On Definition of Affine Algebraic Groups

On Definition of Affine Algebraic Groups

Zensho Nakao*

0. Introduction

An affine algebraic group is defined to be an affine algebraic variety possessing an abstract group structure satisfying the condition that the group multiplication and inversion are polynomial maps.

The objective of this paper is to shorten the definition to only one statement that the group multiplication be a polynomial map. Two examples are given in [N] with concrete computation, where it is shown that, when K is an infinite field, the polynomial group multiplications on $G_a(K)$ and $G_m(K)$ make the group inversions polynomial, i.e., algebra homomorphisms $K[X] \rightarrow K[X]$, and $K[X,1/X] \rightarrow K[X,1/X]$, respectively.

1. Notations

If G is an affine group (or variety), then K[G] denotes the coordinate ring of K-valued functions on G; if $m : G \times G \rightarrow G$ is a group multiplication, then we write $m(x,y) = xy$; and for a fixed $x \in G$, m_x denotes a left translation given by $m_x(y) = xy$ for all $y \in G$. Also, for $f \in K[G]$ and $x \in G$, f.x designates a function in K[G] defined by $(f.x)(y) = f(xy)$ for all $y \in G$. If $f : G \rightarrow H$ is a polynomial map of varieties, then $f^* : K[H] \rightarrow K[G]$ denotes the associated K-algebra homomorphism. But if V is a K-vector space, then V^* denotes the dual space of V.

2. The Theorem

Therem. *If* G *is an affine variety possessing a polynomial group multiplication* $m : G \times G \rightarrow G$ *and an abstract group inversion* $i : G \rightarrow G$, *then the group inversion is also a polynomial map, i.e.,* G *is an affine algebraic group.*

Proof. We will proceed in two steps:

(i) There exists an injective polynomial homomorphism from G into a general linear group GL(V) for some finite dimensional K-linear space V.

There is the co-multiplication $m^* : K[G] \rightarrow K[G] \otimes K[G]$ induced by the polynomial group multiplication $m : G \times G \rightarrow G$. For $f \in K[G]$, let $m^*(f) = \Sigma g_i \otimes h_i$, where g_i and h_i are chosen linearly independent. Then for $x,y \in G$, $f(yx) = f(m(y,x)) = \Sigma g_i(y)h_i(x)$, so for any $y \in G$, $f.y = \Sigma g_i(y)h_i$, hence f.y lies in the K-linear span of $\{h_i\}$ and also $h_i \in f.G$ because we can solve the equation $f.y = \Sigma g_i(y)h_i$ for h_i by making $g_i(y_j)$ non-singular for suitable $y_j \in G$. Let $K[G] = K[x_1,\dots,x_n]$ and let V be the K-linear span of $\{x_i.y : y \in G, i = 1,\dots,n\}$. Then V is finite dimensional, is stable under $(m_x)^*$, and generates K[G] as a K-algebra since all $x_i \in V$.

Received : October 10, 1983

*Department of Electronics Engineering and Computer Science
College of Engineering

Define a representation $r : G \to \mathrm{end}(V)$, the algebra of endomorphisms of V, by sending z to $(m_z)^* \mid V$. In fact, we have $(m_z)^* \mid V \in GL(V)$, the general linear group of automorphisms of V. For $(f,y) \in V \times V^*$, let $X_{f,y}$ be the matrix coefficient defined by $X_{f,y}(T) = y(t(f))$ for $T \in \mathrm{end}(V)$. Then $\mathrm{end}(V)$ is an affine variety with coordinate ring $K[\mathrm{end}(V)] = K[X_{f,y} : (f,y) \in V \times V^*]$. Let $D(T)$ be the determinant of $T \in \mathrm{end}(V)$. Then $GL(V)$ is an affine algebraic group with coordinate ring $K[GL(V)] = K[\mathrm{end}(V)]\,[1/D]$.

Now, for $z \in G$, $X_{f,y} \circ r(z) = y(r(z)(f)) = y((m_z)^*(f)) = y(f.z) = y(\Sigma g_i(z)h_i)$(where we set $m^*(f) = \Sigma g_i \otimes h_i$ as before) $= \Sigma g_i(z)y(h_i)$, i.e., $X_{f,y} \circ r = \Sigma y(h_i)g_i \in K[G]$, which means that $r : G \to \mathrm{end}(V)$ is a polynomial map.

We further claim that $r : G \to GL(V)$ is a polynomial map. The polynomial function $D \circ r \in K[G]$ never vanisnes on G, hence it is a unit by Hilbert's Nullstellensatz. So the quotient $1/(D \circ r) \in K[G]$. Since $1/(D \circ r) = (1/D) \circ r$, the claim is established.

(ii) The co-morphism $r^* : K[GL(V)] \to K[G]$ is surjective.

Since V generates K[G], it is enough to show that each element of a basis $\{a_1,\ldots,a_n\}$ of V has a pre-image. Let $\{y_1,\ldots,y_n\}$ be the basis of V^* dual to $\{a_1,\ldots,a_n\}$. Then, for all $T \in GL(V)$, $T(a_i) = \Sigma y_j(T(a_i))a_j$.

Define $b_i \in K[GL(V)]$ by setting $b_i = \Sigma a_j(e)X_{a_i,y_j}$, where e is the identity element of G. Then, for all $T \in GL(V)$, $b_i(T) = \Sigma a_j(e)X_{a_i,y_j}(T) = \Sigma a_j(e)y_j(T(a_i)) = T(a_i)(e)$. But then, for all $z \in G$, $r^*(b_i)(z) = b_i(r(z)) = b_i((m_z)^* \mid V) = (m_z)^*(a_i)(e) = (a_i.z)(e) = a_i(z)$, so $r^*(b_i) = a_i$, i.e., $V \subset r^*(K[GL(V)])$.

Putting (i) and (ii) together, we see that G is isomorphic to r(G) which is a closed affine algebraic subgroup of GL(V). Hence G is algebraic. This completes the proof.

Reference

[N] Z.Nakao, Polynomial Group Laws. II, Proc. Amer. Math. Soc. 80 (1980), 196–200.