J. reine angew. Math. **629** (2009), 201—220
DOI 10.1515/CRELLE.2009.031

Journal für die reine und
angewandte Mathematik

On the power maps, orders and exponentiality of p-adic algebraic groups

By *Pralay Chatterjee* at Chennai

Abstract. In this paper we study the question of surjectivity of the power maps $g \mapsto g^n$ on p-adic algebraic groups. We give a complete solution of this question in terms of the orders of certain compact analytic subgroups. We next study the p-adic one parameter subgroups of p-adic algebraic groups and find conditions, when the union of all such one parameter groups fills up the entire group. We show that there is a close relation between the above two problems. We also obtain similar results on groups defined over rational numbers.

1. Introduction and statements of the main results

Let $\mathbb{K}$ denote either $\mathbb{Q}_p$ or $\mathbb{R}$. Let G be an analytic group over $\mathbb{K}$. A *one parameter group* ϕ in G is the image of a continuous (hence analytic) group homomorphism $\phi : \mathbb{K} \to G$. The union of all such one parameter groups in G is denoted by $E_{\mathbb{K}}(G)$. Note that if $\mathbb{K} = \mathbb{R}$ then $E_{\mathbb{R}}(G) = \exp\big(L(G)\big)$, where $L(G)$ is the Lie algebra of G and $\exp : L(G) \to G$ is the usual exponential map. In view of this, an analytic group G over $\mathbb{K}$ is said to be *exponential* if $G = E_{\mathbb{K}}(G)$. Let P_n denote the n-th power map defined by $P_n(g) = g^n$ for $g \in G$. It is well known, through the work of M. McCrudden, that a real Lie group is exponential if and only if all the n-th power maps are surjective; for more details the reader is referred to the paper by McCrudden [M] and Section 5 of this article, especially to Theorem 5.2. A considerable amount of work has been done on the so called "exponentiality problem" on real groups, the main theme of which is finding a criterion to decide which real Lie groups are exponential; see [Dj-H] for a survey. We also recall that many real Lie groups fail to be exponential. Thus in view of McCrudden's work it is now natural to ask for a characterization of real Lie groups for which an individual n-th power map is surjective. On the other hand an answer to this question on the power maps on real Lie groups will have immediate implications on the exponentiality problem of such groups.

To put the present work in proper perspective we briefly mention the work that has been done on the n-th power maps and its ramifications to the exponentiality problem. In [Ch1] we have given a necessary and sufficient condition for the surjectivity of the n-th power maps for connected solvable real Lie groups in terms of Cartan subgroups. The theorem has many applications which includes strengthening of Dixmier's characterization of

solvable simply connected real Lie groups which are exponential. In [Ch2] we have given a characterization for the surjectivity of the n-th power maps for general connected algebraic groups over algebraically closed fields of characteristic zero in terms of a maximal torus and its weights, which in turn yields a solution of the exponentiality problem, for this class of groups. As another application we have explicitly determined, for all simple algebraic groups over algebraically closed fields of characteristic zero, the set of integers n for which the n-th power map is surjective. In [Ch3] the author and in [St] R. Steinberg independently extended some of the results of [Ch2] which leads to a complete classification of exponents n for which P_n is surjective for semisimple groups over algebraically closed fields of arbitrary characteristic. More recently, in [Ch4] we have studied n-th power maps of the real points of algebraic groups defined over $\mathbb{R}$ and in [Ch5] we have obtained results for groups, which are not necessarily (Zariski) connected.

Although a criterion to decide which real Lie groups are exponential or which real Lie groups admit surjective n-th power map, is still not available, a lot of work has been done in this direction. But there is hardly any literature on the analogous questions on p-adic analytic groups. In this paper we contribute to the questions regarding P_n, exponentiality and the relation between them, on general p-adic algebraic groups, proving a characterization of surjectivity of P_n and exponentiality on such groups (see Theorems 1.2, 1.4, 1.5 and Corollary 1.7). See also Theorem 1.1, Corollaries 1.3, 1.6 and Section 6 for other results.

We now describe the main results of this paper.

An algebraic group G over a field $\mathbb{K}$ (not necessarily algebraically closed field) is said to be $\mathbb{K}$-*isotropic* if it contains a $\mathbb{K}$-split torus of positive dimension (see [B]); otherwise G is called $\mathbb{K}$-*anisotropic*. If G is defined over $\mathbb{K}$ then the subgroup of $\mathbb{K}$-rational points is denoted by $G(\mathbb{K})$. The following theorem is our first main result and it deals with $\mathbb{Q}_p$-isotropic algebraic groups. The technique of our proof is inspired by M. Ratner's proof of Theorem 5.1 (see [R1], Theorem 1.1, and [R2], Theorem 3.3), which was proved originally by A. Lubotzky and G. Prasad.

Theorem 1.1. *Let G be an algebraic group defined over $\mathbb{Q}_p$. If G is $\mathbb{Q}_p$-isotropic then for any $n \neq 1$ the map $P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is not surjective.*

The next theorem is a characterization result on the surjectivity of P_n. We need the notion of the order $\mathrm{Ord}\big(H(\mathbb{Q}_p)\big)$ associated to an $\mathbb{Q}_p$-anisotropic reductive group H; the reader is referred to Section 2.

Theorem 1.2. *Let G be an algebraic group over $\mathbb{Q}_p$ and $R_u(G)$ be the unipotent radical of G. Let $n \neq 1$ be an integer. Then the following are equivalent*:

(1) *$P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective.*

(2) *$P_n : G/R_u(G)(\mathbb{Q}_p) \to G/R_u(G)(\mathbb{Q}_p)$ is surjective.*

(3) *$G/R_u(G)$ is $\mathbb{Q}_p$-anisotropic (hence $G/R_u(G)(\mathbb{Q}_p)$ is compact) and n is coprime to* $\mathrm{Ord}\big(G/R_u(G)(\mathbb{Q}_p)\big)$.

Consequently, $P_p : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective if and only if $G/R_u(G)(\mathbb{Q}_p)$ is a finite group and $\mathrm{Ord}\big(G/R_u(G)(\mathbb{Q}_p)\big)$ *is coprime to p.*

The above theorem says that if an algebraic group over $\mathbb{Q}_p$ admits a $\mathbb{Q}_p$-anisotropic Levi subgroup then the $\mathbb{Q}_p$-anisotropic Levi subgroup decides which n-th power maps are surjective for the entire group of $\mathbb{Q}_p$-rational points. Thus the question of surjectivity of n-th power maps for the group of $\mathbb{Q}_p$-rational points of a general connected algebraic group over $\mathbb{Q}_p$ reduces to looking at the same question for groups that are $\mathbb{Q}_p$-anisotropic and reductive. In other words the unipotent radical of a $\mathbb{Q}_p$-algebraic group does not play any role. It may be noted that when the underlying groups are $\mathbb{R}$-points of groups defined over $\mathbb{R}$ or algebraic groups over algebraically closed fields of characteristic zero then the unipotent radical does play an important role in deciding which n-th power maps are surjective, exhibiting a striking difference from the p-adic case (see [Ch2], [Ch4]).

As above, the following corollary again shows a surprising difference with the analogous situation in the case of algebraic groups defined over $\mathbb{R}$ or algebraic groups over algebraically closed fields of characteristic zero (compare with the results of [Ch2], [Ch4]).

Corollary 1.3. *Let G be an algebraic group over $\mathbb{Q}_p$. Let H be an algebraic subgroup over $\mathbb{Q}_p$. Let n be an integer. Suppose that $P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective. Then $P_n : H(\mathbb{Q}_p) \to H(\mathbb{Q}_p)$ is surjective.*

In view of Theorem 1.2 we see that the question of surjectivity of P_n on the groups of $\mathbb{Q}_p$-rational points of algebraic groups over $\mathbb{Q}_p$ finally boils down to finding out the orders of groups of $\mathbb{Q}_p$-rational points of $\mathbb{Q}_p$-anisotropic reductive groups. We use the well known classification of absolutely simple simply connected groups over non-archimedean local fields of characteristic zero to obtain results on the orders of $\mathbb{Q}_p$-rational points of $\mathbb{Q}_p$-anisotropic semisimple groups; see Propositions 4.4, 4.6 and Corollary 4.7. We associate integers $M(G)$ and $N(G)$ to a $\mathbb{Q}_p$-anisotropic semisimple group G using certain data arising in the classification of such groups in terms of central division algebras; see Definition 4.11. In addition if G is simply connected, then it may be noted that prime divisors of the integer $M(G)$ and the super natural number $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$ are the same. The following theorem may be regarded as a companion of Theorem 1.2. The first part of the following result completes our understanding of the surjectivity of n-th power map for the class of p-adic algebraic groups which admit simply connected semisimple Levi subgroups.

Theorem 1.4. *Let G be a connected algebraic group over $\mathbb{Q}_p$. Let $n \neq 1$ be an integer. Then we have the following*:

(1) *If $G/R_u(G)$ is semisimple simply connected then $P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective if and only if $G/R_u(G)$ is $\mathbb{Q}_p$-anisotropic and n is coprime to $M\big(G/R_u(G)\big)$.*

(2) *If $G/R_u(G)$ is semisimple (not necessarily simply connected) and $\mathbb{Q}_p$-anisotropic then $P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective if n is coprime to $N\big(G/R_u(G)\big)$.*

See Example 4.12 for an illustration on the computation of $M(G)$.

Our final results are on the question of exponentiality for p-adic algebraic groups. The result of Lubotzky and Prasad (see Theorem 5.1), which inspired the proof of Theorem 1.1, implies that if G is an algebraic group over $\mathbb{Q}_p$ then $G(\mathbb{Q}_p)$ is exponential if and only if G is unipotent. In the case of a real Lie group G, M. McCrudden proved that $E_{\mathbb{R}}(G) = \bigcap_{n=2}^{\infty} P_n(G)$ (see [M] and Theorem 5.2) which in turn implies that G is exponential if

and only if $P_n : G \to G$ is surjective for all n. The following theorem can be thought of as a generalization, of the above result on p-adic algebraic groups due to Lubotzky and Prasad. On the other hand it also can be thought of as a p-adic analogue of the latter result of McCrudden. If G is an algebraic group, we denote the variety of unipotent elements of G by $\mathscr{U}_G$.

