can find a nonzero $h \in C := \mathbb{F}_p[s_0, \dots, s_a, t_1, \dots, t_b]$ such that all elements of R are integral over $C_h := C[1/h]$.

Let $\alpha \in K'$ be a primitive element over L. We may assume without loss of generality that the minimal polynomial of α is of the form

$$f(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \quad \text{with } p_i \in C.$$

Set $A = \mathbb{F}_p[s_0]$ and $k = \mathbb{F}_p(s_0)$, and then think of the p_i's as elements of $C = A[s_1, \dots, s_a, t_1, \dots, t_b]$. Let $q = q(s_1, \dots, s_a, t_1, \dots, t_b) \in C$ be the discriminant of f; note that $q \neq 0$ as f is separable. We then pick $s_1^0, \dots, s_a^0, t_1^0, \dots, t_b^0 \in A$ so that $q(s_1^0, \dots, s_a^0, t_1^0, \dots, t_b^0) \neq 0$ and $h(s_0, s_1^0, \dots, s_a^0, t_1^0, \dots, t_b^0) \neq 0$, and let

$$f_0(x) = x^n + p_{n-1}(s_1^0, \dots, s_a^0, t_1^0, \dots, t_b^0)x^{n-1} + \cdots + p_0(s_1^0, \dots, s_a^0, t_1^0, \dots, t_b^0) \in A[x].$$

By our construction, $f_0(x)$ is a separable polynomial. It follows from Chebotarev's Density Theorem that one can find discrete valuations $v_1^0, \dots v_r^0$ of k corresponding to the irreducible polynomials in A of pairwise distinct degrees such that for each $j \in \{1, \dots, r\}$ the residue polynomial $\overline{f_0(x)}^{(v_j^0)}$ over the residue field $\kappa_{v_j^0}$ is separable and splits into linear factors, and the residue

$$\overline{h(s_0, s_1^0, \dots, s_a^0, t_1^0, \dots, t_b^0)}^{(v_j^0)} \neq 0 \quad \text{in } \kappa_{v_j^0}.$$

Let us show that for each $j = 1, \dots, r$, there exists an embedding

$$\iota_j \colon K \hookrightarrow \bar{k}_{v_j^0} =: \mathcal{K}_j \quad \text{(algebraic closure of } k_{v_j^0})$$

extending the standard embedding of k such that $\iota_j(K') \subset k_{v_j^0}$ and $\iota_j(R)$ is contained in the valuation ring $\mathcal{O}(\mathcal{K}_j)$. We let $\mathfrak{p}_j$ denote the valuation ideal in $k_{v_j^0}$. Then one can find elements $\widetilde{s}_1, \dots, \widetilde{s}_a, \widetilde{t}_1, \dots, \widetilde{t}_b \in k_{v_j^0}$ that are *algebraically independent over* k and congruent, respectively, to $s_1^0, \dots, s_a^0, t_1^0, \dots, t_b^0$ modulo $\mathfrak{p}_j$. This enables us to construct an embedding of $L = k(s_1, \dots, s_a, t_1, \dots, t_b)$ into $k_{v_j^0}$ sending $s_1, \dots, s_a, t_1, \dots, t_b$ to $\widetilde{s}_1, \dots, \widetilde{s}_a, \widetilde{t}_1, \dots, \widetilde{t}_b$. Next, we observe that the polynomial

$$\widetilde{f}(x) := x^n + p_{n-1}(\widetilde{s}_1, \dots, \widetilde{s}_a, \widetilde{t}_1, \dots, \widetilde{t}_b)x^{n-1} + \dots + p_0(\widetilde{s}_1, \dots, \widetilde{s}_a, \widetilde{t}_1, \dots, \widetilde{t}_b)$$

