

ZARISKI-DENSE SUBGROUPS AND TRANSCENDENTAL NUMBER THEORY

GOPAL PRASAD AND ANDREI S. RAPINCHUK

Let K be a field, L be a field extension of K , and G be a connected semisimple algebraic group defined over K . In [6], we called a K -torus T to be K -irreducible if it does not contain any proper K -subtori. We established the existence of such tori in any connected absolutely (almost) simple algebraic group over a global field and gave applications of this result, in particular, to the congruence subgroup problem. Subsequently, in [8] we considered maximal tori in arbitrary semisimple groups, where the notion of irreducible tori had to be replaced with a more general notion of quasi-irreducible tori. As in [8], we will say that a maximal L -torus T of G is L -quasi-irreducible (or, quasi-irreducible over L) if it does not contain any L -subtori other than (almost direct) products of the subtori $T^{(i)} := T \cap G^{(i)}$, where $G^{(1)}, \dots, G^{(s)}$ are the connected L -simple normal subgroups of G . In [8], we proved the existence of K -quasi-irreducible tori in G if K is a finitely generated field of characteristic zero. (A noteworthy feature of the argument in [8] is that it is based on the technique of embedding relevant finitely generated fields into nonarchimedean local fields, developed and used earlier in [7] for a different purpose.)

Assume now that K is a finitely generated subfield of the field \mathbb{R} of real numbers. In [8] we proved that any Zariski-dense subsemigroup of $G(K)$ contains a regular \mathbb{R} -regular element x such that the centralizer T of x in G is a K -quasi-irreducible torus and the cyclic subgroup of $T(K)$ generated by x is Zariski-dense in T . Since such elements will also play an important role in the current paper, we recall for the reader's convenience that a semisimple element $x \in G$ is called *regular* if the identity component $Z_G(x)^\circ$ of its centralizer is a (maximal) torus; note that $x \in Z_G(x)^\circ$ ([4], 11.12). Regular elements form a Zariski-open subset of G (cf. [4], §12). A regular element x of $G(L)$ will be called L -quasi-irreducible if the maximal L -torus $T := Z_G(x)^\circ$ is L -quasi-irreducible, and x will be called L -quasi-irreducible anisotropic if, in addition, T is anisotropic over L . We will say that an element $x \in G(K)$ is *without components of finite order*, if in some (equivalently, any) decomposition $x = x_1 \cdots x_t$, with $x_i \in \mathcal{G}_i$, where $\mathcal{G}_1, \dots, \mathcal{G}_t$ are the connected absolutely simple normal subgroups of G , all the x_i 's have infinite order. It is easy to see that (for $x \in G(K)$) this notion is equivalent to the one introduced in [8].

An element $x \in G(\mathbb{R})$ is called \mathbb{R} -regular if the number of eigenvalues, counted with multiplicity, of modulus 1 of $\text{Ad } x$ is minimum possible. Such an element

Received June 30, 2004.

is necessarily semisimple, and the identity component of its centralizer contains a maximal \mathbb{R} -split torus of G in its center (see [5], 1.5 and 1.6(1)).

The purpose of the current paper, which is a sequel to [8], is to use L -quasi-irreducible anisotropic elements to answer questions posed by Y. Benoist [3] and by T.J. Hitchman and R. Spatzier. Corollaries 1 and 2 of this paper answer the question of Hitchman and Spatzier and these are being used by Hitchman in his study of smooth deformation rigidity of “standard” actions of lattices in semisimple groups of real rank one on compact manifolds.

Let now G be a connected semisimple algebraic group defined over \mathbb{R} and Γ be a Zariski-dense subsemigroup of $G(\mathbb{R})$. We observe that Γ contains a finitely generated Zariski-dense subsemigroup, hence while dealing with questions about the existence of elements in Γ with certain special properties, Γ can be assumed to be finitely generated. We will therefore assume in the sequel that Γ is finitely generated. We fix a finitely generated subfield K of \mathbb{R} over which G is defined and such that $\Gamma \subset G(K)$. In the following, all finitely generated field extensions of K are assumed to be contained in the field \mathbb{C} of complex numbers.

First, we notice that Theorem 2 of [8] generalizes to the following.

Theorem 1. *Given a finitely generated extension field L of K , there exists a Zariski-dense subset $\Delta(L)$ of Γ with the following property: every $\gamma \in \Delta(L)$ is \mathbb{R} -regular, L -quasi-irreducible anisotropic, and is without components of finite order.*

One can prove Theorem 1 in exactly the same way as Theorem 2 was proven in [8]; for this we need to replace K by L in the statement and proof of Theorem 3 of [8]. The argument uses embeddings ε_p of a finite extension of L , over which G splits, into various p -adic fields \mathbb{Q}_p 's which take the ring \mathcal{R} generated by the matrix entries of a finite set of generators of Γ (here G is being viewed as a K -subgroup of GL_n in terms of a fixed K -embedding) into \mathbb{Z}_p (see Proposition 1 of [8]); it yields a Zariski-dense set of regular \mathbb{R} -regular elements $\gamma \in \Gamma$ without components of finite order such that for the splitting field F of the K -torus $T = Z_G(\gamma)^\circ$, the Galois group $\mathrm{Gal}(FL/L)$ contains the Weyl group $W(G, T)$; such a torus T is quasi-irreducible and anisotropic over L .