Theorem 1.5. *Let G be an algebraic group over $\mathbb{Q}_p$. Let $\alpha \in G(\mathbb{Q}_p)$ be a semisimple element with $\alpha \in \bigcap_{n=1}^{\infty} P_{p^n}\big(G(\mathbb{Q}_p)\big)$. Then the cyclic group generated by α is finite and $\mathrm{Ord}(\alpha)$ is coprime to p. Further, we have the following equality of sets*:

$$E_{\mathbb{Q}_p}\big(G(\mathbb{Q}_p)\big) = \bigcap_{n=2}^{\infty} P_n\big(G(\mathbb{Q}_p)\big) = \mathscr{U}_G(\mathbb{Q}_p).$$

We have the following corollary which is a strengthening of Theorem 5.1 due to Lubotzky and Prasad.

Corollary 1.6. *Let G be an algebraic group over $\mathbb{Q}_p$. Let $\phi : \mathbb{Q} \to G(\mathbb{Q}_p)$ be an abstract homomorphism. Then there is a nilpotent element X in $L(G)(\mathbb{Q}_p)$ such that $\phi(t) = \exp(tX)$ for all $t \in \mathbb{Q}$.*

As a consequence of Theorem 1.2 and Theorem 1.5 we can draw the following corollary.

Corollary 1.7. *Let G be a Zariski connected algebraic group over $\mathbb{Q}_p$. Then the following are equivalent*:

(1) *$P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective for all n.*

(2) *$P_p : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective.*

(3) *G is unipotent.*

(4) *$G(\mathbb{Q}_p)$ is exponential.*

The paper is organised as follows. In the following section we fix some standard notations and recall some preliminaries. In Section 3 we prove Theorems 1.1, 1.2 and Corollary 1.3. Section 4 deals with the detailed analysis of the order of anisotropic p-adic algebraic groups and Theorem 1.4 is proved. In Section 5 we prove Theorem 1.5, Corollary 1.6 and Corollary 1.7. In the final Section 6 we draw similar conclusions on groups defined over rational numbers. We also make few remarks and pose a question in this section.

2. Notations and preliminaries

In this section we fix some notations and recall some known results. For basic results on the theory of algebraic groups we refer to [B], [B-T] and [P-R]. Let $\mathbb{K}$ be a perfect field, not necessarily algebraically closed. We denote by $\overline{\mathbb{K}}$ the algebraic closure of $\mathbb{K}$. Let G be an algebraic group defined over $\mathbb{K}$. The center and the unipotent radical of an algebraic group

G will be denoted by $Z(G)$ and $R_u(G)$ respectively. We denote the group of $\mathbb{K}$-rational points of G by $G(\mathbb{K})$. If $g \in G(\mathbb{K})$ and if $g = g_s g_u$ is the Jordan decomposition of g then $g_s, g_u \in G(\mathbb{K})$. A non-abelian connected algebraic group defined over a field $\mathbb{K}$ is said to be *absolutely simple* (resp. $\mathbb{K}$-*simple*) if it does not admit any Zariski closed normal connected subgroup of positive dimension (resp. defined over $\mathbb{K}$). It is well known that if G is a reductive group defined over a local field $\mathbb{K}$ then G is $\mathbb{K}$-anisotropic if and only if the group $G(\mathbb{K})$ is compact in the topology induced by the topology on $\mathbb{K}$. If G is an algebraic group defined over $\mathbb{Q}_p$ then $G(\mathbb{Q}_p)$ is an analytic p-adic group.

We need certain notions related to central division algebras over local fields. Let D be a finite dimensional central division algebra over a local field $\mathbb{F}$. Note that $\dim_{\mathbb{F}} D$ is always the square of an integer. This integer is called the *degree* of D over $\mathbb{F}$. Let $\mathrm{Nrd}_{D/\mathbb{F}} : D \to \mathbb{F}$ be the usual reduced norm of D (see [P-R], Section 1.4, page 27). We define the subgroup $\mathrm{SL}_1(D)$ of the multiplicative group D^* by $\mathrm{SL}_1(D) = \{x : \mathrm{Nrd}_{D/\mathbb{F}}(x) = 1\}$. Let $\mathbf{SL}_1(D)$ denote the algebraic group over $\mathbb{F}$ such that $\mathbf{SL}_1(D)(\mathbb{F}) = \mathrm{SL}_1(D)$.

We also need some facts associated to profinite groups. See [R-Z], [S] and [W] for details. A topological group G is called *profinite* if it is compact and totally disconnected. Such a group is topologically isomorphic to a projective limit of finite groups. A *supernatural number* is a formal infinite product $\prod p^{n(p)}$, over all primes p, where $n(p)$ is a non-negative integer or infinity. Product, divisibility, l.c.m and g.c.d of a set (possibly infinite) of supernatural numbers are defined in the natural way. In particular, l.c.m of an infinite set of integers is a supernatural number. If G is a finite group its order is denoted by $\mathrm{Ord}(G)$. We now define the order, $\mathrm{Ord}(G)$ of a profinite group G by,

$$\mathrm{Ord}(G) = \text{l.c.m}\{\mathrm{Ord}(G/U) : U \text{ is an open subgroup of } G\}.$$

It can be easily seen that in the above definition of order, the term 'open subgroup' can be replaced by 'open normal subgroup'. Note that if G is a profinite group then $\mathrm{Ord}(G)$ is a supernatural number. Let $x \in G$ and let $\langle x \rangle$ denote the subgroup generated by x. First note that the closure of the group generated by x is again a profinite group in its own right. Then we define $\mathrm{Ord}(x)$ to be the order of the profinite group $\overline{\langle x \rangle}$. Lagrange's theorem holds for profinite groups (see [W], Proposition 2.1.2) i.e. if H is a closed subgroup of G then $\mathrm{Ord}(H)$ divides $\mathrm{Ord}(G)$. In particular, if $x \in G$ then $\mathrm{Ord}(x)$ divides $\mathrm{Ord}(G)$. A profinite group is said to be *finitely generated* if there is a finite set $A \subset G$ such that the topological closure of the group generated by A is all of G. Let p be a prime number. A profinite group G is called a *pro-p group* if p is the only prime which divides $\mathrm{Ord}(G)$. If G is a compact p-adic analytic group then it is a profinite group and in this case G admits an open maximal pro-p subgroup. Hence $\mathrm{Ord}(G) = mp^{n(p)}$ where $m \in \mathbb{N}$, g.c.d$(m, p) = 1$ and $n(p) \in \mathbb{N} \cup \{\infty\}$ (see [S], Section 1.4). Note that if G is an $\mathbb{Q}_p$-anisotropic reductive algebraic group then $G(\mathbb{Q}_p)$ is a profinite group and hence we can talk of $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$.

3. Surjectivity of *n*-th power maps and orders of anisotropic groups

In this section we prove Theorems 1.1, 1.2, 1.4 and Corollary 1.3.

Proof of Theorem 1.1. We first fix a positive integer m and consider the general linear group $\mathrm{GL}_m(\overline{\mathbb{Q}}_p)$, where $\overline{\mathbb{Q}}_p$ denotes an algebraic closure of $\mathbb{Q}_p$. Let D be the closed

subgroup of $\mathrm{GL}_m(\overline{\mathbb{Q}}_p)$ consisting of diagonal matrices, and B be the closed subgroup of $\mathrm{GL}_m(\overline{\mathbb{Q}}_p)$ consisting of upper-triangular matrices. We equip $\mathrm{GL}_m(\overline{\mathbb{Q}}_p)$, B and D with the usual $\mathbb{Q}_p$-structure so that they become algebraic groups defined over $\mathbb{Q}_p$. For every $1 \leqq i \leqq m$ we define the character (over $\mathbb{Q}_p$) $\mu_i : B \to \overline{\mathbb{Q}}_p^*$ by

$$\mu_i \begin{pmatrix} x_1 & & & & \\ & \ddots & & * & \\ & & x_i & & \\ & 0 & & \ddots & \\ & & & & x_m \end{pmatrix} = x_i.$$

Let $\| \cdot \|_{\mathbb{Q}_p} : \mathbb{Q}_p \to \mathbb{R}$ be the usual p-adic valuation on $\mathbb{Q}_p$. For a finite extension $\mathbb{L}$ of $\mathbb{Q}_p$, let $\| \cdot \|_{\mathbb{L}} : \mathbb{L} \to \mathbb{R}$ be the unique extension of $\| \cdot \|_{\mathbb{Q}_p}$.

Claim. Let $\alpha \in D(\mathbb{Q}_p)$ such that $\|\mu_l(\alpha)\|_{\mathbb{Q}_p} \neq 1$ for some l, $1 \leqq l \leqq m$. We claim that there is no sequence $\{g_i\}_{i \geqq 1} \subset \mathrm{GL}_m(\mathbb{Q}_p)$ with $g_1 = \alpha$ and $g_i = g_{i+1}^n$ for all $i \geqq 1$.

We will arrive at a contradiction assuming the existence of such a sequence $\{g_i\}_{i \geqq 1}$. Consider the group $\Gamma \subset \mathrm{GL}_m(\mathbb{Q}_p)$ generated by the set $\{g_i\}_{i \geqq 1}$. Clearly the group Γ is an abelian subgroup of $\mathrm{GL}_m(\mathbb{Q}_p)$. Further note that the degree of the characteristic polynomial of g for $g \in \mathrm{GL}_m(\mathbb{Q}_p)$ is m. It is well-known that the number of algebraic extensions of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$ of a given degree is finite (see [P-R], Section 6.4). Let $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$ so that for every $g \in \mathrm{GL}_m(\mathbb{Q}_p)$, all the eigen-values of g lie in $\mathbb{F}$. Since Γ is abelian we can do simultaneous upper triangulation of the matrices $\{g_i\}_{i \geqq 1}$ as elements of $\mathrm{GL}_m(\mathbb{F})$ i.e. we can choose a basis of $\mathbb{F}^m$ with respect to which the matrices of $\{g_i\}_{i \geqq 1}$ are all upper-triangular. Thus there exists $A \in \mathrm{GL}_m(\mathbb{F})$ so that $Ag_iA^{-1} \in B$ for all $i \geqq 1$. As $g_i = g_{i+1}^n$ we have $Ag_iA^{-1} = (Ag_{i+1}A^{-1})^n$ for all $i \geqq 1$. Hence

$$\|\mu_r(Ag_{i+1}A^{-1})\|_{\mathbb{F}}^n = \|\mu_r(Ag_iA^{-1})\|_{\mathbb{F}}, \quad \text{for } i \geqq 1 \text{ and } 1 \leqq r \leqq m.$$

As the valuation $\| \cdot \|_{\mathbb{F}} : \mathbb{F} \to \mathbb{R}$ is discrete we conclude that

$$\|\mu_r(Ag_iA^{-1})\|_{\mathbb{F}} = 1 \quad \text{for } i \geqq 1 \text{ and } 1 \leqq r \leqq m.$$

Hence for every $i \geqq 1$ if $y \in \mathbb{F}$ is an eigenvalue of g_i then $\|y\|_{\mathbb{F}} = 1$. In particular this holds for α. But $\mu_l(\alpha)$ is an eigenvalue of α with $\|\mu_l(\alpha)\|_{\mathbb{F}} = \|\mu_l(\alpha)\|_{\mathbb{Q}_p} \neq 1$. This is a contradiction. This completes the proof of the claim.

