EXISTENCE OF IRREDUCIBLE $\mathbb{R}$-REGULAR ELEMENTS IN ZARISKI-DENSE SUBGROUPS

Gopal Prasad and Andrei S. Rapinchuk

Let $G$ be a connected semisimple algebraic group defined over the field $\mathbb{R}$ of real numbers. An element $x$ of $G(\mathbb{R})$ is called $\mathbb{R}$-regular if the number of eigenvalues, counted with multiplicity, of modulus 1 of $\text{Ad} x$ is minimum possible. (If $G$ is $\mathbb{R}$-anisotropic, i.e., the group $G(\mathbb{R})$ is compact, every element of $G(\mathbb{R})$ is $\mathbb{R}$-regular.) The existence of $\mathbb{R}$-regular elements in an arbitrary subsemigroup $\Gamma$ of $G(\mathbb{R})$ which is Zariski-dense in $G$ was proved by Y. Benoist and F. Labourie [3] using Oseledet’s multiplicative ergodic theorem, and then reproved by the first-named author [15] by a direct argument. Recently G.A. Margulis and G.A. Soifer asked us a question, which arose in their joint work with H. Abels on the Auslander problem, about the existence of $\mathbb{R}$-regular elements with some special properties. The purpose of this note is to answer their question in the affirmative. Before formulating the result, we recall (cf. [16], Remark 1.6(1)) that an $\mathbb{R}$-regular element $x$ is necessarily semisimple, so if in addition it is regular, then $T := Z_G(x)^o$ is a maximal torus; moreover, $x$ belongs to $T$ (see [4], Corollary 11.12).

**Theorem 1.** Let $G$ be a connected semisimple real algebraic group. Then any Zariski-dense subsemigroup $\Gamma$ of $G(\mathbb{R})$ contains a $\mathbb{R}$-regular element $x$ such that the cyclic subgroup generated by it is a Zariski-dense subgroup of the maximal torus $T := Z_G(x)^o$.

**Remark 1.** Let $\Gamma$, $x$, and $T = Z_G(x)^o$ be as in Theorem 1. Let $T_s$ (resp., $T_a$) be the maximal $\mathbb{R}$-split (resp., $\mathbb{R}$-anisotropic) subtorus of $T$. Then $T = T_s \cdot T_a$ (an almost direct product), $T_s$ is a maximal $\mathbb{R}$-split torus of $G$ since $x$ is $\mathbb{R}$-regular (see [16], Lemma 1.5), and $T_a(\mathbb{R}) \simeq \mathbb{R}/\mathbb{Z}^r$, where $r = \text{dim } T_a$. There is a positive integer $d$ such that $x^d = y \cdot z$ with $y \in T_s(\mathbb{R})$ and $z \in T_a(\mathbb{R})$. Then the cyclic group $C$ generated by $z$ is dense in $T_a$ in the Zariski-topology and since $T_a(\mathbb{R})$ is a compact Lie group, $C$ is actually dense in $T_a(\mathbb{R})$ in the usual compact Hausdorff topology on the latter. Thus, in particular, if $G(\mathbb{R})$ is compact, then any dense subsemigroup contains a Kronecker element, i.e., an element such that the closure of the subsemigroup generated by it is a maximal torus.

Also, since the cyclic subgroup generated by $x$ is dense in $T$ in the Zariski-topology, $Z_G(x) = Z_G(T) = T$. Thus the centralizer of $x$ is connected.

Received March 14, 2002.
Revised version received July 9, 2002.
Remark 2. Let \( \Gamma, x \) and \( T = Z_G(x) \) be as in Theorem 1. Assume, in addition, that \( \Gamma \) is a subgroup. Then the subset \( \{ \gamma x^n \gamma^{-1} \mid \gamma \in \Gamma, n \in \mathbb{Z} - \{0\} \} \), which consists of \( \mathbb{R} \)-regular elements with the properties described in Theorem 1, is Zariski-dense in \( G \). To see this note that the cyclic subgroup generated by \( x \) is dense in \( T \) and, as is well-known, the union of the conjugates of \( T \) under a Zariski-dense subset (of \( G \)) is Zariski-dense in \( G \).

The proof of Theorem 1 uses the result of [15], some facts about \( \mathbb{R} \)-regular elements established in [16] and suitable generalizations of our recent results about irreducible tori [17]. We recall that a torus \( T \) defined over a field \( K \) is called \( K \)-irreducible if it does not contain any proper \( K \)-subtori, and a regular semisimple element \( x \in G(K) \), where \( G \) is a semisimple \( K \)-group, \( K \)-irreducible if the torus \( T = Z_G(x) \) is \( K \)-irreducible. To handle arbitrary semisimple groups, these notions need to be generalized as follows.

Let \( G \) be a connected semisimple algebraic group defined over a field \( K \). Then \( G = G^{(1)} \cdots G^{(s)} \), an almost direct product of connected \( K \)-simple groups \( G^{(i)} \) (cf. [19]). Given a maximal torus \( T \) of \( G \), we let \( T^{(i)} \) denote the maximal torus \( T \cap G^{(i)} \) of \( G^{(i)} \), for any \( i = 1, \ldots, s \). We say that a maximal \( K \)-torus \( T \) of \( G \) is \( K \)-quasi-irreducible if it does not contain any \( K \)-subtori other than those which are almost direct product of some of the \( T^{(i)} \)'s. Furthermore, a regular semisimple element \( x \in G(K) \) will be called \( K \)-quasi-irreducible if \( T = Z_G(x) \) is \( K \)-quasi-irreducible, and \( x \) will be called \( K \)-quasi-irreducible anisotropic if, in addition, \( T \) is anisotropic over \( K \). We also say that an element \( x \in G \) is without components of finite order if in some (equivalently, any) decomposition \( x = x_1 \cdots x_s \) with \( x_i \in G^{(i)} \), all the \( x_i \)'s have infinite order. (Of course, if \( G \) is absolutely, or even \( K \)-, simple, then the notions of \( K \)-irreducibility and \( K \)-quasi-irreducibility for maximal \( K \)-tori of \( G \) and regular semisimple elements of \( G(K) \) coincide, and elements without components of finite order are simply elements of infinite order.) It is easy to see that a \( K \)-quasi-irreducible element \( x \in G(K) \), which is without components of finite order, generates a Zariski-dense subgroup of the corresponding torus \( T = Z_G(x) \).

