Algebraic groups over finite fields, a quick proof of Lang's theorem

Peter Müller

September 28, 2001

Abstract

We give an easy proof of Lang's theorem about the surjectivity of the Lang map $g \mapsto g^{-1}F(g)$ on a linear algebraic group defined over a finite field, where F is a Frobenius endomorphism. [1]

Let $G \leq \mathrm{GL}_n(k)$ be a connected linear algebraic group over an algebraic closure k of a finite field. For q a power of the characteristic of k, the endomorphism $[q]$ of $\mathrm{GL}_n(k)$ which raises the entries of $\mathrm{GL}_n(k)$ to the qth power is called the standard Frobenius endomorphism of $\mathrm{GL}_n(k)$. An endomorphism F of G (as algebraic groups) is called a Frobenius endomorphism of G if some power of F is the restriction of $[q]$ to G. The important theorem of Lang [4], in the version used in the theory of finite groups of Lie type, is

Theorem. *The map $g \mapsto g^{-1}F(g)$ is surjective on G.*

The usual argument uses differentials, see [1, 16.4], [2, 3.10], [5, 3.3.16]. In [6], Steinberg gives a different argument avoiding differentials, showing that $g \mapsto g^{-1}F(g)$ is a finite morphism of G to itself.

We give yet another proof, which rests on very basic (and easily proven) properties of algebraic groups. The argument can be used at an early stage in text books on algebraic groups.

Proof. The group G acts morphically from the right on itself, where $g \in G$ sends $x \in G$ to $g^{-1}xF(g)$. By [3, 8.3], there is a closed orbit Ω. Choose $x \in \Omega$. Lang's theorem follows from connectivity of G once we know that Ω has the

---

[1]Primary: 20G40, Secondary: none

same dimension as G, because then $G = \Omega$, so G is also the orbit through 1. By [3, 4.1], we need to show that $g^{-1}xF(g) = x$ has only finitely many solutions $g \in G$. Rewrite this as $f(g) = g$, where $f(g) := xF(g)x^{-1}$. Let m be a positive integer such that F^m is a standard Frobenius endomorphism with $x = F^m(x)$. Let r be the order of the group element $xF(x)F^2(x)\cdots F^{m-1}(x)$. Then $f^{mr}(g) = F^{mr}(g)$ for all $g \in G$. So $f^{mr}(g) = g$ has only finitely many solutions in G, so this is even more true for the equation $f(g) = g$. The claim follows. $\qquad\square$

Remark. It would be interesting to prove the more general Lang-Steinberg theorem in a similar fashion. This theorem (see [6]) states the following: Let σ be an endomorphism of the connected linear algebraic group G over any algebraically closed field, such that σ fixes only finitely many elements of G. Then $g \mapsto g^{-1}\sigma(g)$ is surjective on G.

References

[1] Armand Borel, *Linear algebraic groups*, second ed., Springer-Verlag, New York, 1991.

[2] François Digne and Jean Michel, *Representations of finite groups of Lie type*, Cambridge University Press, Cambridge, 1991.

[3] James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York, 1975, Graduate Texts in Mathematics, No. 21.

[4] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[5] T. A. Springer, *Linear algebraic groups*, Birkhäuser Boston, Mass., 1981.

[6] Robert Steinberg, *On theorems of Lie-Kolchin, Borel, and Lang*, Contributions to algebra (collection of papers dedicated to Ellis Kolchin), Academic Press, New York, 1977, pp. 349–354.

IWR, Universität Heidelberg, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail: Peter.Mueller@iwr.uni-heidelberg.de