Now we get back to the proof of the theorem. Let G be an algebraic group over $\mathbb{Q}_p$ which is $\mathbb{Q}_p$-isotropic. We assume that for some $n \geqq 1$, the power map

$$P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$$

is surjective. We will then arrive at a contradiction. As G is $\mathbb{Q}_p$-isotropic, G has a $\mathbb{Q}_p$-torus S with $\dim S \geqq 1$, which is split over $\mathbb{Q}_p$. It is well known that there is a faithful (algebraic) representation of G into $\mathrm{GL}_m(\overline{\mathbb{Q}}_p)$, defined over $\mathbb{Q}_p$, for some integer m. We identify G with its image in $\mathrm{GL}_m(\overline{\mathbb{Q}}_p)$. Note that as D is a maximal $\mathbb{Q}_p$-split torus of $\mathrm{GL}_m(\overline{\mathbb{Q}}_p)$ we can get

$\beta \in \mathrm{GL}_m(\mathbb{Q}_p)$ so that $\beta S\beta^{-1} \subset D$. As $\dim S \geqq 1$ there exists $\gamma \in S(\mathbb{Q}_p)$ and a character $\mu_l : B \to \overline{\mathbb{Q}}_p^*$ so that $\|\mu_l(\beta\gamma\beta^{-1})\|_{\mathbb{Q}_p} \neq 1$. Now as $P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective there is a sequence $\{\gamma_i\}_{i\geqq 1} \subset G(\mathbb{Q}_p)$ with $\gamma_1 = \gamma$ and $\gamma_i = \gamma_{i+1}^n$ for all $i \geqq 1$. Set $g_i = \beta\gamma_i\beta^{-1}$. Then $\{g_i\}_{i\geqq 1}$ is a sequence in $\mathrm{GL}_m(\mathbb{Q}_p)$ as in the above claim. This is a contradiction. This completes the proof of the theorem. □

Our next goal is to deal with the surjectivity questions of n-th power maps of groups which are $\mathbb{Q}_p$-rational points of an anisotropic algebraic group defined over $\mathbb{Q}_p$. Such groups turn out to be profinite groups. This directs us to first consider the surjectivity questions of n-th power maps of profinite groups.

We need the following well known result in the proof of the next lemma.

Theorem 3.1 ([R-Z], Proposition 2.5.1). *Let G be a finitely generated profinite group. Then the identity element of G admits a countable base consisting of a decreasing sequence of open normal subgroups.*

The following lemma is not difficult to prove (see [S]). For the sake of completeness we include a proof here.

Lemma 3.2. *Let G be a profinite group. Then $P_n : G \to G$ is surjective if and only if n is coprime to* $\mathrm{Ord}(G)$. *In particular, if $x \in G$ then $P_n : \overline{\langle x\rangle} \to \overline{\langle x\rangle}$ is surjective if and only if n is coprime to* $\mathrm{Ord}(x)$.

Proof. We will prove the first part of the lemma. The second part follows immediately from the first part.

Let us first assume that n is coprime to $\mathrm{Ord}(G)$. We will show that $P_n : G \to G$ is surjective. Since every element of G lies in a finitely generated closed subgroup, it is enough to show that $P_n : H \to H$ is surjective, where H is a finitely generated closed subgroup of G. Note that, by Lagrange's theorem, n is coprime to $\mathrm{Ord}(H)$. As H is finitely generated, by Theorem 3.1 it follows that H will admit a base $\{U_i\}_{i=1}^{\infty}$ at the identity $e \in H$ where U_i is open normal subgroup of H and $U_{i+1} \subset U_i$, for all $i \geqq 1$. Further note that H is topologically isomorphic to $\varprojlim H/U_i$ and

$$\mathrm{Ord}(H) = \mathrm{l.c.m}\{\mathrm{Ord}(H/U_i) : i \geqq 1\}.$$

Note that since H is compact and U_i is open normal in H, $\mathrm{Ord}(H/U_i)$ is finite. For simplicity we write $H_i = H/U_i$, for all i. We have the natural map $\phi_{i+1} : H_{i+1} \to H_i$ for all i. Let $(\alpha_i) \in \varprojlim H_i \subset \prod H_i$. We will prove the existence of an n-th root of (α_i) using the compactness of H. As n is coprime to $\mathrm{Ord}(H)$ it follows that n is coprime to $\mathrm{Ord}(H_i)$ for all $i \geqq 1$. Hence $P_n : H_i \to H_i$ is surjective for all i. For each natural number k we define a subset S_k of $\varprojlim H_i$ in the following way:

$$S_k = \{(x_i) \in \varprojlim H_i : \alpha_1 = x_1^n, \ldots, \alpha_k = x_k^n\}.$$

It is easy to see that $S_k \subset \varprojlim H_i$ is a closed set for every k. First, we will show that $S_k \neq \emptyset$ for all k. We are going to exhibit an element $(y_i) \in S_k$ inductively; more precisely, we first define the $(k+l)$-th coordinate y_{k+l} inductively for all $l \geqq 0$. As n is coprime to $\mathrm{Ord}(H_k)$ it

will remain coprime to $\mathrm{Ord}(\phi_{k+1}(H_{k+1}))$. So $P_n : \phi_{k+1}(H_{k+1}) \to \phi_{k+1}(H_{k+1})$ is surjective. Note that as $(\alpha_i) \in \varprojlim H_i$ we have $\alpha_k \in \phi_{k+1}(H_{k+1})$. Choose $y_k \in \phi_{k+1}(H_{k+1})$ so that $\alpha_k = y_k^n$. Suppose we have chosen $y_{k+l} \in H_{k+l}$. We now choose $y_{k+l+1} \in \phi_{k+l+1}^{-1}(y_{k+l})$. We need to define elements y_i for $1 \leqq i \leqq k-1$. Define $y_{k-1} = \phi_k(y_k), \ldots, y_1 = \phi_2(y_2)$. It is immediate that $(y_i) \in S_k$. Thus $S_k \neq \emptyset$ for all k. It is clear that $S_{k+1} \subset S_k$ for all k. So intersection of any finite collection of such (closed) sets is nonempty. As $\varprojlim H_i$ is compact we conclude that $\bigcap_{k \geqq 1} S_k \neq \emptyset$. It is easy to see that any element of $\bigcap_{k \geqq 1} S_k$ is an n-th root of (α_i).

We now show the converse. Suppose $P_n : G \to G$ is surjective. Then

$$P_n : G/U \to G/U$$

is surjective for all open normal subgroups U of G. Hence n is coprime to the integer $\mathrm{Ord}(G/U)$ for all such U. As

$$\mathrm{Ord}(G) = \mathrm{l.c.m}\{\mathrm{Ord}(G/U) : U \text{ is an open normal subgroup of } G\},$$

we conclude that n is coprime to $\mathrm{Ord}(G)$. □

It is well known that for a compact connected real Lie group G the exponential map from the Lie algebra to G is surjective and consequently $P_n : G \to G$ is surjective for all n. Using certain results of [Ch5] one can further deduce that if G is a compact real Lie group, not necessarily connected, then $P_n : G \to G$ is surjective if and only if n is coprime to the order $\mathrm{Ord}(G/G^0)$ of the finite group, G/G^0, where G^0 is the connected component of the identity. Since compact p-adic groups are totally disconnected, the following theorem may be regarded as a p-adic analogue of the above result.

Theorem 3.3. *Let G be a compact p-adic analytic group over $\mathbb{Q}_p$. Then the following holds*:

(1) *$P_n : G \to G$ is surjective if and only if n is coprime to* $\mathrm{Ord}(G)$.

(2) *$P_q : G \to G$ is surjective for all but finitely many primes q.*

(3) *If G is not a finite group then $P_p : G \to G$ is not surjective.*

Proof. Since G is a compact p-adic analytic group, it is a profinite group. The first statement follows from Lemma 3.2. The second statement follows from the first statement and the fact that if G is a compact p-adic analytic group then $\mathrm{Ord}(G) = mp^{n(p)}$ where $m \in \mathbb{N}$ and $n(p) \in \mathbb{N} \cup \{\infty\}$ (see Section 2). Further recall that if G is a compact p-adic analytic group then it admits an open pro-p subgroup U such that the integer $\mathrm{Ord}(G/U)$ is coprime to p. Now if G is not finite then U is also not finite. Hence $n(p) = \infty$. Hence if G is not finite then p divides $\mathrm{Ord}(G)$. Thus by Lemma 3.2 it follows that $P_p : G \to G$ is not surjective. □

Corollary 3.4. *Let G be a reductive algebraic group defined over $\mathbb{Q}_p$ (G is not necessarily Zariski connected). Suppose* $\dim G \geqq 1$. *Then $P_p : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is not surjective.*

Proof. If G is $\mathbb{Q}_p$-isotropic then by Theorem 1.1, $P_p : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is not surjective. Now if the Zariski connected component of identity, G^0 is anisotropic over $\mathbb{Q}_p$ then $G(\mathbb{Q}_p)$ is a compact p-adic analytic group. Further as $\dim G \geqq 1$ the group $G(\mathbb{Q}_p)$ is not finite. Hence by Theorem 3.3 it follows that $P_p : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is not surjective. □

We now give proofs of Theorem 1.2 and Corollary 1.3. We need the following definition. An element x in a p-adic analytic group G is said to be a *compact element* if $\overline{\langle x \rangle}$ is a compact subgroup of G.