has a root in $k_{v_j^0}$. Indeed, the residue $\overline{\widetilde{f}(x)}^{(v_j^0)}$ coincides with $\overline{f^0(x)}^{(v_j^0)}$, hence is a product of distinct linear factors over $\kappa_{v_j^0}$. So, the fact that $\widetilde{f}(x)$ has a root in $k_{v_j^0}$ follows from Hensel's Lemma, and in turn implies that the above embedding $L \hookrightarrow k_{v_j^0}$ extends to an embedding $K' \hookrightarrow k_{v_j^0}$. Now, for the required embedding ι_j we take the unique extension of the latter to K. We only need to show that $\iota_j(R) \subset \mathcal{O}(\mathcal{K}_j)$. According to our construction, we have the inclusion $\iota_j(C) \subset \mathcal{O}(k_{v_j^0}) \subset \mathcal{O}(\mathcal{K}_j)$. Furthermore, $\iota_j(h) = h(s_0, \widetilde{s}_1, \dots, \widetilde{s}_a, \widetilde{t}_1, \dots, \widetilde{t}_b)$ is a unit in $\mathcal{O}(k_{v_j^0})$, so $\iota_j(C_h) \subset \mathcal{O}(\mathcal{K}_j)$. Since every element of R is integral over C_h, the inclusion $\iota_j(R) \subset \mathcal{O}(\mathcal{K}_j)$ follows.

Now, let v_j is the pullback to K (via ι_j) of the standard valuation on $\mathcal{K}_j$. Since $\iota_j(K') \subset k_{v_j^0}$ and K/K' is finite, the completion K_{v_j} is locally compact. All other properties in (1) immediately follow from our construction. Furthermore, by our construction, for $i \neq j$, the local fields $k_{v_i^0}$ and $k_{v_j^0}$ have the residue fields of different sizes. Since K_{v_i} and K_{v_j} are purely inseparable extensions of these fields while the residue fields are perfect, (2) follows. □

Proof of Theorem 2. Let $\pi \colon G \to \bar{G}$ be a central K-isogeny onto the corresponding adjoint group. It is easy to see that if $\gamma' \in \Gamma'$ is such that $\pi(\gamma')$ is a regular semisimple element of infinite order that is generic over K, then γ' possesses all these properties as well. Thus, we may assume from the beginning that G is adjoint. Next, as we have seen at the beginning of this section, we may assume that Γ' is finitely generated. Fixing a faithful K-representation $G \hookrightarrow \mathrm{GL}_n$, we can find a finitely generated subring R of K so that $\Gamma' \subset \mathrm{GL}_n(R)$. Let $\mathfrak{g} = L(G)$ be the Lie algebra of G. Any nontrivial K-isogeny $\varphi \colon H \to G$, with H connected and adjoint, is purely inseparable and the image of the differential $d\varphi$ is either zero or contains the unique irreducible $\mathrm{Ad}\, G$-submodule $\mathfrak{m}$ of $\mathfrak{g}$. Let $\rho \colon G \to \mathrm{GL}(\mathfrak{m})$ denote the corresponding representation. Let F be the subfield of K generated by the traces $\mathrm{tr}\, \rho(\gamma)$, $\gamma \in \Gamma$; clearly, F is infinite. Pick a super-regular $\gamma_0 \in \Gamma$; then $\rho(\gamma_0)$ is super-regular in $\rho(G)$. Let $\chi(t)$ be the characteristic polynomial of $\rho(\gamma_0)$ which by Lemma 5.3 has coefficients in F. Write $\chi(t) = (t-1)^a f(t)$, where $f(t) \in F[t]$ is such that $f(1) \neq 0$. Since γ_0 is super-regular in G, the polynomial $f(t)$ does not have multiple roots. Expanding K, we may assume that f splits over K into linear factors. Then, since f is separable, for any subfield $K' \subset K$ containing F and such that K/K' is purely inseparable, the polynomial f splits into linear factors already over K'.

Now, using Lemma 5.6, we find a subfield $K' \subset K$ containing F such that K/K' is purely inseparable and discrete valuations $v_1, \dots, v_r$ (where r is the number of nontrivial conjugacy classes in the Weyl group of G) of K satisfying conditions (1) and (2) therein. Set $V = \{v_1, \dots, v_r\}$. Then for any $v \in V$, the completion K_v is locally compact by construction and the closure of Γ in $G(K_v)$ is compact due to the inclusions $\Gamma \subset \mathrm{GL}_n(R)$ and $R \subset \mathcal{O}(K_v)$, verifying condition (0) of Proposition 5.2. Let (H_v, E_v, φ_v) be a minimal