Using Theorem 1 and a simple induction, one obtains the following.

Corollary 1. *Let L_0 be a finitely generated field extension of K . For any $n \geq 1$, there exist regular \mathbb{R} -regular elements $\gamma_1, \dots, \gamma_n \in \Gamma$ without components of finite order such that if L_j is the minimal splitting field (over K) of the K -torus $T_j := Z_G(\gamma_j)^\circ$, then T_i is quasi-irreducible and anisotropic over the compositum $L_0 L_1 \dots L_{i-1}$, for all $i \leq n$.*

Let $\Delta(L) (\subset \Gamma \subset G(K))$ be as in Theorem 1 and let $\gamma \in \Delta(L)$. Then $T := Z_G(\gamma)^\circ$ is a maximal K -torus which contains a maximal \mathbb{R} -split torus of G , $\gamma \in T$ ([4], 11.12), and T is quasi-irreducible and anisotropic over L . The

identity component of the Zariski-closure of the cyclic subgroup generated by γ is a subtorus of T defined over K , and as γ is without components of finite order, this subtorus equals T . Thus the cyclic subgroup generated by γ is dense in T . (This implies, in particular, that $T = Z_G(T) = Z_G(\gamma)$, i. e., $Z_G(\gamma)$ is connected.) We now record some simple, but useful, facts pertaining to this situation. As usual, for a torus T , $X(T)$ will denote the group of characters of T .

Lemma 1. *Let T be a torus defined and anisotropic over a field \mathcal{L} , and $\gamma \in T(\mathcal{L})$ be an element that generates a Zariski-dense subgroup of T .*

- (1) *If $\chi \in X(T)$ is such that $\chi(\gamma) \in \mathcal{L}^\times$, then $\chi = 0$.*
- (2) *Given linearly independent characters $\chi_1, \dots, \chi_m \in X(T)$, if $s_1, \dots, s_m \in \mathbb{Z}$ are such that $\chi_1(\gamma)^{s_1} \cdots \chi_m(\gamma)^{s_m} \in \mathcal{L}^\times$, then $s_1 = \dots = s_m = 0$.*

Proof. (1): For any σ in the absolute Galois group $\text{Gal}(\mathcal{L}^s/\mathcal{L})$, one has

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

Since γ generates a Zariski-dense subgroup of T , we conclude that $\chi^\sigma = \chi$, i.e. χ is defined over \mathcal{L} . But then $\chi = 0$ as T is anisotropic over \mathcal{L} .

(2): Let $\chi = s_1\chi_1 + \dots + s_m\chi_m$. Then

$$\chi(\gamma) = \chi_1(\gamma)^{s_1} \cdots \chi_m(\gamma)^{s_m} \in \mathcal{L}^\times,$$

so $\chi = 0$ by (1), and (2) follows. □

The following proposition generalizes Lemma 1 to the case of several tori.

Proposition 1. *Let L_0 be a finitely generated field containing K . Given regular semisimple elements $\gamma_1, \dots, \gamma_n \in G(K)$, we let $T_i = Z_G(\gamma_i)^\circ$ be the corresponding tori. Let L_i denote the splitting field of T_i over K , for $i \leq n$. Assume that for each $i \leq n$, the following two conditions hold*

- (1) *γ_i generates a Zariski-dense subgroup of T_i ;*
- (2) *T_i is anisotropic over the compositum $L_0L_1 \cdots L_{i-1}$.*

Then, given linearly independent characters $\chi_1^{(i)}, \dots, \chi_{m_i}^{(i)} \in X(T_i)$ and integers $s_{i,j}$ (where $i = 1, \dots, n$; $j = 1, \dots, m_i$), a relation of the form

$$(1) \quad \prod_{i=1}^n \prod_{j=1}^{m_i} \chi_j^{(i)}(\gamma_i)^{s_{i,j}} \in L_0^\times$$

implies that all the $s_{i,j}$'s are zero.

Proof. The relation (1) obviously implies that

$$\prod_{j=1}^{m_n} \chi_j^{(n)}(\gamma_n)^{s_{n,j}} \in L_0L_1 \cdots L_{n-1}.$$

Applying Lemma 1(2), we obtain $s_{n,1} = \dots = s_{n,m_n} = 0$. Then a simple induction completes the proof. \square

For convenience of reference we state separately the assertion of the proposition for the case of two tori.