Proof of Theorem 1.2. Note that if G is an algebraic group over $\mathbb{Q}_p$ then $G/R_u(G)$ is a reductive algebraic group over $\mathbb{Q}_p$. Hence the implication $(2 \Leftrightarrow 3)$ follows immediately from Theorem 1.1 and Lemma 3.2. Next, the group $G/R_u(G)(\mathbb{Q}_p)$ is a quotient of the group $G(\mathbb{Q}_p)$ and hence $(1 \Rightarrow 2)$ follows.

We now prove $(2 \Rightarrow 1)$. Let us assume that $P_n : G/R_u(G)(\mathbb{Q}_p) \to G/R_u(G)(\mathbb{Q}_p)$ is surjective. Let L be a Levi subgroup of G defined over $\mathbb{Q}_p$. Then $G = LR_u(G)$ (as a semidirect product) and $G(\mathbb{Q}_p) = L(\mathbb{Q}_p)R_u(G)(\mathbb{Q}_p)$. Clearly L is anisotropic over $\mathbb{Q}_p$ and hence $L(\mathbb{Q}_p)$ is compact. Let $g \in G(\mathbb{Q}_p)$. Consider the Jordan decomposition $g = g_s g_u$ where $g_s, g_u \in G(\mathbb{Q}_p)$. Now observe that there is a $c \in G(\mathbb{Q}_p)$ so that $cg_sc^{-1} \in L(\mathbb{Q}_p)$. Also as $P_n : G/R_u(G)(\mathbb{Q}_p) \to G/R_u(G)(\mathbb{Q}_p)$ is surjective it follows that $P_n : L(\mathbb{Q}_p) \to L(\mathbb{Q}_p)$ is surjective and hence by Lemma 3.2, n is coprime to $\mathrm{Ord}\big(L(\mathbb{Q}_p)\big)$. Hence cg_sc^{-1} is a compact element. This implies that g_s is a compact element and $\mathrm{Ord}(g_s) = \mathrm{Ord}(cg_sc^{-1})$ is coprime to n. By Lemma 3.2 it follows that $P_n : \overline{\langle g_s \rangle} \to \overline{\langle g_s \rangle}$ is surjective, where the closure $\overline{\langle g_s \rangle}$ is taken in the p-adic topology of $G(\mathbb{Q}_p)$. Hence there is $h \in \overline{\langle g_s \rangle}$ so that $h^n = g_s$. Also note that $h \in \overline{\langle g_s \rangle} \subset Z_G(g_u)$. Now as g_u is unipotent we can extract an n-th root of g_u in the Zariski closure of the group generated by g_u. Hence g has an n-th root in $G(\mathbb{Q}_p)$.

The last part follows immediately from the three equivalent statements in the theorem and from (3) of Theorem 3.3. □

Proof of Corollary 1.3. Let G be an algebraic group over $\mathbb{Q}_p$ and H be an algebraic $\mathbb{Q}_p$-subgroup of G. Let L and M be $\mathbb{Q}_p$-Levi subgroups of G and H respectively. Then by [P-R], Theorem 2.3, page 58, there exists $b \in R_u(G)(\mathbb{Q}_p)$ so that $bMb^{-1} \subset L$. Hence $bM(\mathbb{Q}_p)b^{-1} \subset L(\mathbb{Q}_p)$. Now let $n \neq 1$ be an integer so that $P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective. Then, by Theorem 1.2, L is $\mathbb{Q}_p$-anisotropic (hence $L(\mathbb{Q}_p)$ is compact) and n is coprime to $\mathrm{Ord}\big(L(\mathbb{Q}_p)\big)$. Hence it follows that M is $\mathbb{Q}_p$-anisotropic and $\mathrm{Ord}\big(M(\mathbb{Q}_p)\big)$ divides $\mathrm{Ord}\big(L(\mathbb{Q}_p)\big)$. We again apply Theorem 1.2 to conclude that $P_n : H(\mathbb{Q}_p) \to H(\mathbb{Q}_p)$ is surjective. □

4. Determination of orders of anisotropic groups

As mentioned in the introduction, by Theorem 1.2, the problem of explicit determination of the integers n for which $P_n : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective for a general connected $\mathbb{Q}_p$-algebraic group G reduces to finding orders $\mathrm{Ord}\big(H(\mathbb{Q}_p)\big)$ for $\mathbb{Q}_p$-anisotropic reductive groups H. Since a large class of $\mathbb{Q}_p$-anisotropic reductive groups are semisimple ones, which in turn are made of $\mathbb{Q}_p$-simple simply connected groups using almost direct products, it is necessary that we set out our first goal to obtain results on $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$ where G is a $\mathbb{Q}_p$-simple simply connected $\mathbb{Q}_p$-anisotropic group.

We begin by recalling the following well known classification of absolutely simple simply connected anisotropic groups over non-archimedean local fields of characteristic zero.

Theorem 4.1 ([P-R], Theorem 6.5). *Let G be a simply connected absolutely simple anisotropic group over a non-archimedean local field $\mathbb{F}$ of characteristic zero. Then as $\mathbb{F}$ groups, G is isomorphic to $\mathbf{SL}_1(D)$ for some finite dimensional central division algebra D over $\mathbb{F}$.*

Let $\mathbb{K}$ be a field, not necessarily algebraically closed, of characteristic zero and let $\mathbb{F}$ be a finite extension of $\mathbb{K}$. Let $\mathscr{R}_{\mathbb{F}/\mathbb{K}}$ denote the *Weil restriction functor* from the category of $\mathbb{F}$-algebraic groups to the category of $\mathbb{K}$-algebraic groups. The following result is again well known.

Theorem 4.2 ([Sp], Section 6.2.1, and [T], Section 3.1.2). *Let $\mathbb{K}$ be a field, not necessarily algebraically closed, of characteristic zero. Let G be a $\mathbb{K}$-simple simply connected algebraic group. Then there exists a finite extension $\mathbb{F}$ (unique up to $\mathbb{K}$-isomorphism of fields) of $\mathbb{K}$ and a simply connected absolutely simple $\mathbb{F}$-group H (unique up to $\mathbb{F}$-isomorphism of algebraic groups) so that G is $\mathbb{K}$-isomorphic to $\mathscr{R}_{\mathbb{F}/\mathbb{K}}(H)$. Moreover, if G is $\mathbb{K}$-anisotropic then H is $\mathbb{F}$-anisotropic.*

Let G be a $\mathbb{Q}_p$-simple simply connected $\mathbb{Q}_p$-anisotropic group. Then by Theorem 4.2, there exists a finite extension $\mathbb{F}$ of $\mathbb{Q}_p$ and a simply connected absolutely simple anisotropic $\mathbb{F}$-group H so that G is $\mathbb{Q}_p$-isomorphic to $\mathscr{R}_{\mathbb{F}/\mathbb{Q}_p}(H)$. Hence as p-adic groups $G(\mathbb{Q}_p)$ is isomorphic to $\mathscr{R}_{\mathbb{F}/\mathbb{Q}_p}(H)(\mathbb{Q}_p) = H(\mathbb{F})$. On the other hand, by Theorem 4.1, H is isomorphic to $\mathbf{SL}_1(D)$ as $\mathbb{F}$-algebraic group, for some finite dimensional central division algebra D over $\mathbb{F}$. Hence as (compact) p-adic group $G(\mathbb{Q}_p)$ is isomorphic to $\mathbf{SL}_1(D)(\mathbb{F}) = \mathrm{SL}_1(D)$. Thus in order to find $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$ for an arbitrary $\mathbb{Q}_p$-simple simply connected anisotropic group G it is enough to find $\mathrm{Ord}\big(\mathrm{SL}_1(D)\big)$ where D is a central division algebra over a finite extension $\mathbb{F}$ of $\mathbb{Q}_p$. We next determine the orders of such groups.

In the proof of the next result we need some facts and terminologies which we borrow from [P-R], Section 1.4, page 27–33 (it may be noted that our notations are slightly different from that of [P-R], Section 1.4).

As above let $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$. If D is a finite dimensional central division algebra over $\mathbb{F}$, the dimension, $\dim_{\mathbb{F}} D = d^2$ for some integer d. Let v be the valuation on $\mathbb{F}$ which is obtained by the unique extension of the usual p-adic valuation, considered additively, on $\mathbb{Q}_p$. Moreover note that the valuation v uniquely extends to a valuation $\tilde{v}$ on D by the formula

$$\tilde{v}(x) = \frac{1}{d} v\big(\mathrm{Nrd}_{D/\mathbb{F}}(x)\big), \quad \text{for } x \in D.$$

Since $\mathbb{F}$ is complete it follows that D is complete in the metric given by the valuation. Let

$$\mathscr{O}_D = \{x \in D : \tilde{v}(x) \geqq 0\} \quad \text{and} \quad \mathfrak{B}_D = \{x \in D : \tilde{v}(x) > 0\}.$$

Note that $\mathfrak{B}_D = \{x \in D : \tilde{v}(x) > 0\}$ is a maximal right and left ideal of $\mathscr{O}_D$. Let $\mathfrak{D} = \mathscr{O}_D/\mathfrak{B}_D$ be the residue division algebra of D. We first identify the residue field of $\mathbb{Q}_p$ with the finite

field $\mathbb{F}_p$, consisting of p elements. Note that the residue field of $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$. We identify the residue field of $\mathbb{F}$ with the finite field $\mathbb{F}_{p^r}$, consisting of p^r elements where r is the degree of the extension of the residue field of $\mathbb{F}$ over $\mathbb{F}_p$. Now observe that $\mathfrak{D}$ is a finite dimensional extension of $\mathbb{F}_{p^r}$. Being a division algebra consisting of finitely many elements, $\mathfrak{D}$ is a field extension of the field $\mathbb{F}_{p^r}$. Consequently $\mathfrak{D} = \mathbb{F}_{p^r}(\alpha)$ for some $\alpha \in \mathfrak{D}$. We may choose $\beta \in \mathcal{O}_D$ so that $\beta + \mathfrak{B}_D = \alpha$. Let $L = \mathbb{F}(\beta)$ and let $\mathfrak{L}$ be the corresponding residue field. Clearly $\mathfrak{L}$ is a finite dimensional field extension of the finite field $\mathbb{F}_{p^r}$. Moreover it is shown in [P-R], Section 1.4.2, that

$$\dim_{\mathbb{F}_{p^r}} \mathfrak{L} = d \quad \text{where } \dim_{\mathbb{F}} D = d^2.$$

We also need the following fact from the theory of profinite groups, which follows from well known results in [R-Z] and [W].