quasi-model of (G, K_v, Γ). Since the representation $\rho \circ \varphi_v$ is contained in the adjoint representation of H_v, we obtain from Proposition 3.10 of [Pin98] that E_v ($\subset K_v$) contains F. Since F and K' have the same closure in K_v and f splits over K' into linear factors, we conclude that all eigenvalues of $\rho(\gamma_0)$ lie in E_v. On the other hand, by the definition of a quasi-model, there exists $\gamma \in H_v(E_v)$ such that $\varphi_v(\gamma) = \gamma_0$. Applying Lemma 5.4 to the isogeny $\rho \circ \varphi_v \colon H_v \to \rho(G)$, we obtain that H_v is E_v-split, which verifies condition (1) of Proposition 5.2. Finally, as we have seen, E_v contains K', and therefore the extension K_v/E_v is purely inseparable. So, since the fields K_{v_j} for $j = 1, \dots, r$ have finite residue fields of pairwise different sizes, the same is true for the fields E_{v_j}, making these fields pairwise nonisomorphic. Applying Proposition 5.5, we see that (E_V, H_V, φ_V) is a minimal model of (K_V, G, Γ), verifying condition (2) of Proposition 5.2. Now, the assertion of Theorem 2 on the existence of generic elements immediately follows from Proposition 5.2. □

Acknowledgments

Both authors were supported by NSF through grants DMS-1401380 and DMS-1301800. The second-named author was also supported by the Humboldt and the Simons Foundations. Part of the paper was written in the summer of 2016 when he visited the University of Bielefeld whose hospitality is thankfully acknowledged.

References

[CF10] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, 2nd ed., London Mathematical Society, London, 2010. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965; Including a list of errata. MR3618860

[Che85] Catherine Chevalley, *Claude Chevalley* (Spanish), Mathesis **1** (1985), no. 4, 649–656. Mathesis. MR1106703

[Jan96] Gerald J. Janusz, *Algebraic number fields*, 2nd ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR1362545

[Lam01] T. Y. Lam, *A first course in noncommutative rings*, 2nd ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001. MR1838439

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556

[Pin98] Richard Pink, *Compact subgroups of linear algebraic groups*, J. Algebra **206** (1998), no. 2, 438–504. MR1637068

[Pin00] Richard Pink, *Strong approximation for Zariski dense subgroups over arbitrary global fields*, Comment. Math. Helv. **75** (2000), no. 4, 608–643. MR1789179

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen. MR1278263

[PR03] Gopal Prasad and Andrei S. Rapinchuk, *Existence of irreducible $\mathbb{R}$-regular elements in Zariski-dense subgroups*, Math. Res. Lett. **10** (2003), no. 1, 21–32. MR1960120

[PR09] Gopal Prasad and Andrei S. Rapinchuk, *Weakly commensurable arithmetic groups and isospectral locally symmetric spaces*, Publ. Math. Inst. Hautes Études Sci. **109** (2009), 113–184. MR2511587

[PR14] Gopal Prasad and Andrei S. Rapinchuk, *Generic elements in Zariski-dense subgroups and isospectral locally symmetric spaces*, Thin groups and superstrong approximation, Math. Sci. Res. Inst. Publ., vol. 61, Cambridge Univ. Press, Cambridge, 2014, pp. 211–252. MR3220892

[Ser92a] Jean-Pierre Serre, *Lie algebras and Lie groups*, 2nd ed., Lecture Notes in Mathematics, vol. 1500, Springer-Verlag, Berlin, 1992. MR1176100

[Ser92b] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992. With a foreword by Henri Darmon and the author. MR1162313

[Ser12] Jean-Pierre Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11, CRC Press, Boca Raton, FL, 2012. MR2920749

[Sch14] J. Schwartz, *Weak commensurability of Zariski-dense subgroups of algebraic groups defined over fields of positive characteristic*, PhD dissertation, University of Virginia, 2014.

[Vin71] È. B. Vinberg, *Rings of definition of dense subgroups of semisimple linear groups.* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971), 45–55. MR0279206

[Wei84] Boris Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Ann. of Math. (2) **120** (1984), no. 2, 271–315. MR763908

Department of Mathematics, University of Michigan, Michigan
Email address: gprasad@umich.edu

Department of Mathematics, University of Virginia, Virginia
Email address: asr3x@virginia.edu

Originally published in English