Corollary 2. *Let $\gamma_1, \gamma_2 \in G(K)$ be two regular semisimple elements without components of finite order, and T_1 and T_2 be the identity components of their centralizers in G . Assume that T_1 is quasi-irreducible and anisotropic over K , and T_2 possesses these properties over L_1 , the splitting field of T_1 over K . If $\chi_i \in X(T_i)$ are nontrivial characters, where $i = 1, 2$, then a relation of the form*

$$\chi_1(\gamma_1)^{s_1} = \chi_2(\gamma_2)^{s_2},$$

with $s_1, s_2 \in \mathbb{Z}$, implies that $s_1 = s_2 = 0$.

Proposition 2. *Assume that K is a real number field. Then for any two elements $\gamma_1, \gamma_2 \in G(K)$ with the properties described in Corollary 2 and any nontrivial characters $\chi_i \in X(T_i)$, the ratio*

$$\theta := \frac{\log \chi_1(\gamma_1)}{\log \chi_2(\gamma_2)}$$

is transcendental over \mathbb{Q} for any values of the logarithms.

Proof. It follows from Corollary 2 that θ is irrational. Then according to a theorem proved independently by Gel'fond and Schneider in 1934 (this theorem solved Hilbert's seventh problem), θ is in fact transcendental (cf. [2]). \square

A character χ of an \mathbb{R} -torus T is called *positive* if for every $x \in T(\mathbb{R})$, the value $\chi(x)$ is a positive real number. Any positive character of T is defined over \mathbb{R} . Given an arbitrary character $\chi \in X(T)$, the character $\chi + \bar{\chi}$, where $\bar{\chi}$ is the character obtained by applying the complex conjugation to χ , satisfies

$$(\chi + \bar{\chi})(x) = \chi(x)\overline{\chi(x)} = |\chi(x)|^2,$$

for all $x \in T(\mathbb{R})$. Thus, for any character χ and $x \in T(\mathbb{R})$, the square of the absolute value of $\chi(x)$ is the value assumed by the positive character $\chi + \bar{\chi}$ of T at x .

We now fix a maximal compact subgroup \mathcal{K} of $\mathcal{G} := G(\mathbb{R})$. Let \mathfrak{g} be the Lie algebra of \mathcal{G} and \mathfrak{k} be the subalgebra corresponding to \mathcal{K} . Let \mathfrak{p} be the orthogonal complement of \mathfrak{k} in \mathfrak{g} under the Killing form $\langle \cdot, \cdot \rangle$ on \mathfrak{g} . Then $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ is a Cartan decomposition of \mathfrak{g} . Let \mathfrak{a} be a Cartan subspace contained in \mathfrak{p} , and $\mathcal{A} = \exp \mathfrak{a}$ be the connected abelian subgroup of \mathcal{G} with Lie algebra \mathfrak{a} . We fix a (closed) Weyl chamber \mathfrak{a}^+ in \mathfrak{a} . Let S be the Zariski-closure of \mathcal{A} . Then S is a maximal \mathbb{R} -split torus of G and $\mathcal{A} = S(\mathbb{R})^\circ$.

Let T be a \mathbb{R} -torus of G containing S . As S is \mathbb{R} -split, every character of S is defined over \mathbb{R} . Now given a character α of S , let χ be a complex character

of T whose restriction to S is α . Then the restriction of the positive character $\chi + \bar{\chi}$ to S is 2α . Thus every character lying in the subgroup $2X(S)$ extends to a positive character of any \mathbb{R} -torus of G containing S .

Let $g \in \mathcal{G}$ and let $x \in \mathcal{G}$ be its semisimple Jordan component. Let H be the Zariski-closure of the cyclic group generated by x and T be a maximal \mathbb{R} -torus of G containing H . Let \mathcal{C} be the maximal compact subgroup of $T(\mathbb{R})$ and T_s be the maximal \mathbb{R} -split subtorus of T . Then $T(\mathbb{R})$ is a direct product of \mathcal{C} and $T_s(\mathbb{R})^\circ$ and any positive character of T is trivial on \mathcal{C} . Moreover, $H(\mathbb{R}) \cap \mathcal{C}$ is the unique maximal compact subgroup of $H(\mathbb{R})$, $H_s := (H \cap T_s)^\circ$ is the maximal \mathbb{R} -split subtorus of H° , and hence $H(\mathbb{R})$ is a direct product of $H(\mathbb{R}) \cap \mathcal{C}$ and the Euclidean group $H_s(\mathbb{R})^\circ = H(\mathbb{R}) \cap T_s(\mathbb{R})^\circ$. Let $x = x_e \cdot x_h$, with $x_e \in H(\mathbb{R}) \cap \mathcal{C}$ and $x_h \in H_s(\mathbb{R})^\circ$. Then x_e is called the *elliptic* component of x (or of g), and x_h the *hyperbolic* component. There is an element $z \in \mathcal{G}$ which conjugates \mathcal{C} into \mathcal{K} and $T_s(\mathbb{R})^\circ$ into \mathcal{A} such that $zx_hz^{-1} = \exp X$, with $X \in \mathfrak{a}^+$. The element X is the unique element of \mathfrak{a}^+ such that the hyperbolic component of g is a conjugate of $\exp X$, and we will denote it by $\ell(g)$. Thus we get a map $\ell : \mathcal{G} \rightarrow \mathfrak{a}^+$.