Lemma 4.3 ([R-Z] and [W]). *Let G be a profinite group. Let $\{U_i\}_{i=0}^{\infty}$ be a base consisting of open normal subgroups with $U_0 = G$ and $U_{i+1} \subset U_i$, for all $i \geqq 0$. Then*

$$\mathrm{Ord}(G) = \prod_{i \geqq 0} \mathrm{Ord}(U_i/U_{i+1}).$$

With the above facts and notations in mind we will prove Proposition 4.4.

Proposition 4.4. *Let $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$. Let r be the degree of the residue field of $\mathbb{F}$ over the residue field of $\mathbb{Q}_p$. Let D be a finite dimensional central division algebra over $\mathbb{F}$ with $\dim_{\mathbb{F}} D = d^2$. Then*

$$\mathrm{Ord}\big(\mathrm{SL}_1(D)\big) = \big(1 + p^r + \cdots + (p^r)^{d-1}\big)p^{\infty}.$$

Proof. Let $\dim_{\mathbb{F}} D = d^2$. We first get a filtration of $\mathrm{SL}_1(D)$ as follows. We set

$$U_i = (1 + \mathfrak{B}_D^i) \cap \mathrm{SL}_1(D), \quad \text{for } i \geqq 1$$

and $U_0 = \mathrm{SL}_1(D)$. Note that $\{U_i\}_{1=0}^{\infty}$ are normal subgroups of D^* and they form a base of $\mathrm{SL}_1(D)$ consisting of open subgroups (see [P-R], Section 1.4.4 and note that our notations are slightly different from theirs). Clearly $U_{i+1} \subset U_i$, for all $i \geqq 0$. Using [P-R], Proposition 1.8, we get isomorphisms of the following groups:

$$U_0/U_1 \simeq \{x \in \mathfrak{L}^* : \mathrm{Nr}_{\mathfrak{L}/\mathbb{F}_{p^r}}(x) = 1\}.$$

Moreover, if $i \geqq 1$ we have

$$U_i/U_{i+1} \simeq \mathfrak{L}, \quad \text{if } i \not\equiv 0 \pmod{d}$$

and

$$U_i/U_{i+1} \simeq \{x \in \mathfrak{L} : \mathrm{Tr}_{\mathfrak{L}/\mathbb{F}_{p^r}}(x) = 0\}, \quad \text{if } i \equiv 0 \pmod{d}.$$

We use these isomorphisms to find $\mathrm{Ord}(U_0/U_1)$ and $\mathrm{Ord}(U_i/U_{i+1})$ for all $i \geqq 1$. Note that $\mathfrak{L}$ over $\mathbb{F}_{p^r}$ is a finite Galois extension of degree d where $\dim_{\mathbb{F}} D = d^2$. Hence the Galois group $\mathrm{Gal}(\mathfrak{L} \mid \mathbb{F}_{p^r})$ is cyclic. Let $\mathrm{Gal}(\mathfrak{L} \mid \mathbb{F}_{p^r}) = \langle \sigma \rangle$. By Hilbert Theorem 90 we have

$$\{x \in \mathfrak{L}^* : \mathrm{Nr}_{\mathfrak{L}/\mathbb{F}_{p^r}}(x) = 1\} = \big\{y\big(\sigma(y)\big)^{-1} : y \in \mathfrak{L}^*\big\}$$

and

$$\{x \in \mathfrak{Q} : \mathrm{Tr}_{\mathfrak{Q}/\mathbb{F}_{p^r}}(x) = 0\} = \{y - (\sigma(y)) : y \in \mathfrak{Q}\}.$$

It follows immediately that

$$\mathrm{Ord}\big(\{y(\sigma(y))^{-1} : y \in \mathfrak{Q}^*\}\big) = \mathrm{Ord}(\mathfrak{Q}^*/\mathbb{F}_{p^r}^*) = \frac{p^{rd}-1}{p^r-1} = 1 + p^r + \cdots + (p^r)^{d-1}$$

and

$$\mathrm{Ord}\big(\{y - (\sigma(y)) : y \in \mathfrak{Q}\}\big) = \mathrm{Ord}(\mathfrak{Q}/\mathbb{F}_{p^r}) = \frac{p^{rd}}{p^r} = p^{r(d-1)}.$$

Clearly $\mathrm{Ord}(\mathfrak{Q}) = p^{rd}$. Hence

$$\mathrm{Ord}(U_0/U_1) = 1 + p^r + \cdots + (p^r)^{d-1}.$$

Moreover, if $i \geqq 1$ we have

$$\mathrm{Ord}(U_i/U_{i+1}) = p^{rd}, \quad \text{if } i \not\equiv 0 \pmod{d}$$

and

$$\mathrm{Ord}(U_i/U_{i+1}) = p^{r(d-1)}, \quad \text{if } i \equiv 0 \pmod{d}.$$

Now we use Lemma 4.3 to conclude the proof of the proposition. □

In the following definition we associate two integers r_G and d_G to a $\mathbb{Q}_p$-anisotropic $\mathbb{Q}_p$-simple group G.

Definition 4.5. Let G be $\mathbb{Q}_p$-simple and $\mathbb{Q}_p$-anisotropic. Theorem 4.2 says that there exists a finite degree field extension $\mathbb{F}$, unique up to a $\mathbb{Q}_p$-isomorphism, and an absolutely simple algebraic group H over $\mathbb{F}$, unique up to $\mathbb{F}$-isomorphism, so that $\mathscr{R}_{\mathbb{F}/\mathbb{Q}_p}(H)$ is the simply connected cover (over $\mathbb{Q}_p$) of G. Define r_G to be the degree of the residue field of $\mathbb{F}$ over the residue field of $\mathbb{Q}_p$. By Theorem 4.1, H is $\mathbb{F}$-isomorphic to $\mathbf{SL}_1(D)$ for some central division algebra over $\mathbb{F}$. Hence $\sqrt{\dim H + 1}$ is an integer (in fact it is the degree of D over $\mathbb{F}$). We define d_G to be $\sqrt{\dim H + 1}$.

Now we may reformulate the above proposition as follows.

Proposition 4.6. *Let G be a simply connected $\mathbb{Q}_p$-simple $\mathbb{Q}_p$-anisotropic algebraic group. Then*

$$\mathrm{Ord}\big(G(\mathbb{Q}_p)\big) = \big(1 + p^{r_G} + \cdots + (p^{r_G})^{d_G-1}\big)p^{\infty}.$$

Recall that if G is an absolutely simple simply connected $\mathbb{Q}_p$-anisotropic group then $r_G = 1$ and $d_G = \sqrt{\dim G + 1}$. Hence for such an algebraic group G we obtain the following result which gives a transparent formula for $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$ in terms of the dimension of G.

Corollary 4.7. *Let G be an algebraic group over $\mathbb{Q}_p$ which is absolutely simple, simply connected and anisotropic. Then*

$$\mathrm{Ord}\big(G(\mathbb{Q}_p)\big) = (1 + p + \cdots + p^{d-1})p^{\infty}$$

where $d = \sqrt{\dim G + 1}$.

We now prove a result on the order of $G(\mathbb{Q}_p)$ where G is a $\mathbb{Q}_p$-simple $\mathbb{Q}_p$-anisotropic group, not necessarily simply connected. We need the following simple lemma.

Lemma 4.8. *Let G be a compact p-adic analytic group and H be a closed subgroup. Let m be an integer such that $x^m \in H$, for all $x \in G$. If q is a prime dividing* $\mathrm{Ord}(G)$ *then q divides* $m\,\mathrm{Ord}(H)$.

Proof. Follows easily from Lagrange's theorem for profinite groups and the fact that $\mathrm{Ord}(G) = mp^{n(p)}$ where $m \in \mathbb{N}$, g.c.d$(m, p) = 1$ and $n(p) \in \mathbb{N} \cup \{\infty\}$. □

We need another useful lemma.

Lemma 4.9. *Let G and $\tilde{G}$ be $\mathbb{Q}_p$-anisotropic reductive groups and let $\phi : \tilde{G} \to G$ be a surjective algebraic group homomorphism defined over $\mathbb{Q}_p$ with* $\mathrm{Ker}\,\phi$ *being a central subgroup in $\tilde{G}$. Suppose d is an integer so that $x^d = 1$ for all $x \in \mathrm{Ker}\,\phi$. Then prime divisors of* $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$ *will divide* $d\,\mathrm{Ord}\big(\tilde{G}(\mathbb{Q}_p)\big)$.

Proof. Consider the exact sequence of algebraic groups defined over $\mathbb{Q}_p$:

$$1 \to \mathrm{Ker}\,\phi \to \tilde{G} \xrightarrow{\phi} G \to 1.$$

Note that $\mathrm{Ker}\,\phi$ is a central subgroup of $\tilde{G}$ defined over $\mathbb{Q}_p$.

Then using [Se], Corollary 2 of Section 5.6 and Proposition 43 of Section 5.7, we have another exact sequence:

$$1 \to \mathrm{Ker}\,\phi(\mathbb{Q}_p) \to \tilde{G}(\mathbb{Q}_p) \xrightarrow{\phi} G(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, \mathrm{Ker}\,\phi),$$

where $H^1(\mathbb{Q}_p, \mathrm{Ker}\,\phi)$ denotes the first Galois-cohomology group of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p \mid \mathbb{Q}_p)$ with coefficients in the abelian group $\mathrm{Ker}\,\phi$. This implies that $H^1(\mathbb{Q}_p, \mathrm{Ker}\,\phi)$ is a torsion group with $x^d = 1$ for all $x \in H^1(\mathbb{Q}_p, \mathrm{Ker}\,\phi)$. Hence for every $g \in G(\mathbb{Q}_p)$ we have $g^d \in \phi\big(\tilde{G}(\mathbb{Q}_p)\big)$. Note that $\phi\big(\tilde{G}(\mathbb{Q}_p)\big)$ is closed subgroup of $G(\mathbb{Q}_p)$ in the p-adic topology and consequently by Lagrange's theorem the primes dividing the order of $\mathrm{Ord}\big(\phi\big(\tilde{G}(\mathbb{Q}_p)\big)\big)$ divide $\mathrm{Ord}\big(\tilde{G}(\mathbb{Q}_p)\big)$. Thus it follows from Lemma 4.8 that the primes dividing $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$ will divide $d\,\mathrm{Ord}\big(\tilde{G}(\mathbb{Q}_p)\big)$. □

Proposition 4.10. *Let G be a $\mathbb{Q}_p$-simple $\mathbb{Q}_p$-anisotropic group. Let $\tilde{G}$ be the simply connected cover of G defined over $\mathbb{Q}_p$. Then prime divisors of* $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$ *divide* $d_G\,\mathrm{Ord}\big(\tilde{G}(\mathbb{Q}_p)\big)$.

