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 \( G \leq \text{GL}_n(k) \) 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 \( \text{GL}_n(k) \) which raises the entries of \( \text{GL}_n(k) \) to the \( q \)th power is called the standard Frobenius endomorphism of \( \text{GL}_n(k) \). 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 \( \Omega \). Choose \( x \in \Omega \). Lang’s theorem follows from connectivity of \( G \) once we know that \( \Omega \) has the

¹Primary: 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.

**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 $\sigma$ be an endomorphism of the connected linear algebraic group $G$ over any algebraically closed field, such that $\sigma$ fixes only finitely many elements of $G$. Then $g \mapsto g^{-1}\sigma(g)$ is surjective on $G$.

**References**


IWR, UNIVERSITÄT HEIDELBERG, IM NEUENHEIMER FELD 368, 69120 HEIDELBERG, GERMANY

E-mail: Peter.Mueller@iwr.uni-heidelberg.de

2
The first eight chapters study general algebraic group schemes over a field and culminate in a proof of the Barsotti-Chevalley theorem, realizing every algebraic group as an extension of an abelian variety by an affine group. After a review of the Tannakian philosophy, the author provides short accounts of Lie algebras and finite group schemes. The later chapters treat reductive algebraic groups over arbitrary fields, including the Borel-Chevalley structure theory. Solvable algebraic groups are studied in detail. Prerequisites have also been kept to a minimum so that the book is accessible to The proof involves Kronecker’s theory of pencils and the Lang-Steinberg theorem for algebraic groups. Besides the motivation mentioned above, this problem came up in a recent paper of Guralnick, Larsen and Tiep [7] where a concept of character level for the complex irreducible characters of finite, general or special, linear and unitary groups was studied and bounds on the number of orbits was needed. 1. Introduction 2. Hermitian Matrices over Finite Fields 3. Quivers 4. Algebraic Groups and Descent 5. Orbits 6. Further Remarks References. 1 4 5 7 8 10 12. 1. Introduction. See [5, Lemma 3.1]. We give a quick proof. Lemma 2.1. Let $A \in M_n(q^2)$. Then the following are equivalent. (1) $A$ is similar to a Hermitian matrix.