We now observe that without loss of generality the subsemigroup \( \Gamma \) in Theorem 1 can be assumed to be finitely generated, hence contained in \( G(K) \), where \( K \) is a suitable finitely generated subfield of \( \mathbb{R} \) over which \( G \) is defined; therefore, we see that Theorem 1 is a consequence of the following.

Theorem 2. Let \( K \) be a finitely generated subfield of \( \mathbb{R} \), and \( G \) be a connected semisimple algebraic \( K \)-group. Then any finitely generated subsemigroup \( \Gamma \) of \( G(K) \) which is Zariski-dense in \( G \) contains a Zariski-dense set of \( \mathbb{R} \)-regular \( K \)-quasi-irreducible anisotropic elements without components of finite order.

One of the ingredients of the proof of Theorem 2 is the following refinement (with a different proof) of Theorem 1 of [17]. We observe that this refinement is valid for an arbitrary semisimple group defined over an infinite field (of any characteristic) while the result in [17] was established only for absolutely almost simple groups over global fields.
Theorem 3. Let $G$ be a connected semisimple algebraic group defined over an infinite field $K$, $r$ be the number of nontrivial conjugacy classes in the absolute Weyl group of $G$. Furthermore, let $S$ be a set of $r$ nontrivial inequivalent nonarchimedean valuations of $K$ such that for every $v \in S$, the completion $K_v$ is locally compact and splits $G$. Then

(i) for each $v \in S$, we can choose a maximal $K_v$-torus $T_v$ of $G$ so that any $K$-torus $T$ which is conjugate to $T_v$ under an element of $G(K_v)$, for all $v \in S$, is $K$-quasi-irreducible and anisotropic over $K$;
(ii) there exists an open subset $U$ of $G_S := \prod_{v \in S} G(K_v)$ with the following properties:

(a) $U$ intersects every open subgroup of $G_S$, and for any element $x = (x_v)$ of $U$, all the $x_v$’s are elements without components of finite order;
(b) $\delta_S^{-1}(\delta_S(G(K)) \cap U)$, where $\delta_S: G(K) \to G_S$ is the diagonal embedding, consists of $K$-quasi-irreducible anisotropic elements.

First, we need to fix some notations and conventions. Given a maximal torus $T$ of $G$, we let $\Phi(G,T)$ denote the root system of $G$ with respect to $T$. As usual, we will identify the absolute Weyl group $W(G,T) = N_G(T)/T$ with a normal subgroup of $\text{Aut} \Phi(G,T)$. For $x \in W(G,T)$, we let $[x]$ denote the conjugacy class of $x$ in $W(G,T)$, and for a subset $X$ of $W(G,T)$, we let $[X]$ denote the collection of conjugacy classes $[x]$ with $x \in X$ (in particular, $[W(G,T)]$ is the set of all conjugacy classes in $W(G,T)$). Next, given two maximal tori $T_1$, $T_2$ and an element $g \in G$ such that $T_2 = gT_1g^{-1}$, we let $\iota_g$ denote the isomorphism from $\text{Aut} \Phi(G,T_1)$ to $\text{Aut} \Phi(G,T_2)$ induced by $\text{Int} g$. We notice that given another $g' \in G$ with the property $T_2 = g'T_1(g')^{-1}$, we have $g'g^{-1} \in N_G(T_2)$ and $\iota_{g'} = \text{Int} w \circ \iota_g$, where $w$ is the class of $g'g^{-1}$ in $W(G,T_2)$; in particular, there is a well-defined bijection $\iota_{T_1,T_2} : [W(G,T_1)] \to [W(G,T_2)]$ satisfying the standard properties: $\iota_{T,T} = \text{id}$, $\iota_{T_1,T_2} \circ \iota_{T_2,T_3} = \iota_{T_1,T_3}$, and $\iota_{T_1,T_2} = \iota_{T_2,T_3} \circ \iota_{T_1,T_3}$. Finally, if a maximal torus $T$ is defined over a field $L \supseteq K$, we will denote by $L_T$ its minimal splitting field over $L$ and by $\mathcal{S}(T,L)$ the corresponding Galois group $\text{Gal}(L_T/L)$. Since $G$ is semisimple, $\Phi(G,T)$ generates the character group $X(T)$, and therefore the action of $\mathcal{S}(T,L)$ on $\Phi(G,T)$ allows one to identify it with a subgroup of $\text{Aut} \Phi(G,G)$.

Proof of Theorem 3(i). Let $\pi : \tilde{G} \to G$ be the simply connected cover of $G$ defined over $K$, where $\pi$ is a central isogeny. By our assumption, for each $v \in S$, the group $G$, and hence also its simply connected cover $\tilde{G}$, splits over $K_v$ and therefore, $\tilde{G}$ possesses a maximal torus $\tilde{C}_v$ which is defined and split over $K_v$. According to a theorem of A. Grothendieck (see [5], Theorem 7.9, and also [8] for the characteristic zero case), the $K$-variety $\mathcal{T}$ of maximal tori of $G$ is a $K$-rational homogeneous space of $\tilde{G}$, hence has the weak approximation property (see [14], Proposition 7.3). Since the orbit $\tilde{G}(K_v) \cdot \tilde{C}_v$ (which coincides with the $\tilde{G}(K_v)$-conjugacy class of $\tilde{C}_v$) is open in $\mathcal{T}(K_v)$ for all $v \in S$, by the weak
approximation property of $\tilde{T}$ there exists a maximal $K$-torus $\tilde{T}_0$ of $\tilde{G}$ which splits over $K_v$ for all $v \in S$. Set $T_0 = \pi(\tilde{T}_0)$.

