Mathematical Research Letters **10**, 621–624 (2002)

ON POWER MAPS IN ALGEBRAIC GROUPS

Robert Steinberg

Our goal in this note is a simple proof of the following result.

Theorem 1. *Let G be a (connected) semisimple algebraic group, p the characteristic exponent of the base field K, and n a positive integer which is prime to p. Then the power map P_n on G defined by $x \to x^n$ is surjective if and only if n is prime to the bad primes for G and also to the central primes, those that divide the order of the center of G.*

It will be recalled that p is defined to be 1 or the characteristic of K according as that characteristic is 0 or not, while a bad prime is one which divides some coefficient of the highest root of some simple component of G. For the simple groups, the bad primes are: 2 for all types except A_n, 3 for all exceptional types, and 5 only for the type E_8; and the central primes (all of which occur if G is simply connected and none if G is adjoint) are: all primes dividing $n+1$ for type A_n, 2 for types $B_n,\ C_n,\ D_n$ and E_7, and 3 for type E_6.

Chatterjee [**C**, Theorem C] has proved this result under the restriction that $p = 1$, i.e., that char $K = 0$. Our proof is considerably simpler than his, in part because his proof is imbedded in a development in which a number of other interesting results are obtained. Following his general approach, we base our proof of Theorem 1 on the following result (see [**C**, Theorem 4.1]).

Theorem 2. *Let G be an arbitrary (linear) algebraic group and assume, as in Theorem 1, that n is prime to p. Then P_n is surjective on G if and only if n is prime to $|Z_G(u)/Z_G(u)^0|$ for every unipotent element u of G.*

We call attention also to Proposition 4 below in which a necessary and sufficient condition for the surjectivity of P_n on the set of semisimple elements of an algebraic group is given.

We continue with our proof of Theorem 2 (given in Propositions 3 and 4 below) and conclude with a brief discussion of how Theorem 2 implies Theorem 1. Although the transition proceeds exactly as in [**C**], we want to at least indicate here how the assumptions on n come into play.

To start our development, we prove:

Received December 2, 2002

Proposition 3. *Assume, as in Theorem* 2, *that G is any algebraic group, p is the characteristic exponent of the base field K and n is a positive integer prime to p.*

(a) *If u is any unipotent element of G, there exists a unique unipotent element v of G such that $v^n = u$. Thus P_n is surjective on the unipotent elements of G. Further $Z_G(v) = Z_G(u)$.*

(b) *If x is any element of G and $x = su$ is its Jordan decomposition (so that s and u are its semisimple and unipotent parts), then x is an n^{th} power in G if and only if s is an n^{th} power in $Z_G(u)$.*

(c) *P_n is surjective on G if and only if it is surjective on the semisimple elements of $Z_G(u)$ for every unipotent element u of G.*

Proof. (a) If $p = 1$, this holds (as in [**C**]) because every unipotent element is contained in a unique 1-parameter subgroup. If $p \neq 1$, then the order of every unipotent element is a power of p. Let q be a power of p so large that $w^q = 1$ for every unipotent w in G, and let a and b be integers such that $an + bq = 1$. Then $v = u^a$ is a unipotent element such that $v^n = u$, and it is unique because from $v^n = u$ it follows that $v = u^a$. Finally, the centralizers $Z_G(u)$ and $Z_G(v)$ are clearly contained in each other. We note that for the surjectivity here, the condition $(n, p) = 1$ is also necessary, at least whenever G has nontrivial unipotent elements, for if it fails, so that p is a prime and p divides n, then any unipotent element of the maximal possible order cannot be an n^{th} power.

(b) Assume that x is an n^{th} power in G, so that $x = y^n$ for some y. Let $y = tv$ be its Jordan decomposition. Then $s = t^n$ and $u = v^n$. Since $t \in Z_G(v)$, it follows from (a) that $t \in Z_G(u)$ and thus that s is an n^{th} power in $Z_G(u)$. Clearly the converse holds.

(c) This follows at once from (b). □

In view of (c), Theorem 2 follows from:

Proposition 4. *If H is any algebraic group and p is the characteristic exponent of the base field K, then P_n is surjective on the semisimple elements of H if and only if n is prime to $|H/H^0|'$, the part of the number $|H/H^0|$ that is prime to p.*

Proof. We use $(*)$ if yH^0 is semisimple as an element of H/H^0, i.e., if its order is prime to p, then $y_s \in yH^0$. Here y_s is the semisimple part of y. Since the morphism of algebraic groups $f : H \to H/H^0$ preserves the Jordan decomposition, $f(y_s) = f(y)_s = f(y)$, the last because $f(y)$ is semisimple. Thus $y_s \in yH^0$ and $(*)$ holds. Now assume in Proposition 4 that P_n is surjective on the semisimple elements of H. Then by $(*)$ it is also surjective on the elements of H/H^0 of orders prime to p. Thus $(**)$ n is prime to $|H/H^0|'$, which proves the easy half of our proposition.