Proof. Recall that there exists a finite extension $\mathbb{F}$ of $\mathbb{Q}_p$ and a finite dimensional central division algebra D over $\mathbb{F}$ such that $\tilde{G}$ is $\mathbb{Q}_p$-isomorphic to the anisotropic simple

algebraic group $\mathscr{R}_{\mathbb{F}/\mathbb{Q}_p}\big(\mathbf{SL}_1(D)\big)$. Also recall that as $\overline{\mathbb{Q}}_p$-groups, $\mathbf{SL}_1(D)$ is isomorphic to $\mathrm{SL}_d(\overline{\mathbb{Q}}_p)$ where $\dim_{\mathbb{F}} D = d^2$. Hence as $\overline{\mathbb{Q}}_p$-groups the group $\mathscr{R}_{\mathbb{F}/\mathbb{Q}_p}\big(\mathbf{SL}_1(D)\big)$ is isomorphic to the direct product $\mathrm{SL}_d(\overline{\mathbb{Q}}_p)^{[\mathbb{F}:\mathbb{Q}_p]}$. Hence

$$\operatorname{Ker}\phi \subset Z(\tilde{G}) = Z\big(\mathscr{R}_{\mathbb{F}/\mathbb{Q}_p}\big(\mathbf{SL}_1(D)\big)\big) = Z\big(\mathrm{SL}_d(\overline{\mathbb{Q}}_p)^{[\mathbb{F}:\mathbb{Q}_p]}\big).$$

Thus $Z(\tilde{G})$ is a direct product of $[\mathbb{F}:\mathbb{Q}_p]$ many copies of the finite cyclic group of order d. This implies that $\operatorname{Ker}\phi$ is a torsion group with $x^d = 1$ for all $x \in \operatorname{Ker}\phi$. Thus it follows from Lemma 4.9 that if q is a prime dividing $\operatorname{Ord}\big(G(\mathbb{Q}_p)\big)$ then q divides the integer $d\operatorname{Ord}\big(\tilde{G}(\mathbb{Q}_p)\big)$. The proof is completed by noting that $d = d_G$. □

Definition 4.11. For a semisimple connected anisotropic algebraic group H over $\mathbb{Q}_p$ we associate two integers $M(H)$ and $N(H)$ in the following way. First recall that H is $\mathbb{Q}_p$-isomorphic to an almost direct product of $\mathbb{Q}_p$-simple simply connected groups. Each such $\mathbb{Q}_p$-simple group is called factor of G. Let $H_1, \ldots, H_k$ be the non-$\mathbb{Q}_p$-isomorphic $\mathbb{Q}_p$-simple factors of H defined over $\mathbb{Q}_p$. Clearly all such factors are $\mathbb{Q}_p$-anisotropic over $\mathbb{Q}_p$. We now define

$$M(H) = p\prod_{i=1}^{k}\big(1 + p^{r_{H_i}} + \cdots + (p^{r_{H_i}})^{(d_{H_i}-1)}\big)$$

and

$$N(H) = M(H)\prod_{i=1}^{k} d_{H_i}.$$

Note that the prime factors of $M(H)$ are the same as the prime factors of the supernatural number $\prod_{i=1}^{k}\operatorname{Ord}\big(H_i(\mathbb{Q}_p)\big)$. We also note that $M(H) = M(\tilde{H})$ and $N(H) = N(\tilde{H})$, where $\tilde{H}$ is the simply connected cover of H defined over $\mathbb{Q}_p$.

All the above observations now lead to the proof of Theorem 1.4.

Proof of Theorem 1.4. In view of Theorem 1.2 it is enough to assume the $\mathbb{Q}_p$-algebraic group G to be semisimple. Let $H_1, \ldots, H_k$ be the $\mathbb{Q}_p$-simple simply connected (anisotropic) factors of G. Then G is $\mathbb{Q}_p$-isomorphic to $\prod_{i=1}^{k} H_i/Z$ where Z is some central subgroup of $\prod_{i=1}^{k} H_i$, defined over $\mathbb{Q}_p$. Further, if G is simply connected then G is $\mathbb{Q}_p$-isomorphic to the direct product $\prod_{i=1}^{k} H_i$. So part (1) of the theorem follows from Theorem 1.2 and Proposition 4.6.

Now we prove part (2) of the theorem. We use an argument similar to the proof of Proposition 4.10. Let G be a semisimple $\mathbb{Q}_p$-anisotropic group. Following the above notation we have the exact sequence of groups defined over $\mathbb{Q}_p$:

$$1 \to Z \to \prod_{i=1}^{k} H_i \xrightarrow{\psi} G \to 1.$$

Now $Z \subset \prod_{i=1}^{k} Z(H_i)$. Further note that for each i, we have $x^{d_{H_i}} = 1$, for all $x \in Z(H_i)$. Thus $x^{\prod_{i=1}^{k} d_{H_i}} = 1$ for all $x \in Z$. Thus it follows from Lemma 4.9 that if q is a prime dividing $\mathrm{Ord}\big(G(\mathbb{Q}_p)\big)$ then q divides $\prod_{i=1}^{k} d_{H_i} \cdot \prod_{i=1}^{k} \mathrm{Ord}\big(H_i(\mathbb{Q}_p)\big)$. Hence q divides $N(G)$. To complete the proof we use Theorem 1.2 and Proposition 4.6. □

We will now illustrate, using an example, the computation of $M(G)$.

Example 4.12. Let $D_1, \ldots, D_k$ be a collection of k many central division algebras over $\mathbb{Q}_p$. Assume that the degree of D_i over $\mathbb{Q}_p$ is d_i for all i. Let us consider the direct product $G = \prod_{i=1}^{k} \mathbf{SL}_1(D_i)$. Then, by Definition 4.11, $M(G) = p \prod_{i=1}^{k} (1 + p + \cdots + p^{(d_i - 1)})$. Let V be a finite dimensional $\overline{\mathbb{Q}}_p$-vector space defined over $\mathbb{Q}_p$. By Theorem 1.4 it follows that, for any $\mathbb{Q}_p$-representation $\phi : G \to \mathrm{GL}(V)$, the n-th power map P_n on the group $G(\mathbb{Q}_p) \ltimes_\phi V(\mathbb{Q}_p)$ is surjective if and only if n is coprime to $p \prod_{i=1}^{k} (1 + p + \cdots + p^{(d_i - 1)})$. Using Corollary 1.3 it also follows that if H is any $\mathbb{Q}_p$-subgroup of $G \ltimes_\phi V$ and if n is coprime to $p \prod_{i=1}^{k} (1 + p + \cdots + p^{(d_i - 1)})$ then $P_n : H(\mathbb{Q}_p) \to H(\mathbb{Q}_p)$ is surjective.

5. Exponentiality of *p*-adic algebraic groups

In this section we prove Theorem 1.5. We begin by recalling the two interesting results which motivate Theorem 1.5. The first one is Theorem 5.1 and it is proved by A. Lubotzky and G. Prasad independently; see also [R1], Theorem 1.1, and [R2], Theorem 3.3, for a proof of this result given by M. Ratner. The second one is Theorem 5.2 which is due to M. McCrudden (see [M]).

Theorem 5.1 (A. Lubotzky, G. Prasad). *Let $\phi : \mathbb{Q}_p \to \mathrm{GL}_n(\mathbb{Q}_p)$ be a continuous (hence analytic) group homomorphism. Then there exists a nilpotent $X \in \mathfrak{gl}_n(\mathbb{Q}_p)$ so that $\phi(t) = \exp(tX)$ for all $t \in \mathbb{Q}_p$. Consequently, if G is an algebraic group over $\mathbb{Q}_p$ then $E_{\mathbb{Q}_p}\big(G(\mathbb{Q}_p)\big) = \mathscr{U}_G(\mathbb{Q}_p)$.*

The above result implies that for an algebraic group G over $\mathbb{Q}_p$, the subgroup $G(\mathbb{Q}_p)$ is exponential if and only if the group G is unipotent. This feature is very special to p-adic algebraic groups and does not happen in the case of real Lie groups.

Theorem 5.2 (M. McCrudden). *Let G be a real Lie group. Then $E_{\mathbb{R}}(G) = \bigcap_{n \geq 2} P_n(G)$.*

Hence it follows immediately that a real Lie group G is exponential if and only if $P_n : G \to G$ is surjective for all n.

We need the following lemmas to prove Theorem 1.5. For $x \in G$, let $\mathrm{Zcl}(x)$ denote the Zariski closure of the group $\langle x \rangle$, generated by x. A sequence of integers $\{a_n\}_{n=1}^{\infty} \subset \mathbb{N}$ is said to be *multiplicatively closed* if $a_i a_j \in \{a_n\}_{n=1}^{\infty}$ for all i, j.

Lemma 5.3. *Let G be an algebraic group over $\mathbb{Q}_p$ and $\alpha \in G(\mathbb{Q}_p)$. Let $\{a_n\}_{n=1}^{\infty} \subset \mathbb{N}$ be a multiplicatively closed sequence of integers. Assume that for every n there exists $\beta_n \in G(\mathbb{Q}_p)$ so that $\alpha = \beta_n^{a_n}$. Then for every integer n there exists $\gamma_n \in \mathrm{Zcl}(\alpha)(\mathbb{Q}_p)$ so that $\alpha = \gamma_n^{a_n}$.*

Proof. We first recall that for any positive integer m there exists a positive integer r so that if $F \subset \mathrm{GL}_m(\mathbb{Q}_p)$ any finite group then $\mathrm{Ord}(F)$ divides r. This follows immediately from the fact that the corresponding statement holds if $\mathrm{GL}_n(\mathbb{Q}_p)$ is replaced by $\mathrm{GL}_n(\mathbb{Z}_p)$ (see [S1], Theorem 1, page 124) and the fact that any compact subgroup of $\mathrm{GL}_n(\mathbb{Q}_p)$ is conjugate to a subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ which is a maximal compact subgroup of $\mathrm{GL}_n(\mathbb{Q}_p)$ (see [S1], Theorems 1 and 2, page 122). From the above fact it follows that if H is an $\mathbb{Q}_p$-algebraic group then there is an integer l so that if $F \subset H(\mathbb{Q}_p)$ is a finite subgroup then $\mathrm{Ord}(F)$ divides l. Thus we observe that if H is as above then there is an integer l so that if $x \in H(\mathbb{Q}_p)$ with $\mathrm{Ord}(x) < \infty$ then $\mathrm{Ord}(x)$ divides l.