We fix a bijection between $S$ and the set of nontrivial conjugacy classes in $W(G, T_0)$ and for $v \in S$, we will denote the corresponding conjugacy class by $c_v$. We have the following:

**Lemma 1.** For each $v \in S$, there exists a maximal $K_v$-torus $T_v$ of $G$ such that $c_v \in \iota_{T_v, T_0}([\mathcal{S}(T_v, K_v) \cap W(G, T_v)])$.

**Proof.** The central isogeny $\pi: \tilde{G} \to G$ induces an isomorphism

$$\tilde{\pi}: W(\tilde{G}, \tilde{T}_0) \to W(G, T_0).$$

Let $\tilde{c}_v$ be the conjugacy class in $W(\tilde{G}, \tilde{T}_0)$ such that $\tilde{\pi}(\tilde{c}_v) = c_v$, and $x \in W(\tilde{G}, \tilde{T}_0)$ be a representative of $\tilde{c}_v$. Since $\tilde{T}_0$ splits over $K_v$, $\tilde{G}/K_v$ and the torus $\tilde{T}_0/K_v$ are obtained respectively from a Chevalley group-scheme over $\mathbb{Z}$ and a split-torus $\mathbb{Z}$-subscheme by base change $\mathbb{Z} \to K_v$. From this we see that there exists a finite subgroup $\mathcal{N}$ of $\tilde{N}_0(K_v)$, where $\tilde{N}_0 = N_{\tilde{G}}(\tilde{T}_0)$, that contains representatives of all elements of $W(\tilde{G}, \tilde{T}_0)$. Let $y \in \mathcal{N}$ be a representative of $x$.

The homomorphism $\zeta: \tilde{\mathbb{Z}} \to \tilde{N}_0(K_v)$ defined by $\zeta(1) = y$ can be thought of as a continuous 1-cocycle on the group $\text{Gal}(\tilde{K}_v^\text{ur}/K_v)$ with values in $\tilde{N}_0(K_v^\text{ur})$, where $K_v^\text{ur}$ is the maximal unramified extension of $K_v$ (we recall that being locally compact, $K_v$ is either a finite extension of the field $\mathbb{Q}_p$ of $p$-adic numbers or it is the field of Laurent power series in one variable over a finite field, and therefore there exists an isomorphism $\tilde{\mathbb{Z}} \simeq \text{Gal}(\tilde{K}_v^\text{ur}/K_v)$ sending 1 to the Frobenius automorphism $\varphi$, and hence also as a continuous 1-cocycle on $\mathcal{S}_v := \text{Gal}(K_v^\text{ur}/K_v)$ with values in $\tilde{N}_0(K_v^\text{ur})$, where $K_v^s$ is a separable closure of $K_v$ containing $K_v^\text{ur}$.

Since $H^1(K_v, \tilde{G}) = \{1\}$ (Kneser [10] for characteristic zero and Bruhat-Tits [7] for general local fields with perfect residue field of cohomological dimension $\leq 1$), there exists $g \in \tilde{G}(K_v^s)$ such that $\zeta(\gamma) = g^{-1}\gamma(g)$ for all $\gamma \in \mathcal{S}_v$. We claim that the torus $T_v := \pi(g\tilde{T}_0g^{-1})$ is defined over $K_v$ and has the required property. Obviously, it suffices to show that $\tilde{T}_v := g\tilde{T}_0g^{-1}$ is defined over $K_v$ and

$$\gamma(\tilde{T}_v) = \gamma(g)\tilde{T}_0\gamma(g)^{-1} = g(\gamma^{-1}(g)\tilde{T}_0(\gamma^{-1}(g))^{-1}g^{-1} = g\tilde{T}_0g^{-1} = \tilde{T}_v$$

as $\gamma^{-1}(g) = \zeta(\gamma) \in \tilde{N}_0(K_v^s)$, implying that $\tilde{T}_v$ is in fact defined over $K_v$ ([4], AG 14.4). To prove (1), we will consider the action of an arbitrary $\gamma \in \mathcal{S}_v$ on $\Phi(\tilde{G}, \tilde{T}_v)$, and compute the corresponding action of $\iota_{g^{-1}}(\gamma)$ on $\Phi(\tilde{G}, \tilde{T}_0)$. Let $\alpha_0 \in \Phi(\tilde{G}, \tilde{T}_0)$, and let $\alpha \in \Phi(\tilde{G}, \tilde{T}_v)$ be defined by the formula $\alpha(t) = \alpha_0(\gamma^{-1}tg)$. Since $\tilde{T}_0$ is $K_v$-split, and hence $\alpha_0$ is defined over $K_v$, for any $t \in \tilde{T}_0(K_v^s)$ we obtain the following

$$\iota_{g^{-1}}(\gamma)(\alpha_0)(t) = \gamma(\gamma^{-1}(g)\gamma^{-1}(t)\gamma^{-1}(g)^{-1})$$
\[= \gamma(\alpha_0((g^{-1} \gamma^{-1}(g))\gamma^{-1}(t)(\gamma^{-1}(g)^{-1}g))) = \alpha_0((g^{-1} \gamma(g))^{-1}t(g^{-1} \gamma(g))),\]

i.e. \(\tau_{g^{-1}}(\gamma)\alpha_0 = \tilde{\zeta}(\gamma)\alpha_0\), where \(\tilde{\zeta}(\gamma)\) is the image of \(\zeta(\gamma)\) in \(W(\bar{G}, \bar{T}_0)\). Thus, \(\tau_{g^{-1}}(\mathcal{S}(\bar{T}_v, K_v)) = \text{Im} \tilde{\zeta}\). In particular, \(x = \tilde{\zeta}(\varphi) \in \tau_{g^{-1}}(\mathcal{S}(\bar{T}_v, K_v))\), and (1) follows. The proof of Lemma 1 is complete.