Let $\{\alpha_1, \dots, \alpha_r\}$, where $r = \text{rk}_{\mathbb{R}} G = \dim S$, be the basis of the root system of G , with respect to S , determined by the Weyl chamber \mathfrak{a}^+ , and let $\beta_i = 2\alpha_i$. Then β_1, \dots, β_r are linearly independent characters which uniquely extend to positive characters of any \mathbb{R} -torus of G containing S . We will identify $\mathcal{A} = S(\mathbb{R})^\circ$ and \mathfrak{a} with \mathbb{R}^r as follows: $a \in \mathcal{A}$ will be identified with $(\log \beta_1(a), \dots, \log \beta_r(a))$ and $X \in \mathfrak{a}$ will be identified with $(d\beta_1(X), \dots, d\beta_r(X))$; where, for $i \leq r$, $d\beta_i$ denotes the derivative of β_i .

Given a \mathbb{R} -torus T of G such that the maximal \mathbb{R} -split subtorus T_s of T is a maximal \mathbb{R} -split torus of G , and an element $g \in T(\mathbb{R})$, there is a $z \in \mathcal{G}$ such that $zT_sz^{-1} = S$ and $zg_hz^{-1} = \exp X$, with $X \in \mathfrak{a}^+$, where g_h is the hyperbolic component of g . Then $\ell(g) = X$. For $i \leq r$, let χ_i be the unique positive character of T extending the character $\text{Int } z^{-1} \cdot \beta_i$ of T_s , and $d\chi_i$ be the derivative of χ_i . Note that $\chi_i(g_h) = \chi_i(g)$ for all i . Now it is obvious that

$$\begin{aligned} \ell(g) &= (d\chi_1(\text{Ad } z^{-1}(X)), \dots, d\chi_r(\text{Ad } z^{-1}(X))) \\ &= (\log \chi_1(g), \dots, \log \chi_r(g)). \end{aligned}$$

An interesting result of Benoist [3] is that if Γ is a Zariski-dense subsemigroup of \mathcal{G} , then $\ell(\Gamma)$ generates a dense subgroup of \mathfrak{a} . At the end of [3], Benoist asks if one can always find a *finite* subset F of Γ such that $\ell(F)$ generates a dense subgroup of \mathfrak{a} . The following theorem answers Benoist's question in the affirmative if Γ is a Zariski-dense subsemigroup of $G(K)$, K a real number field.

Theorem 2. *Assume that K is a real number field. Every Zariski-dense subsemigroup Γ of $G(K)$ contains a finite subset F such that $\ell(F)$ generates a dense subgroup of \mathfrak{a} .*

Proof. Let $r = \text{rk}_{\mathbb{R}} G$ and pick an integer $n \geq r^2 - r + 2$. Using Corollary 1 with $L_0 = K$, we find regular \mathbb{R} -regular elements $\gamma_1, \dots, \gamma_n \in \Gamma$ with the properties

described therein. Then

$$\ell(\gamma_j) = (\log \chi_1^{(j)}(\gamma_j), \dots, \log \chi_r^{(j)}(\gamma_j)),$$

for some linearly independent positive characters $\chi_1^{(j)}, \dots, \chi_r^{(j)}$ of the torus $T_j = Z_G(\gamma_j)^\circ$, for every $j \leq n$. It follows from Proposition 1 that the positive algebraic numbers $\chi_i^{(j)}(\gamma_j)$, where $i \leq r, j \leq n$, are multiplicatively independent. According to Corollary 7.4 of [10], given multiplicatively independent positive algebraic numbers $\alpha_{i,j}, 1 \leq i \leq r, 1 \leq j \leq n$, with $n \geq r^2 - r + 2$, the subgroup of $(\mathbb{R}_+^*)^r$ generated by the n elements

$$(\alpha_{1,j}, \dots, \alpha_{r,j}), \quad 1 \leq j \leq n,$$

is dense in $(\mathbb{R}_+^*)^r$. This implies at once that the subgroup of $\mathbb{R}^r \simeq \mathfrak{a}$ generated by the $\ell(\gamma_j)$'s, for $j \leq n$, is dense. \square

Assuming the following well known, but very difficult, conjecture in transcendental number theory ([1]), one can answer Benoist's question in the affirmative for any Zariski-dense subsemigroup of \mathcal{G} .