Now suppose $\alpha \in G(\mathbb{Q}_p)$ is as in the statement of the theorem. Consider the $\mathbb{Q}_p$-algebraic group $Z_G(\alpha)/\mathrm{Zcl}(\alpha)$. Let l be the integer for which the contention of the above observation holds for the group $Z_G(\alpha)/\mathrm{Zcl}(\alpha)$. By the assumption of the theorem, for every integer n there exists $\beta \in G(\mathbb{Q}_p)$ so that $\alpha = \beta_n^{a_n}$. Clearly $\beta_n \in Z_G(\alpha)(\mathbb{Q}_p)$ and the coset $\beta_n \mathrm{Zcl}(\alpha)$ is a finite order element in $Z_G(\alpha)/\mathrm{Zcl}(\alpha)$. Hence $\beta_n^l \in \mathrm{Zcl}(\alpha)$. Also observe that the set $\{\mathrm{g.c.d}(a_n, l) \mid n \geqq 1\}$ is a finite set and let it be $\{d_1, \ldots, d_k\}$. We set $d = \prod_{i=1}^{k} d_i$. Clearly $\beta_n^d \in \mathrm{Zcl}(\alpha)$. Now as $\{a_n\}$ is multiplicatively closed, we may choose a_k in $\{a_n\}$ such that d divides a_k. Again applying the same property of the sequence $\{a_n\}$, there exists $\delta_n \in G(\mathbb{Q}_p)$ so that $\alpha = \delta_n^{a_k a_n}$. Clearly as d divides a_l it follows that $\delta_n^{a_k} \in \mathrm{Zcl}(\alpha)$. If we set $\gamma_n = \delta_n^{a_k}$ then $\gamma_n \in \mathrm{Zcl}(\alpha)$ and $\alpha = \gamma_n^{a_n}$ and we are done. □

Lemma 5.4. *Let H be a profinite group with $\mathrm{Ord}(H) = mp^{n(p)}$ where $m \in \mathbb{N}$, $\mathrm{g.c.d}(m, p) = 1$ and $n(p) \in \mathbb{N} \cup \{\infty\}$. Let $\alpha \in H$. Assume that for all k, there exists $\beta \in H$ so that $\alpha = \beta^{p^k}$. Then α is an element of finite order and $\mathrm{Ord}(\alpha)$ divides m. In particular, $\mathrm{Ord}(\alpha)$ is coprime to p.*

Proof. If H is a finite group then the proof is easy and we omit it. Now if H is infinite then $n(p) = \infty$ and there is an open normal subgroup U of H which is pro-p. We now see that the coset αU has p^k-th root in the finite group H/U. Hence, using the finite group case at hand, we conclude that $\mathrm{Ord}(\alpha U)$ divides m. In other words $\alpha^m \in U$. Let $V \subset U$ be any open normal subgroup of H. We claim that $\alpha^m \in V$. Observe that $\mathrm{Ord}(H/V) = mp^l$ for some integer l. By assumption, there exists $\beta \in H$ such that $\alpha = \beta^{p^l}$. Then $\alpha^m = \beta^{mp^l}$. But $\beta^{mp^l} \in V$ and hence $\alpha^m \in V$. Thus for every open subgroup V of U, which is normal in H, α^m lies in V. This forces the equality $\alpha^m = e$. □

Proof of Theorem 1.5. We start with the proof of the first part of the theorem. Let $\alpha \in G(\mathbb{Q}_p)$ be a semisimple element with $\alpha \in \bigcap_{n=1}^{\infty} P_{p^n}\big(G(\mathbb{Q}_p)\big)$. Considering the multiplicatively closed sequence $\{p^n\}_{n=1}^{\infty}$, we use Lemma 5.3 to see that $\alpha \in \bigcap_{n=1}^{\infty} P_{p^n}\big(\mathrm{Zcl}(\alpha)(\mathbb{Q}_p)\big)$. Let us denote by T the Zariski connected component of $\mathrm{Zcl}(\alpha)$. Then T is a torus defined over $\mathbb{Q}_p$.

Recall that there exists a $\mathbb{Q}_p$-split subtorus T_s and an $\mathbb{Q}_p$-anisotropic subtorus T_a of T such that $T = T_s T_a$ with $\mathrm{Ord}(T_a \cap T_s) < \infty$. Let $F = (T_a \cap T_s)(\mathbb{Q}_p)$. We further recall that

$T_a(\mathbb{Q}_p)T_s(\mathbb{Q}_p)$ is a finite index subgroup of $T(\mathbb{Q}_p)$. Note that $T(\mathbb{Q}_p)$ is also a finite index subgroup of $\mathrm{Zcl}(\alpha)(\mathbb{Q}_p)$. Thus $T_a(\mathbb{Q}_p)T_s(\mathbb{Q}_p)$ is a finite index subgroup $\mathrm{Zcl}(\alpha)(\mathbb{Q}_p)$; let this finite index be k.

Recall that, for every n there exists $\beta \in \mathrm{Zcl}(\alpha)(\mathbb{Q}_p)$ so that $\alpha = \beta^{p^n}$. This implies that $\alpha^k = (\beta^k)^{p^n}$. Clearly there exist $\gamma_a, \delta_a \in T_a(\mathbb{Q}_p)$ and $\gamma_s, \delta_s \in T_a(\mathbb{Q}_p)$ so that $\alpha^k = \gamma_s\gamma_a$ and $\beta^k = \delta_s\delta_a$. This implies that $\delta_s^{p^n} \in \gamma_s F$. Now as T_s is a $\mathbb{Q}_p$-split torus, the subgroup F and the elements γ_s, δ_s can be regarded as lying in the direct product $(\mathbb{Q}_p^*)^{\dim T_s}$. Let us denote by K the compact analytic subgroup $\mathrm{Units}(\mathbb{Z}_p)^{\dim T_s}$ of $(\mathbb{Q}_p^*)^{\dim T_s}$. Clearly $F \subset K$ and as, for every n one has $\delta_s^{p^n} \in \gamma_s F$, it follows that $\delta_s, \gamma_s \in K$. Thus $\alpha^k \in KT_a(\mathbb{Q}_p)$ has p^n-th root in the group $KT_a(\mathbb{Q}_p)$. But the group $KT_a(\mathbb{Q}_p)$ is a compact analytic p-adic group. We now apply Lemma 5.4 to conclude that α^k is of finite order. Thus α is of finite order and consequently, $\mathrm{Zcl}(\alpha)(\mathbb{Q}_p)$ is the group generated by α. Further, $\alpha \in \bigcap_{n=1}^{\infty} P_{p^n}\big(\mathrm{Zcl}(\alpha)(\mathbb{Q}_p)\big)$. Hence $\mathrm{Ord}(\alpha)$ is coprime to p.

To prove the second part of the theorem we observe that the following containments can be easily proved:

$$\mathscr{U}_G(\mathbb{Q}_p) \subset E_{\mathbb{Q}_p}\big(G(\mathbb{Q}_p)\big) \subset \bigcap_{n=2}^{\infty} P_n\big(G(\mathbb{Q}_p)\big).$$

In view of this it now remains to prove that $\bigcap_{n=2}^{\infty} P_n\big(G(\mathbb{Q}_p)\big) \subset \mathscr{U}_G(\mathbb{Q}_p)$. It is enough to show that if $g \in G(\mathbb{Q}_p)$ is semisimple and $g \in \bigcap_{n=2}^{\infty} P_n\big(G(\mathbb{Q}_p)\big)$, then $g = e$. By the first part of the theorem it follows that g is of finite order. Hence $\mathrm{Zcl}(g)(\mathbb{Q}_p) = \langle g \rangle$ and further by Lemma 5.3, $P_n : \langle g \rangle \to \langle g \rangle$ is surjective, for all n. This forces $g = e$. □

Proof of Corollary 1.6. Let $\mathscr{N}_G$ be the variety of nilpotent elements in $L(G)$. Note that both $\mathscr{U}_G$ and $\mathscr{N}_G$ are defined over $\mathbb{Q}_p$ and there is a $\mathbb{Q}_p$-isomorphism of varieties, $\exp : \mathscr{N}_G \to \mathscr{U}_G$. Thus $\exp : \mathscr{N}_G(\mathbb{Q}_p) \to \mathscr{U}_G(\mathbb{Q}_p)$ is a bijection of the sets of $\mathbb{Q}_p$-rational points.

Let $\phi : \mathbb{Q} \to G(\mathbb{Q}_p)$ be an abstract homomorphism. Observe that

$$\phi(\mathbb{Q}) \subset \bigcap_{n=1}^{\infty} P_n\big(G(\mathbb{Q}_p)\big) = \mathscr{U}_G(\mathbb{Q}_p).$$

Thus there exists $X \in \mathscr{N}_G(\mathbb{Q}_p)$ such that $\phi(1) = \exp(X)$. Let $k \neq 0$ be a positive integer. For the same reason as above, there exists $Y \in \mathscr{N}_G(\mathbb{Q}_p)$ such that $\phi(1/k) = \exp(Y)$. But then $\exp(X) = \big(\phi(1/k)\big)^k = \exp(kY)$. Hence $Y = X/k$. Thus we have shown

$$\phi(1/k) = \exp(X/k).$$

This implies that $\phi(t) = \exp(tX)$, for all $t \in \mathbb{Q}$. □

Proof of Corollary 1.7. The implication $(1 \Rightarrow 2)$ is obvious. The implications $(1 \Leftrightarrow 3 \Leftrightarrow 4)$ follow immediately from Theorem 1.5.