For all \(v \in S\), we fix a maximal \(K_v\)-torus \(T_v\) of \(G\) as in the preceding lemma. To prove Theorem 3, let \(T\) be a maximal \(K\)-torus of \(G\) such that for every \(v\) in \(S\), there exists a \(g_v \in G(K_v)\) so that \(T = g_v^{-1}T_vg_v\); the existence of such a \(T\) follows from the weak approximation property of the \(K\)-variety \(T\) of maximal tori of \(G\). Then \(\tau_{g_v}(\mathcal{S}(T, K_v)) = \mathcal{S}(T_v, K_v)\), so it follows from Lemma 1 that

\[
c_v \in \tau_{T_v,T_0}(\mathcal{S}(T_v, K_v) \cap W(G, T_v)) = \tau_{T_v,T_0}(\tau_{T,T_v}(\mathcal{S}(T, K_v) \cap W(G, T)))
\]

\[
= \tau_{T,T_0}(\mathcal{S}(T, K_v) \cap W(G, T)) \subset \tau_{T,T_0}(\mathcal{S}(T, K) \cap W(G, T)).
\]

Thus, if \(g \in G\) is chosen so that \(T_0 = gTg^{-1}\), then the subgroup \(\tau_g(\mathcal{S}(T, K) \cap W(G, T))\) of (the finite group) \(W(G, T_0)\) meets every conjugacy class of the latter. However, conjugates of a proper subgroup of a finite group cannot fill up the group, so we conclude that

\[\tau_g(\mathcal{S}(T, K) \cap W(G, T)) = W(G, T_0),\]

and therefore \(\mathcal{S}(T, K) \supset W(G, T)\). This obviously implies that \(T\) is anisotropic over \(K\).

Now, to prove that \(T\) is \(K\)-quasi-irreducible, we observe that each of the \(K\)-simple components \(G^{(i)}\) of \(G\) can in turn be decomposed further into an almost direct product of connected absolutely almost simple groups: \(G^{(i)} = G_1^{(i)} \cdots G_t^{(i)}\), where the subgroups \(G_j^{(i)}\), \(j = 1, \ldots, t_i\), are transitively permuted by the absolute Galois group \(\mathcal{S} = \text{Gal}(K^s/K)\), where \(K^s\) is a separable closure of \(K\). Since \(G\) splits over \(K_T\), all of its connected absolutely almost simple normal subgroups are defined over \(K_T\), so this permutation action of \(\mathcal{S}\) factors through \(\mathcal{S}(T, K)\). Let \(T^{(i)} = T \cap G^{(i)}\) and \(\Phi_j^{(i)}(v)\) be the (direct) sum of the \(V_j^{(i)}\) for \(j = 1, \ldots, t_i\). We claim that any \(\mathcal{S}(T, K)\)-invariant subspace \(V\) of \(V\) is the direct sum of some of the \(V_j^{(i)}\)’s. Indeed, since

\[V = \bigoplus_{i=1}^s \bigoplus_{j=1}^{t_i} V_j^{(i)} \quad \text{and} \quad W(G, T) = \prod_{i=1}^s \prod_{j=1}^{t_i} W(G_j^{(i)}, T_j^{(i)}),\]

the facts that 1) \(W(G_j^{(i)}, T_j^{(i)})\) acts on \(V_j^{(i)}\) irreducibly for all \(i\) and \(j\), and 2) \(\mathcal{S}(T, K)\) contains \(W(G, T)\), imply that \(Y\) is the direct sum of some of the \(V_j^{(i)}\)’s. However, for any fixed \(i\), as \(\mathcal{S}(T, K)\) acts transitively on the set of the \(V_j^{(i)}\)’s our claim follows. If now \(T'\) is a \(K\)-subtorus of \(T\), then the subspace \(\tilde{Y} := \text{Ker}(X(T) \xrightarrow{\text{res}} X(T')) \otimes \mathbb{Q}\) is of the form \(\oplus_{i \in I} V^{(i)}\) for some \(I \subset \{1, \ldots, s\}\), and hence \(T'\) is an almost direct product of the \(T_j^{(i)}\)’s for \(i \in \{1, \ldots, s\} - I\), as claimed.
**Proof of Theorem 3(ii).** For each \( v \in S \), we let \( R_v \) denote the set of regular elements in \( T_v(K_v) \) and consider the map

\[
\psi_v : G(K_v) \times R_v \to G(K_v), \quad \psi_v(g, x) = gxg^{-1}.
\]