Schanuel's conjecture. *If $z_1, \dots, z_n \in \mathbb{C}$ are linearly independent over \mathbb{Q} , then the transcendence degree (over \mathbb{Q}) of the field generated by*

$$z_1, \dots, z_n; e^{z_1}, \dots, e^{z_n}$$

is $\geq n$.

Theorem 3. *Assume that Schanuel's conjecture holds, and let $r = \text{rk}_{\mathbb{R}} G$. Then there exist $r + 1$ elements $\gamma_1, \dots, \gamma_{r+1} \in \Gamma$ such that $\ell(\gamma_1), \dots, \ell(\gamma_{r+1})$ generate a dense subgroup of \mathfrak{a} .*

Proof. It follows from the result of [3] mentioned above that there exist elements $\delta_1, \dots, \delta_r \in \Gamma$ such that the vectors $\ell(\delta_1), \dots, \ell(\delta_r)$ form a basis of \mathfrak{a} as a vector space over \mathbb{R} . Let

$$\ell(\delta_i) = (a_{i,1}, \dots, a_{i,r}),$$

and let P be the field generated by the $a_{i,j}$'s over \mathbb{Q} . The transcendence degree of P/\mathbb{Q} is at most r^2 .

Now, given $g \in G(\mathbb{R})$, there are uniquely determined real numbers $x_1(g), \dots, x_r(g)$ such that

$$\ell(g) = \sum_{i=1}^r x_i(g) \ell(\delta_i).$$

Let $\ell(g) = (\varphi_1(g), \dots, \varphi_r(g))$. Then

$$(2) \quad \varphi_1(g), \dots, \varphi_r(g) \in P(x_1(g), \dots, x_r(g)).$$

According to a well known result of Kronecker, the elements $\ell(\delta_1), \dots, \ell(\delta_r)$ and $\ell(\gamma)$ generate a dense subgroup of \mathfrak{a} if and only if $1, x_1(\gamma), \dots, x_r(\gamma)$ are linearly independent over \mathbb{Q} . We will show that there exists a $\gamma \in \Gamma$ with this

property. Assume by way of contradiction that for every $\gamma \in \Gamma$, the numbers $1, x_1(\gamma), \dots, x_r(\gamma)$ are linearly dependent over \mathbb{Q} . Then given elements $\gamma_1, \dots, \gamma_n \in \Gamma$, the transcendence degree over \mathbb{Q} of the field

$$\mathcal{P}(\gamma_1, \dots, \gamma_n) := P(x_1(\gamma_1), \dots, x_r(\gamma_1); \dots; x_1(\gamma_n), \dots, x_r(\gamma_n))$$

is $\leq n(r - 1) + r^2$.

Fix $n > 1$ and pick regular \mathbb{R} -regular elements $\gamma_1, \dots, \gamma_n \in \Gamma (\subset G(K))$ with the properties described in Corollary 1 for $L_0 = K$. From the description of $\ell(g) (= (\varphi_1(g), \dots, \varphi_r(g)))$ given before Theorem 2, we know that

$$\varphi_1(\gamma_i) = \log \chi_1^{(i)}(\gamma_i), \dots, \varphi_r(\gamma_i) = \log \chi_r^{(i)}(\gamma_i),$$

for some linearly independent positive characters $\chi_1^{(i)}, \dots, \chi_r^{(i)}$ of $T_i = Z_G(\gamma_i)^\circ$. It now follows from Proposition 1 that the elements

$$\varphi_1(\gamma_1), \dots, \varphi_r(\gamma_1); \dots; \varphi_1(\gamma_n), \dots, \varphi_r(\gamma_n)$$

are linearly independent over \mathbb{Q} .

According to Schanuel’s conjecture, the transcendence degree of the field generated by the elements

$$\varphi_1(\gamma_1), \dots, \varphi_r(\gamma_1); \dots; \varphi_1(\gamma_n), \dots, \varphi_r(\gamma_n);$$

and

$$e^{\varphi_1(\gamma_1)}, \dots, e^{\varphi_r(\gamma_1)}; \dots; e^{\varphi_1(\gamma_n)}, \dots, e^{\varphi_r(\gamma_n)}$$

is $\geq nr$. However, since $e^{\varphi_j(\gamma_i)} = \chi_j^{(i)}(\gamma_i)$ is algebraic over K for all i, j , we conclude that the transcendence degree of the field generated by

$$\varphi_1(\gamma_1), \dots, \varphi_r(\gamma_1); \dots; \varphi_1(\gamma_n), \dots, \varphi_r(\gamma_n)$$