Consider the converse, where it is assumed that $(**)$ holds. Let s be any semisimple element of H and m its order in H/H^0. Then m divides $|H/H^0|$ and it is prime to p because s is semisimple. Thus $(m,\ n) = 1$ by $(**)$. Assuming,

from now on, only the condition $(m,n)=1$ on s and no condition at all on H, we shall show that s is an n^{th} power in H.

We reduce first to the case in which s^m lies in the center of H^0, by replacing H by $Z_H(s^m)$. This may be done because s^m, since it is in H^0, lies in a torus in H and hence also lies in $Z_H(s^m)^0$.

We next reduce to the case in which H^0 is a torus T. Since s acts, by the conjugation i_s, as a semisimple automorphism of H^0, it stabilizes a maximum torus T [**St**, Theorem 7.5], and we may replace H by $\langle T, s\rangle$, and thus H^0 by T, because s^m lies in T, in fact lies in every maximal torus of H, because it is a semisimple element of the center of H^0.

We next show that P_n is surjective on $Z_T(s)$. Let σ denote conjugation by s, acting on T, so that $Z_T(s)$ is just the set of elements of T that are fixed by σ. We have $\sigma^m = 1$ because $s^m \in T$. Now if $x \in Z_T(s)$ is arbitrary we must find a $t \in Z_T(s)$ such that $t^n = x$. Since T is a torus, there exists $t_0 \in T$ such that $t_0^n = x$. Although σ might not fix t_0, it does fix $t_1 = \prod \sigma^i(t_0)$ $(0 \le i \le m-1)$ and $t_2 = t_0^n = x$. Further, $t_1^n = x^m$ and $t_2^n = x^n$, the first because $\sigma^i(t_0)^n = \sigma^i(t_0^n) = \sigma^i(x) = x$ for every i. Since $(m,n) = 1$, there exist integers a and b such that $am + bn = 1$. Then $t = t_1^a t_2^b$ is fixed by σ and $t^n = x^{am}x^{bn} = x$, as required.

Since $s^m \in Z_T(s)$, it follows from what has just been shown that $s^m = t^n$ for some $t \in Z_T(s)$. Then, with a and b as above, $(t^a s^b)^n = t^{an}s^{bn} = s^{am}s^{bn} = s$. Thus s is an n^{th} power in H, and Proposition 4 and Theorem 2 are completely proved. □

Consider now Theorem 1. The proof given in [**C**] that this result follows from Theorem 2 works in all characteristics and we have nothing new to add to it. Thus we shall discuss it very briefly. One must show, of course, that the primes that occur as divisors of the various numbers $|Z_G(u)/Z_G(u)^0|$ for the groups in Theorem 1 are, aside from p, the bad primes and the central primes. If u is a regular unipotent element of G, one which is contained in a unique Borel subgroup B, it is easy to see that $Z_G(u) = Z(G) \cdot Z_U(u)$ (see [**S-St**, III 3.7(a)]) with U the unipotent radical of B, and then that $|Z(G)|$ divides $|Z_G(u)/Z_G(u)^0|$. Thus the central primes all occur. For the bad primes, other than p, one uses regular unipotent elements of suitably chosen semisimple subgroups of G. That no other primes can occur is a result of Springer [**S-St**, III 3.17], which holds, remarkably, even if the unipotent element u is replaced by a collection of several such elements.

References

[B] A. Borel, *Linear Algebraic Groups*, Second Edition, Graduate Texts in Mathematics, Vol. 126, Springer-Verlag, New York, 1991.

[C] P. Chatterjee, *On the surjectivity of power maps of algebraic groups in characteristic zero*, Math. Res. Lett. **9**, 2002, 741-756.

[S] T. A. Springer, *Linear Algebraic Groups*, Second Edition, Progress in Mathematics, Vol. 9, Birkhuser Boston, Inc., Boston, 1998.

[S-St] T. A. Springer and R. Steinberg, *Conjugacy classes, Seminar on algebraic groups and related finite groups*, Lecture Notes in Mathematics, Vol. 131, Springer, Berlin, 1970, 167-266.

[St] R. Steinberg, *Endomorphisms of linear algebraic groups*, Memoirs Amer. Math. Soc., **80**, 1968.

Department of Mathematics, University of California, Los Angeles, CA 90095-1555, U.S.A.

E-mail address: rst@math.ucla.edu