It follows from the implicit function theorem that \( \psi_v \) is an open map. For \( i = 1, \ldots, s \), we let \( \theta^{(i)} : G^{(i)} \to \overline{G}^{(i)} \) be the natural central isogeny to the adjoint group \( \overline{G}^{(i)} \) of \( G^{(i)} \), and let \( \theta : G \to \overline{G}^{(1)} \times \cdots \times \overline{G}^{(s)} \) denote the resulting central isogeny. Furthermore, for \( v \in S \), we let \( T_v^{(i)} = T_v \cap G^{(i)} \), \( \overline{T}_v^{(i)} = \theta^{(i)}(T_v^{(i)}) \), and pick an open torsion-free subgroup \( \Sigma_v^{(i)} \) of \( \overline{T}_v^{(i)}(K_v) \). Set

\[
\Sigma_v = \theta^{-1}(\Sigma_v^{(1)} \times \cdots \times \Sigma_v^{(s)}),
\]

and consider the open subset \( U_v := \psi_v(G(K_v), R_v \cap \Sigma_v) \) of \( G(K_v) \). Given an open subgroup \( \Omega_v \) of \( G(K_v) \), the \( v \)-adically open subgroup \( \Omega_v \cap \Sigma_v \) of \( T_v(K_v) \) intersects the Zariski-open subset \( R_v \) (cf. [14], Lemma 3.2), and therefore \( U_v \cap \Omega_v \neq \emptyset \). We claim moreover that any \( x_v \in U_v \) is without components of finite order. To prove this claim, after replacing \( x_v \) by a conjugate, we may assume that \( x_v \in R_v \cap \Sigma_v \). If \( x_v = x_v^{(1)} \cdots x_v^{(s)} \) with \( x_v^{(i)} \in G^{(i)} \), then

\[
\theta(x_v) = (\theta^{(1)}(x_v^{(1)}), \ldots, \theta^{(s)}(x_v^{(s)})) \in \Sigma_v^{(1)} \times \cdots \times \Sigma_v^{(s)}.
\]

Now if for some \( i \), \( x_v^{(i)} \) has finite order, then since \( \Sigma_v^{(i)} \) is torsion-free, we obtain that \( \theta^{(i)}(x_v^{(i)}) = 1 \), and therefore, \( x_v^{(i)} \in Z(G^{(i)}) \). But then \( x_v \) is not regular, a contradiction. It follows that \( U := \prod_{v \in S} U_v \) satisfies condition (a).

Finally, if \( \delta_S(x) \in \delta_S(G(K)) \cap U \), then \( x \) is regular semisimple and the torus \( T = Z_G(x)^0 \) is \( G(K_v) \)-conjugate to \( T_v \) for all \( v \in S \). So, by (i), \( T \) is \( K \)-quasi-irreducible and anisotropic. This completes the proof of Theorem 3. \( \Box \)

**Remark 3.** For \( v \in S \), let \( \mathcal{O}_v \) be the ring of integers in \( K_v \). As \( \overline{T}_0 \), and hence \( \overline{G} \), splits over \( K_0 \), \( \overline{G}/K_v \) and \( \overline{T}_0/K_v \) are obtained respectively from a Chevalley group-scheme \( \overline{G}_v \) over \( \mathbb{Z} \) and a split-torus \( \mathbb{Z} \)-subscheme of \( \overline{G}_v \) by base change \( \mathbb{Z} \to \mathcal{O}_v \to K_v \). From this we can see that the subgroup \( \mathcal{N} \) in the proof of Lemma 1 can be chosen inside \( \overline{N}_0(\mathcal{O}_v) := \overline{N}_0(K_v) \cap \overline{G}_v(\mathcal{O}_v) \). Then \( \zeta \) can be thought of as a continuous 1-cocycle on \( \overline{\mathbb{Z}} \simeq \text{Gal}(K_v^{ur}/K_v) \) with values in \( \overline{G}_v(\mathcal{O}_v^{ur}) \), where \( \mathcal{O}_v^{ur} \) is the ring of integers of \( K_v^{ur} \), and instead of using the triviality of \( H^1(K_v, \overline{G}) \), we can use the triviality of \( H^1(K_v^{ur}/K_v, \overline{G}_v(\mathcal{O}_v^{ur})) \), which easily follows from Lang’s theorem on the triviality of Galois cohomology of connected algebraic groups over finite fields, see Theorem 6.8 of [14].

**Remark 4.** If \( K \) is a global field, then given any finite set \( V_0 \) of places of \( K \), using, for example, Tchebotarev’s Density Theorem, one can find a set \( S \) of \( r \) nonarchimedean places outside \( V_0 \) (where \( r \) is the same as in the statement of Theorem 3) such that \( G \) splits over \( K_v \) for all \( v \in S \). For every \( v \in S \), we choose a maximal \( K_v \)-torus \( T_v \) of \( G \) so that the assertion of Lemma 1 holds, and let \( T_0 \) be a maximal \( K \)-torus of \( G \) which is \( G(K_v) \)-conjugate to \( T_v \) for each \( v \in S \).
(the existence of such a $T_0$ follows from the weak approximation property of the $K$-variety $T$ of maximal tori of $G$). Now for any maximal $K$-torus $T$ of $G$ which is $G(K_v)$-conjugate to $T_0$ for all $v \in S$, $G(T, K) \supset W(G, T)$ (see the proof of Theorem 3(i)), hence such a $T$ is $K$-quasi-irreducible and anisotropic over $K$, yielding a generalization, and an alternative proof, of Theorem 1(i) of [17].

Another ingredient of the proof of Theorem 2 is the following proposition which is a variant of Proposition 1 of [18]. For the reader’s convenience we give the full proof although it is similar to the argument given in [18].