is $\geq nr - d$, where d is the transcendence degree of K over \mathbb{Q} . Since according to (2) the elements $\varphi_i(\gamma_j)$ are contained in $\mathcal{P}(\gamma_1, \dots, \gamma_n)$, we obtain that

$$nr - d \leq n(r - 1) + r^2,$$

which yields a contradiction if $n > d + r^2$. □

Remark 1. If $\text{rk}_{\mathbb{R}}G = 1$, then one has unconditional affirmative answer to Benoist’s question. In fact, using Corollary 1 (with $L_0 = K$), one can find regular \mathbb{R} -regular elements $\gamma_1, \gamma_2 \in \Gamma$ with the properties required to be able to apply Corollary 2. Since γ_1 and γ_2 are \mathbb{R} -regular, the elements $\ell(\gamma_1), \ell(\gamma_2) \in \mathfrak{a} \simeq \mathbb{R}$ are nontrivial. Furthermore, $\ell(\gamma_i) = \log \chi_i(\gamma_i)$ for some positive characters $\chi_i \in X(T_i)$, and Corollary 2 implies that $\ell(\gamma_1)$ and $\ell(\gamma_2)$ are noncommensurable, hence they generate a dense subgroup of \mathfrak{a} .

Lengths of closed geodesics in locally symmetric spaces. Let T be a maximal \mathbb{R} -torus of G , T_s the maximal \mathbb{R} -split subtorus of T and \mathcal{C} be the maximal compact subgroup of $T(\mathbb{R})$. Then $T(\mathbb{R})$ is a direct product of \mathcal{C} and $T_s(\mathbb{R})^\circ$. As before, let \mathcal{K} be a maximal compact subgroup of $\mathcal{G} = G(\mathbb{R})$ and \mathfrak{p} be the orthogonal complement of the Lie subalgebra \mathfrak{k} of \mathcal{K} in the Lie algebra

\mathfrak{g} of \mathcal{G} under the Killing form. We fix a $z \in \mathcal{G}$ such that $z\mathcal{C}z^{-1} \subset \mathcal{K}$ and $zT_s(\mathbb{R})^\circ z^{-1} \subset \exp \mathfrak{p}$. Let $\mathfrak{X} = \mathcal{K} \backslash \mathcal{G}$ be the symmetric space of \mathcal{G} with the Riemannian metric given by the restriction of the Killing form to \mathfrak{p} . Let Γ be a discrete torsion-free Zariski-dense subgroup of \mathcal{G} . Then \mathfrak{X}/Γ is a Riemannian locally symmetric space.

Let $x = x_e \cdot x_h$, with $x_e \in \mathcal{C}$ and $x_h = \exp \text{Ad } z^{-1}(X) \in T_s(\mathbb{R})^\circ$, $X \in \mathfrak{p}$. Then for any character χ of T , $|\chi(x)| = |\chi(x_h)| = \exp d\chi(\text{Ad } z^{-1}(X))$, where $d\chi$ is the derivative of χ . The curve $t \mapsto \mathcal{K} \exp(tX)z$, $t \in \mathbb{R}$, is a geodesic on \mathfrak{X} which passes through the point $\mathcal{K}z$ and $\mathcal{K} \exp(tX)z \cdot x = \mathcal{K} \exp((t+1)X)z$. Therefore, if $x \in \Gamma$, then the image of this geodesic is a closed (in fact a periodic) geodesic in \mathfrak{X}/Γ of length $\lambda(x) = \langle X, X \rangle^{1/2}$. Observe that

$$\langle X, X \rangle = \langle \text{Ad } z^{-1}(X), \text{Ad } z^{-1}(X) \rangle = \sum (\log |\alpha(x)|)^2 = \sum \frac{1}{4} (\log |\alpha(x)|^2)^2,$$

where the summations are over the set of roots of \mathfrak{g} with respect to T .

Let T_1 and T_2 be two maximal \mathbb{R} -tori in G , and let $\gamma_i \in T_i(\mathbb{R}) \cap \Gamma$, $i = 1, 2$. As explained above, these elements determine closed geodesics in \mathfrak{X}/Γ . The lengths $\lambda(\gamma_1)$ and $\lambda(\gamma_2)$ of these closed geodesics are given by

$$(3) \quad \lambda(\gamma_1)^2 = \sum_{i=1}^p s_i^{(1)} (\log \chi_i^{(1)}(\gamma_1))^2, \quad \lambda(\gamma_2)^2 = \sum_{i=1}^p s_i^{(2)} (\log \chi_i^{(2)}(\gamma_2))^2,$$

where $\chi_1^{(i)}, \dots, \chi_p^{(i)}$ are certain positive characters of T_i , and the $s_i^{(j)}$'s are positive rational numbers.