We now prove the implication $(2 \Rightarrow 3)$. Let G be an algebraic group over $\mathbb{Q}_p$. Now as $P_p : G(\mathbb{Q}_p) \to G(\mathbb{Q}_p)$ is surjective it follows that $P_p : G/R_u(G)(\mathbb{Q}_p) \to G/R_u(G)(\mathbb{Q}_p)$ is surjective. As $G/R_u(G)$ is Zariski connected, to show that $G/R_u(G)$ is trivial we need $\dim G/R_u(G) = 0$. Now appeal to the last part of Theorem 1.2 to complete the proof. □

Remark 5.5. In [Mo], M. Moskowitz defined an algebraic group G to be exponential if each point of G is contained in a Zariski connected abelian algebraic subgroup of G; see also related results in [Ch2], [Ch3] and [Wu]. For a complex algebraic group G if we define the set $E_{\mathbb{C}}\big(G(\mathbb{C})\big)$ as in the introduction, then G is exponential in the sense of Moskowitz if and only if $E_{\mathbb{C}}\big(G(\mathbb{C})\big) = G(\mathbb{C})$. However, if $\mathbb{K}$ is either $\mathbb{Q}_p$ or $\mathbb{R}$ and if G is an algebraic group over $\mathbb{K}$ then it is not true in general that the condition $G(\mathbb{K}) = E_{\mathbb{K}}\big(G(\mathbb{K})\big)$ is equivalent to saying that every point of $G(\mathbb{K})$ lies in a Zariski connected abelian ($\mathbb{K}$-) subgroup of G. For instance, if G is a split torus over $\mathbb{R}$ then clearly $P_2 : G(\mathbb{R}) \to G(\mathbb{R})$ is not surjective and hence $E_{\mathbb{R}}\big(G(\mathbb{R})\big) \neq G(\mathbb{R})$. Also, if G is any torus over $\mathbb{Q}_p$ then it follows from Corollary 1.7 that $E_{\mathbb{Q}_p}\big(G(\mathbb{Q}_p)\big) \neq G(\mathbb{Q}_p)$. Whereas, in both the above cases, G itself is obviously a Zariski connected abelian algebraic group over $\mathbb{K}$.

6. Groups over $\mathbb{Q}$ and concluding remarks

The first half of this section is devoted to obtaining results on n-th power maps on $G(\mathbb{Q})$ where G is an algebraic group defined over $\mathbb{Q}$. The proof of some of the results follows a similar path as in the case of groups over $\mathbb{Q}_p$ (hence we omit such proofs) while the proof of the other results are direct applications of results obtained in the earlier sections.

Theorem 6.1. *Let G be an algebraic group over $\mathbb{Q}$ which is $\mathbb{Q}$-isotropic and let $n \neq 1$. Then $P_n : G(\mathbb{Q}) \to G(\mathbb{Q})$ is not surjective.*

Proof. The proof of this theorem is similar to that of Theorem 1.1 and we omit it. □

Theorem 6.2. *Let G be an algebraic group over $\mathbb{Q}$. Then we have the following*:

(1) *Let $\alpha \in \bigcap_{k=1}^{\infty} P_{m^k}\big(G(\mathbb{Q})\big)$ be a semisimple element. Then α is a finite order element and* $\mathrm{Ord}(\alpha)$ *is coprime to m.*

(2)

$$\bigcap_{n=1}^{\infty} P_n\big(G(\mathbb{Q})\big) = \mathscr{U}_G(\mathbb{Q}),$$

in particular, $P_n : G(\mathbb{Q}) \to G(\mathbb{Q})$ surjective for all n if and only if G is unipotent.

(3) *Let $\phi : \mathbb{Q} \to G(\mathbb{Q})$ be an abstract group homomorphism then there exists a nilpotent $X \in L(G)(\mathbb{Q})$ so that $\phi(t) = \exp(tX)$ for all $t \in \mathbb{Q}$. In particular, if G is reductive and $\mathbb{Q}$-anisotropic then any such abstract homomorphism is trivial.*

Proof. We will take advantage of the fact that if G is an algebraic group over $\mathbb{Q}$ then $G(\mathbb{Q}) \subset G(\overline{\mathbb{Q}}) \subset G(\overline{\mathbb{Q}}_p)$ for every prime p. Further, the Jordan decomposition of an element in $G(\overline{\mathbb{Q}})$ coincides with that in the group $G(\overline{\mathbb{Q}}_p)$, for every p.

Proof of (1). Let α be as in the first statement. Let p be a prime divisor of m. Then from the fact that $\alpha \in \bigcap_{k=1}^{\infty} P_{m^k}\big(G(\mathbb{Q})\big)$ it follows easily that

$$\alpha \in \bigcap_{k=1}^{\infty} P_{p^k}\big(G(\mathbb{Q})\big) \subset \bigcap_{k=1}^{\infty} P_{p^k}\big(G(\mathbb{Q}_p)\big).$$

Now by Theorem 1.5 it follows that α is of finite order and $\mathrm{Ord}(\alpha)$ is coprime to p. Thus $\mathrm{Ord}(\alpha)$ is coprime to m.

Proof of (2). It is easy to see that $\mathscr{U}_G(\mathbb{Q}) \subset \bigcap_{n=1}^{\infty} P_n\big(G(\mathbb{Q})\big)$. By (1), if

$$\alpha \in \bigcap_{n=1}^{\infty} P_n\big(G(\mathbb{Q})\big)$$

is semisimple then α is of finite order and $\mathrm{Ord}(\alpha)$ is coprime to all integers. Hence $\alpha = e$. Thus $\bigcap_{n=1}^{\infty} P_n\big(G(\mathbb{Q})\big) \subset \mathscr{U}_G(\mathbb{Q})$.

Proof of (3). The proof of the first part is similar to that of Corollary 1.6 and we omit it. The second part follows from the fact that a $\mathbb{Q}$-anisotropic reductive group G does not admit nontrivial nilpotent elements in $L(G)(\mathbb{Q})$. □

We conclude with the following remarks.

Remark 6.3. We note that all of our results in the previous sections can be extended to the groups which are $\mathbb{K}$-rational points of an algebraic group defined over $\mathbb{K}$, where $\mathbb{K}$ is a finite extension of $\mathbb{Q}_p$. After suitable modification of the proofs one may see that orders of relevant groups in Proposition 4.4 will involve the ramification index of $\mathbb{K}$ over $\mathbb{Q}_p$ (or the degree of the residue field of $\mathbb{K}$ over the residue field of $\mathbb{Q}_p$). Consequently, the associated integers in Definition 4.11 and Theorem 1.4 too will involve the ramification index of $\mathbb{K}$ over $\mathbb{Q}_p$.

Remark 6.4. We end the paper with a question. If T is an anisotropic torus over $\mathbb{Q}_p$ (of positive dimension) then $T(\mathbb{Q}_p)$ is a compact p-adic analytic group. It follows easily that the prime p divides the $\mathrm{Ord}\big(T(\mathbb{Q}_p)\big)$. It will be interesting to find out a method to know the other prime divisors of $\mathrm{Ord}\big(T(\mathbb{Q}_p)\big)$.

Acknowledgments

The author thanks Dave Witte Morris and Gopal Prasad for their interest, for making various comments and for pointing out an error in an earlier version of the paper. The

author thanks Riddhi Shah for some helpful discussions on the proof of Lemma 5.3. Thanks are due to Preeti Raman for some useful discussions.

References

[B] *A. Borel*, Linear Algebraic Groups, Second Edition, Grad. Texts Math. **126**, Springer-Verlag, 1986.
[B-T] *A. Borel* and *J. Tits*, Groupes réductifs, Inst. Hautes Ét. Sci. Publ. Math. **27** (1965), 55–150.
[Ch1] *P. Chatterjee*, On the surjectivity of power maps of solvable Lie groups, J. Algebra **248** (2002), 669–687.
[Ch2] *P. Chatterjee*, On the surjectivity of the power maps of algebraic groups in characteristic zero, Math. Res. Lett. **9** (2002), 741–756.
[Ch3] *P. Chatterjee*, On the surjectivity of the power maps of semisimple algebraic groups, Math. Res. Lett. **10** (2003), 625–633.
[Ch4] *P. Chatterjee*, Surjectivity of the power maps of real algebraic groups, preprint.
[Ch5] *P. Chatterjee*, Automorphism invariant Cartan subgroups and power maps of disconnected groups, preprint.
[Dj-H] *D. Z. Djoković* and *K. H. Hofmann*, The surjectivity questions for the exponential function of real Lie groups: a status report, J. Lie Th. **7** (1997), 171–197.
[M] *M. McCrudden*, On *n*-th roots and infinitely divisible elements in a connected Lie group, Math. Proc. Cambridge Philos. Soc. **89** (1981), 293–299.
[Mo] *M. Moskowitz*, Exponentiality of algebraic groups, J. Algebra **186** (1996), 20–31.
[P-R] *V. Platonov* and *A. Rapinchuk*, Algebraic groups and number theory, Academic Press, 1994.
[R1] *M. Ratner*, Raghunathan's conjectures for cartesian products of real and *p*-adic Lie groups, Duke Math. J. **77** (1998), 275–382.
[R2] *M. Ratner*, On the *p*-adic and *S*-arithmetic generalizations of Raghunathan's conjectures, Lie groups and ergodic theory (Mumbai 1996), Tata Inst. Fund. Res. Stud. Math. **14** (1996), 167–202.
[R-Z] *L. Ribes* and *P. Zalesskii*, Profinite Groups, Springer-Verlag, 2000.
[S] *J.-P. Serre*, Galois cohomology, Springer-Verlag, 1997.
[S1] *J.-P. Serre*, Lie algebras and Lie groups, Lect. Notes Math. **1500**, Springer-Verlag, 1992.
[Sp] *T. A. Springer*, Linear Algebraic Groups, Encyclop. Math. Sci. **55**, Springer-Verlag (1994), 4–121.
[St] *R. Steinberg*, On the power maps in algebraic groups, Math. Res. Lett. **10** (2003), 621–624.
[T] *J. Tits*, Classification of algebraic semisimple groups, Algebraic Groups and Discontinuous Subgroups, Proc. Symp. Pure Math., Boulder, Col., Amer. Math. Soc. (1966), 33–62.
[W] *J. S. Wilson*, Profinite Groups, Oxford University Press, 1998.
[Wu] *M. Wüstner*, On the surjectivity of the exponential function of complex algebraic, complex semisimple and complex splittable Lie groups, J. Algebra **184** (1996), 1082–1092.

The Institute of Mathematical Sciences, C.I.T. Campus, Taramani, Chennai-600113, India
e-mail: pralay@imsc.res.in

Eingegangen 29. Mai 2007, in revidierter Fassung 13. Februar 2008