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

**Proof.** Pick a transcendence basis $\{s_1, \ldots, s_l\}$ of $K$ over $\mathbb{Q}$, and let $A = \mathbb{Z}[s_1, \ldots, s_l]$, $L = \mathbb{Q}(s_1, \ldots, s_l)$. Furthermore, pick an element $\alpha \in K$ so that $K = L[\alpha]$, let $f(x)$ denote the minimal monic polynomial of $\alpha$ over $L$, and set $B = A[\alpha]$. Since $R$ is finitely generated, there exists a nonzero $a \in A$ with the following properties:

\[(2) \quad R \subset B \left[ \frac{1}{a} \right] \quad \text{and} \quad f(x) \in A \left[ \frac{1}{a} \right][x].\]

As $f(x)$ is prime to its derivative $f'(x)$, there exist polynomials $u(x), v(x) \in A[x]$ such that

\[(3) \quad u(x)f(x) + v(x)f'(x) = b\]

for some nonzero $b \in A$. Set $c := ab \in A (= \mathbb{Z}[s_1, \ldots, s_l])$ and choose $z_1, \ldots, z_l \in \mathbb{Z}$ so that $c_0 := c(z_1, \ldots, z_l) \neq 0$. Let $\nu : A \rightarrow \mathbb{Z}$ be the homomorphism specializing $s_i$ to $z_i$, and $F$ be the splitting field over $\mathbb{Q}$ of $g(x) := f''(x)$. It follows from the Tchebotarev Density Theorem that the set of primes

\[\Pi := \{ p \mid F \subset \mathbb{Q}_p \quad \text{and} \quad p \nmid c_0 \}\]

is infinite (this, in fact, can also be proved by an elementary argument). We claim that $\Pi$ is as required.

Indeed, suppose $p \in \Pi$. Then by our construction all roots of $g(x)$ belong to $\mathbb{Q}_p$; moreover, since $c_0 \in \mathbb{Z}_p \times$, the coefficients of $g(x)$ belong to $\mathbb{Z}_p$ by (2), and therefore the roots actually belong to $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is uncountable, there exist elements $t_1, \ldots, t_l \in \mathbb{Z}_p$ which are algebraically independent over $\mathbb{Q}$ and satisfy the congruences $t_i \equiv z_i \pmod{p}$ for all $i = 1, \ldots, l$. Let $\varepsilon : L \rightarrow \mathbb{Q}_p$ be the embedding sending $s_i$ to $t_i$. We claim that $h(x) := f^\varepsilon(x)$ splits over $\mathbb{Z}_p$ into linear factors. For this, we first observe that $\varepsilon(c) \equiv c_0 \pmod{p}$, implying that $\varepsilon(c) \in \mathbb{Z}_p \times$, and therefore $h(x) \in \mathbb{Z}_p[x]$ in view of (2). Moreover, for the canonical homomorphism $\mathbb{Z}_p \rightarrow \mathbb{Z}_p/p\mathbb{Z}_p = : \mathbb{F}_p$, $z \mapsto \bar{z}$, one has $\bar{h}(x) = \bar{g}(x)$, hence by the above, $h(x)$ splits over $\mathbb{F}_p$ into linear factors. On the other hand, it follows from (3) that

\[\bar{u}^\varepsilon(x) \bar{h}(x) + \bar{v}^\varepsilon(x) \bar{h}'(x) = \bar{z}(\bar{b}) \neq 0,\]
which implies that $\tilde{h}(x)$ is prime to its derivative $\tilde{h}'(x)$, and so it does not have multiple roots. Invoking Hensel’s Lemma, we now conclude that $h(x)$ splits over $\mathbb{Z}_p$ into linear factors, as was claimed. It follows that for any extension $\tilde{\varepsilon}: K \to \overline{\mathbb{Q}}_p$ (= an algebraic closure of $\mathbb{Q}_p$) of $\varepsilon$, one has $\tilde{\varepsilon}(K) \subset \mathbb{Q}_p$. Furthermore, as $\tilde{\varepsilon}(\alpha)$ is a root of $h(x)$, and, on the other hand, all the roots of $h(x)$ belong to $\mathbb{Z}_p$, we obtain that $\tilde{\varepsilon}(\alpha) \in \mathbb{Z}_p$, i.e. $\tilde{\varepsilon}(B) \subset \mathbb{Z}_p$. Since by our construction $\varepsilon(a) \in \mathbb{Z}_p^*$, it follows from (2) that $\varepsilon(\mathcal{R}) \subset \mathbb{Z}_p$. Thus, $\varepsilon_p := \tilde{\varepsilon}$ is an embedding which has all of the required properties.

We shall view $G$ as a $K$-subgroup of $\mathbf{GL}_n$ in terms of a fixed embedding. For a subring $R$ of a commutative $K$-algebra $C$, in the sequel $G(R)$ will denote the group $G(C) \cap \mathbf{GL}_n(R)$.

For the proof of Theorem 2, we also need the following:

**Lemma 2.** Let $G$ be a semisimple algebraic group defined over a field $K$ of characteristic zero, and let $R$ be a subring of $K$. Given a finite set $S$ of distinct primes and a system of embeddings $\varepsilon_p: K \to \mathbb{Q}_p$ with the property $\varepsilon_p(\mathcal{R}) \subset \mathbb{Z}_p$, one for each $p \in S$, we let $\varepsilon_S: G(K) \to G_S$ denote the embedding induced by the $\varepsilon_p$’s. Then for any subsemigroup $\Gamma$ of $G(\mathcal{R})$, which is Zariski-dense in $G$, the closure of $\varepsilon_S(\Gamma)$ in $G_S$ is open.