In the following proposition and the theorem, we assume that G is defined over a real number field K , Γ is a discrete torsion-free Zariski-dense subgroup of $G(\mathbb{R})$ contained in $G(K)$, γ_1 and γ_2 are two regular \mathbb{R} -regular elements of Γ with the properties mentioned in Corollary 2; such elements exist by Corollary 1. For $i = 1, 2$, let $T_i = Z_G(\gamma_i)$; T_i is a maximal K -torus which contains a maximal \mathbb{R} -split torus of G .

If $\text{rk}_{\mathbb{R}} G = 1$, the subgroups of positive characters in $X(T_1)$ and $X(T_2)$ are cyclic (as every positive character is defined over \mathbb{R}); let $\chi^{(1)}$ and $\chi^{(2)}$ be their generators such that $\chi^{(i)}(\gamma_i) > 1$. Then it is obvious from the above that $\lambda(\gamma_1) = s \log \chi^{(1)}(\gamma_1)$ and $\lambda(\gamma_2) = s \log \chi^{(2)}(\gamma_2)$, where s is the positive square-root of a positive rational number. From Proposition 2 we now immediately obtain (see also Remark 1):

Proposition 3. *If $\text{rk}_{\mathbb{R}} G = 1$, then the ratio $\lambda(\gamma_1)/\lambda(\gamma_2)$ is a transcendental number.*

Assuming the truth of Schanuel’s conjecture, one can prove a stronger assertion for groups of arbitrary real rank.

Theorem 4. *If Schanuel’s conjecture holds, then $\lambda(\gamma_1)$ and $\lambda(\gamma_2)$ are algebraically independent over \mathbb{Q} .*

Proof. We notice that if z_1, \dots, z_n are algebraic numbers, then Schanuel’s conjecture applied to

$$\alpha_1 = \log z_1, \dots, \alpha_n = \log z_n$$

yields algebraic independence of $\alpha_1, \dots, \alpha_n$ once these elements are linearly independent (over \mathbb{Q}). After renumbering the characters appearing in (3), we can assume that

$$a_1 := \log \chi_1^{(1)}(\gamma_1), \dots, a_{m_1} := \log \chi_{m_1}^{(1)}(\gamma_1)$$

$$(\text{resp.}, b_1 := \log \chi_1^{(2)}(\gamma_2), \dots, b_{m_2} := \log \chi_{m_2}^{(2)}(\gamma_2)),$$

for some $m_1, m_2 \leq p$, form a basis of the \mathbb{Q} -subspace of \mathbb{R} spanned by $\log \chi_i^{(1)}(\gamma_1)$ (resp., $\log \chi_i^{(2)}(\gamma_2)$) for $i \leq p$. It immediately follows from Proposition 1 that the numbers

$$a_1, \dots, a_{m_1}; b_1, \dots, b_{m_2}$$

are linearly independent over \mathbb{Q} , hence algebraically independent by Schanuel’s conjecture. On the other hand, according to (3), $\lambda(\gamma_1)^2$ (resp., $\lambda(\gamma_2)^2$) are given by nonzero homogeneous polynomials of degree two (with rational coefficients) in a_1, \dots, a_{m_1} (resp., b_1, \dots, b_{m_2}), and our assertion follows. \square

Remark 2. Let G be a connected semisimple algebraic group defined over \mathbb{R} such that $G(\mathbb{R})$ does not contain any nontrivial connected compact normal subgroups. If Γ is an infinitesimally rigid discrete subgroup of $G(\mathbb{R})$, for example, if $G(\mathbb{R})$ is not locally isomorphic to either $\text{SL}_2(\mathbb{R})$ or $\text{SL}_2(\mathbb{C})$ and Γ is an irreducible lattice in $G(\mathbb{R})$, or $G(\mathbb{R})$ is locally isomorphic to $\text{SL}_2(\mathbb{C})$ and Γ is a cocompact lattice in $G(\mathbb{R})$, then there is a real number field K such that G is defined over K and $\Gamma \subset G(K)$, see [9], Proposition 6.6.