**Proof.** Given a subset $X$ of $G(K)$, let $\overline{X}^{(S)}$ denote the closure of $\varepsilon_S(X)$ in $G_S$. Also, for an individual $p \in S$, we let $\delta_p: G(K) \to G(\mathbb{Q}_p)$ denote the embedding induced by $\varepsilon_p$ and will use $\overline{X}^{(p)}$ to denote the closure of $\delta_p(X)$ in $G(\mathbb{Q}_p)$. Since a closed subsemigroup of a profinite group is in fact a subgroup (simply because the set of natural numbers $\mathbb{N}$ is dense in the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$), we have $\overline{\Gamma}^{(S)} = \overline{\Delta}^{(S)} (\subset \prod_{p \in S} G(\mathbb{Z}_p))$, where $\Delta$ is the subgroup of $G(\mathcal{R})$ generated by $\Gamma$, so we may assume from the outset that $\Gamma$ is a subgroup. A standard argument (going back to Platonov’s proof [13] of the strong approximation property) shows that $H(p) := \overline{\Gamma}^{(p)}$ is open in $G(\mathbb{Q}_p)$, for every $p \in S$. Indeed, let $G = G^{(1)} \cdot \cdots \cdot G^{(l)}$ be a decomposition of $G$ as an almost direct product of its $\mathbb{Q}_p$-simple factors. Then the Lie algebra $\mathfrak{g}$ of $G$ is the direct sum of the Lie algebras $\mathfrak{g}^{(i)}$ of $G^{(i)}$, $i = 1, \ldots, l$. Moreover, since $G^{(l)}$ is $\mathbb{Q}_p$-simple, the algebra $\mathfrak{g}^{(l)}_{\mathbb{Q}_p}$ does not have any proper ideals. Now, by the $p$-adic analogue of Cartan’s theorem on closed subgroups (see [6], Ch. III, §8, n°2, Thm. 2), $H(p)$ is a $p$-adic Lie group. Let $\mathfrak{h}(p)$ denote its Lie algebra. Since $\Gamma$ is Zariski-dense in $G$, $\mathfrak{h}(p)$ is an ideal of $\mathfrak{g}_{\mathbb{Q}_p}$ (cf. [14], Proposition 3.4), and therefore $\mathfrak{h}(p) = \oplus_{i \in I} \mathfrak{g}^{(i)}_{\mathbb{Q}_p}$ for some subset $I \subset \{1, \ldots, l\}$. If we assume that there is an $i \in \{1, \ldots, l\} - I$, then $F := H(p) \cap \overline{G}^{(i)}(\mathbb{Q}_p)$, where $\overline{G}^{(i)} = G^{(1)} \cdot \cdots \cdot G^{(i-1)}G^{(i+1)} \cdots G^{(l)}$, has the same Lie algebra as $H(p)$, hence is open in $H(p)$. But being a closed subgroup of $G(\mathbb{Z}_p)$, the subgroup $H(p)$ is compact, so $[H(p): F] < \infty$, and hence $[\Gamma : \Gamma \cap \overline{G}^{(i)}] < \infty$. This contradicts the fact that $\Gamma$ is Zariski-dense in $G$, proving that in fact $\mathfrak{h}(p) = \mathfrak{g}_{\mathbb{Q}_p}$, and therefore $H(p)$ is open in $G(\mathbb{Q}_p)$, as claimed.
Now, let $H = \Gamma^{(S)}$. It suffices to show that

$$H \cap G(Q_p) \text{ is open in } G(Q_p),$$

for all $p \in S$. If $\pi_p: G_S \to G(Q_p)$ is the projection corresponding to $p$, then $\pi_p(H) = H(p)$. Since $H(p)$ possesses an open pro-$p$ subgroup, it follows that for a Sylow pro-$p$ subgroup $H_p$ of $H$, the subgroup $\pi_p(H_p)$ is open in $H(p)$, hence also in $G(Q_p)$. But $\pi_q(H_p)$ is finite for any $q \neq p$, so $H_p \cap G(Q_p)$ is open in $H_p$, and (4) follows.

**Remark 5.** The strong approximation theorem of Nori and Weisfeiler (see [11], [20], and also [12]) provides a substantially more precise information about the closure of $\Gamma$, but the (almost obvious) assertion of Lemma 2 is sufficient for our purpose.

**Proof of Theorem 2.** Since $\Gamma$ is finitely generated, there exists a finitely generated subring $R$ of $K$ such that $\Gamma \subset G(R) = G \cap GL_n(R)$. Fix a maximal $K$-torus $T$ of $G$, and let $L$ denote the splitting field of $T$ over $K$. Let $r$ be the number of nontrivial conjugacy classes of the Weyl group $W(G,T)$. Using Proposition 1, one can find a set $S$ consisting of $r$ distinct rational primes such that for each $p \in S$, there exists an embedding $\varepsilon_p: L \hookrightarrow Q_p$ so that $\varepsilon_p(R) \subset Z_p$. Let $v_p$ denote the restriction of the $p$-adic valuation to $K \simeq \varepsilon_p(K)$ (in the sequel, we will make no distinction between $p$ and $v_p$; in particular, we will think of $S$ as also as the set of all the $v_p$'s). Then $K_{v_p} = Q_p$ and $G$ splits over $K_{v_p}$, for all $p \in S$. This means that Theorem 3 applies in our set-up, and we let $U$ denote the open subset of $G_S$ given by assertion (ii) of that theorem. Now if $G$ is $\mathbb{R}$-isotropic, by [15], $\Gamma$ contains an $\mathbb{R}$-regular element $y$, and then by Lemma 3.5 of [16], there exists a nonempty Zariski-open subset $W$ of $G$ ($W$ can clearly be assumed to be defined over $K$) such that for any $x \in G(\mathbb{R}) \cap W$, the element $xy^m$ is $\mathbb{R}$-regular for all sufficiently large $m$. If $G$ is anisotropic over $\mathbb{R}$, we let $y = 1$ and $W = G$. Let $W_S = \prod_{v \in S} W(K_v) \subset G_S$.