Remark 3. Assuming that Schanuel’s conjecture holds, we can prove the following variant of Theorem 4: *Let K be a finitely generated subfield of \mathbb{R} of transcendence degree d over \mathbb{Q} . Let G be a connected semisimple algebraic group defined over K , and Γ be a discrete torsion-free Zariski-dense subgroup of $G(\mathbb{R})$ contained in $G(K)$. Let s be a positive integer and $n > d + s$ be an integer. Let $\gamma_1, \dots, \gamma_n \in \Gamma$ be regular \mathbb{R} -regular elements with the properties described in Corollary 1 for $L_0 = K$. Then there exists an $i \leq n$ such that $\lambda(\gamma_i)$ is transcendental over the field $\mathbb{Q}(\lambda(\gamma_1), \dots, \lambda(\gamma_s))$. Indeed, as in (3), for each $i \leq n$, $\lambda(\gamma_i)$ is given by an expression of the form*

$$\lambda(\gamma_i)^2 = \sum_{k=1}^p s_k^{(i)} (\log \chi_k^{(i)}(\gamma_i))^2,$$

where $\chi_1^{(i)}, \dots, \chi_p^{(i)}$ are certain positive characters of the K -torus $T_i := Z_G(\gamma_i)^\circ$, and the $s_k^{(i)}$ are positive real numbers. After renumbering the characters, we can assume that

$$a_1^{(i)} := \log \chi_1^{(i)}(\gamma_i), \dots, a_{m_i}^{(i)} := \log \chi_{m_i}^{(i)}(\gamma_i),$$

for some $m_i \leq p$ form a basis of the \mathbb{Q} -subspace of \mathbb{R} spanned by $\log \chi_k^{(i)}(\gamma_i)$ for $k \leq p$. Then $\lambda(\gamma_i)^2$ is represented by a nonzero homogeneous polynomial of degree two in terms of $a_1^{(i)}, \dots, a_{m_i}^{(i)}$. Set $A^{(i)} = \{a_1^{(i)}, \dots, a_{m_i}^{(i)}\}$.

It follows from Proposition 1 that the set

$$A = A^{(1)} \cup \dots \cup A^{(n)}$$

is linearly independent over \mathbb{Q} , so by Schanuel's conjecture the transcendence degree over \mathbb{Q} of the field generated by

$$A \cup \{e^a \mid a \in A\}$$

is at least $\#A$. But for $a \in A$, e^a is the value of a character on some element of $G(K)$, so e^a is algebraic over K . We conclude that the transcendence degree over \mathbb{Q} of the field generated by $\{e^a \mid a \in A\}$ is at most d . Therefore, the transcendence degree over \mathbb{Q} of the field L generated by A is at least $\#A - d$. On the other hand, if for all $i \leq n$, $\lambda(\gamma_i)$ is algebraic over $\mathbb{Q}(\lambda(\gamma_1), \dots, \lambda(\gamma_s))$, then, as can be seen easily, the transcendence degree of L over \mathbb{Q} is at most $\sum m_i - (n - s) = \#A - (n - s)$, which would imply that $d + s \geq n$, contradicting the hypothesis that $n > d + s$.

Acknowledgements

We would like to acknowledge partial support from the NSF grants DMS-0100429 and DMS-0138315 and from the BSF grant # 2000171. We thank T.J. Hitchman and Ralf Spatzier for their question. Special thanks are due to Damien Roy for providing an argument that subsequently evolved into the proof of Theorem 3. We also thank Mike Bennett, David Masser and Michel Waldschmidt for correspondence on algebraic independence of logarithms of algebraic numbers and Jean-Pierre Serre for his suggestion to improve the exposition.

References

- [1] J. Ax, *On Schanuel's conjecture*, Ann. of Math. **93** (1971), 252–268.
- [2] A. Baker, *Transcendental Number Theory. Second Edition*. Cambridge Mathematical Library. Cambridge Univ. Press, 1990.
- [3] Y. Benoist, *Propriétés asymptotiques des groupes linéaires (II)*, Analysis on homogeneous spaces and representation theory of Lie groups, Okayama–Kyoto (1997), 33–48, Adv. Stud. Pure Math., **26**, Math. Soc. Japan, Tokyo, 2000.
- [4] A. Borel, *Linear Algebraic Groups. Second Edition*, GTM 126, Springer-Verlag, New York, 1991.
- [5] G. Prasad, M.S. Raghunathan, *Cartan subgroups and lattices in semi-simple groups*, Ann. of Math. **96** (1972), 296–317.
- [6] G. Prasad, A.S. Rapinchuk, *Irreducible tori in semisimple groups*, Intern. Math. Res. Notices **23** (2001), 1229–1242; Erratum, *ibid* **17** (2002), 919–921.
- [7] ———, *Subnormal subgroups of the groups of rational points of reductive algebraic groups*, Proc. Amer. Math. Soc. **130** (2002), 2219–2227.
- [8] ———, *Existence of irreducible \mathbb{R} -regular elements in Zariski-dense subgroups*, Math. Res. Letters **10** (2003), 21–32.
- [9] M.S. Raghunathan, *Discrete subgroups of Lie groups*, Springer-Verlag, 1972.

- [10] M. Waldschmidt, *Transcendance et exponentielles en plusieurs variables*, Invent. Math. **63** (1981), 97–127.

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

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VIRGINIA, CHARLOTTESVILLE, VA 22904
E-mail address: asr3x@virginia.edu