Let $\delta_S$ be as in the preceding lemma and $H$ be the closure of $\delta_S(\Gamma)$ in $G_S$. According to Lemma 2, $H$ is open. Hence by property (a) of $U$ described in Theorem 3(ii), $H \cap U \neq \emptyset$. It follows that $X := H \cap U \cap W_S$ is a nonempty open subset of $H$, and $\delta_S(\Gamma) \cap X$ is dense in $X$. Let $x$ be an element of $\Gamma$ such that $\delta_S(x) \in X$. There exists an open normal subgroup $\Omega$ of $\prod_{p \in S} G(\mathbb{Z}_p)$, of index, say, $d$, such that

$$\delta_S(x)\Omega \subset U.$$

For all large positive integers $m$, say for $m \geq s(x)$, the element $xy^{dm}$ is $\mathbb{R}$-regular. Since $\delta_S(y)^d \in \Omega$, it follows from (5) that $\delta_S(xy^{dm}) \in \delta_S(\Gamma) \cap U$, so by Theorem 3, $xy^{dm}$ is a $\mathbb{R}$-regular $K$-quasi-irreducible anisotropic element without components of finite order. The Zariski-closure of the set $\{xy^{dm} \mid m \geq s(x)\}$ clearly contains $x$. As $x$ was an arbitrary element of $\Gamma$ such that $\delta_S(x) \in X$, and the set of such elements is a Zariski-dense subset of $G$, we conclude that the subset of
\(\Gamma\) consisting of all \(\mathbb{R}\)-regular \(K\)-quasi-irreducible anisotropic elements without components of finite order is Zariski-dense in \(G\). This proves Theorem 2. \(\square\)

**Remark 6.** Let \(K\) and \(G\) be as in Theorem 2 and \(\Gamma\) be a finitely generated Zariski-dense subgroup of \(G(K)\). Let \(L, S,\) for \(p \in S, \varepsilon_p, H, U\) and \(X\) be as in the proof of Theorem 2 and \(\delta_S\) be as in Lemma 2. We fix an element \(x\) of \(\Gamma\) such that \(\delta_S(x) \in X\). Let \(\Omega\) be an open normal subgroup of \(\prod_{p \in S} G(\mathbb{Z}_p)\) as in the proof of Theorem 2 and let \(\Delta = \delta_S^{-1}(\delta_S(\Gamma) \cap \Omega)\). As \(H\) is compact, \(\Delta\) has finite index in \(\Gamma\), hence it is Zariski-dense in \(G\). By Theorem 6.8 of [1], there exists a finite subset \(M\) of \(\Delta\) such that for every \(g \in G(\mathbb{R})\) at least one of the elements \(\gamma g, \gamma \in M,\) is \(\mathbb{R}\)-regular. Let \(Q\) be the set of \(\mathbb{R}\)-regular elements in \(x\Delta\). Then we have \(x\Delta = M^{-1}Q\).

Clearly,
\[
\delta_S(x\Delta) \subset \delta_S(x)\Omega \subset U,
\]
and hence, every element of \(x\Delta\) is \(K\)-quasi-irreducible anisotropic and none of them have components of finite order. This implies the following strengthening of Theorem 2:

*The subgroup \(\Gamma\) is the union of finitely many translates of the subset consisting of all \(\mathbb{R}\)-regular \(K\)-quasi-irreducible anisotropic elements which do not have components of finite order.*

In conclusion, we point out that \(\mathbb{R}\)-regular elements are closely related to the so-called *proximal* elements, which are defined as invertible linear transformations of a finite dimensional vector space, over a nondiscrete locally compact field, which have a unique eigenvalue of maximum absolute value which, in addition, occurs with multiplicity one. We recall that according to Lemma 3.4 of [16] an element \(g \in G(\mathbb{R})\) is \(\mathbb{R}\)-regular if and only if the element \(\rho(g)\) is proximal, where \(\rho\) is the representation of \(G(\mathbb{R})\) constructed as follows: let \(G(\mathbb{R}) = KAN\) be a fixed Iwasawa decomposition, \(g\) and \(n\) be the (real) Lie algebras of \(G(\mathbb{R})\) and \(N\) respectively, and \(k = \dim n\); let \(\sigma\) denote the representation of \(G(\mathbb{R})\) on \(\wedge^k g\) obtained from the adjoint representation, and let \(V\) be the smallest \(G(\mathbb{R})\)-submodule of \(\wedge^k g\) containing the 1-dimensional subspace \(\wedge^k n\); then \(\rho\) is the restriction of \(\sigma\) to \(V\).

Proximal elements were used by H. Furstenberg to analyze the “universal boundary” of a Lie group, and more recently in [2] to investigate the Auslander problem about properly discontinuous groups of affine transformations (not to mention the fact that proximal elements in the nonarchimedean set-up were used by J. Tits in the proof of his celebrated theorem on the existence of free subgroups in nonvirtually solvable linear groups).

Gol’dsheid and Margulis ([9]) have proved that if \(G\) is a connected semisimple \(\mathbb{R}\)-subgroup of \(GL(V)\) such that \(V\) is irreducible as a \(G\)-module, and \(G(\mathbb{R})\) contains a proximal element, then so does any Zariski-dense subsemigroup \(\Gamma\) of \(G(\mathbb{R})\) (a more precise result in this direction was obtained in [1]). Using the result of Gol’dsheid-Margulis in place of the result of [15] and an obvious analogue
of Lemma 3.5 of [16] for proximal elements and repeating verbatim the above argument, one obtains the following.

**Theorem 4.** Let $G$ be a connected semisimple real algebraic subgroup of $GL(V)$ such that $V$ is irreducible as a $G$-module and $G(\mathbb{R})$ contains a proximal element. Then any Zariski-dense subsemigroup $\Gamma$ of $G(\mathbb{R})$ contains a regular semisimple proximal element $x$ which generates a Zariski-dense subgroup of the torus $T := Z_G(x)$.

**Acknowledgements**

Both the authors were supported by grants from NSF and BSF. They thank Margulis and Soifer for their question.

**References**


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109, U.S.A.  
*E-mail address: gprasad@umich.edu*

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VIRGINIA, CHARLOTTESVILLE, VA 22904, U.S.A.  
*E-mail address: asr3x@wyl.math.virginia.edu*