A remark on multivalued algebraic groups

Anand Pillay*
University of Leeds, England

December 25, 2007

Abstract

We point out how suitable algebraic n-valued groups (in the sense of Buchstaber) give rise, in a reasonably canonical manner, to algebraic groups. This is proved using the "group configuration theorem" of Hrushovski. In particular this applies to all algebraic 2-valued groups.

1 Introduction and statement of results

Given a set X, $(X)^n$ denotes the family of n-element subsets of X, modified so that we allow elements to have multiplicity > 1. So a typical element of $(X)^n$ could be written as a formal sum $k_1x_1 + ... + k_rx_r$ or as $\{k_1x_1, .., k_rx_r\}$ where $x_1, .., x_r$ are distinct elements of X and $k_1, .., k_r$ are positive integers whose sum is n. We will say that $y \in (X)^n$ contains $x \in X$ if x appears in y with multiplicity ≥ 1.

The notion of an *n-valued group* developed from work of Buchstaber and Novikov in the 1970's. Soon afterwards Buchstaber developed the theory of formal, or local, n-valued Lie groups and introduced the notion of n-valued algebraic group. Since 1993 Buchstaber and E. Rees have collaborated on the topological and algebraic theory of n-valued groups. As defined in [1] an n-valued group is a set X equipped with a distinguished element e, and operations $*$ from $X \times X$ to $(X)^n$ and *inv* from X to X such that:
(i) $x * (y * z) = (x * y) * z$ for any $x, y, z \in X$.

*This work is supported by a Marie Curie Chair

(ii) $e * x = x * e = nx$ for any $x \in X$,
(iii) Both $x * inv(x)$ and $inv(x) * x$ contain e.

Possibly (i) (associativity) needs some explanation: by $x * (y * z)$ we mean the obvious element of $(X)^{n^2}$, and likewise for $(x * y) * z$. So (i) says that these elements of $(X)^{n^2}$ are equal.

Note that a 1-valued group $(G, \cdot, inv)$ is the same thing as a group, and can also be considered as an n-valued group $(G, *)$ by writing $a * b = n(a \cdot b)$.

There are reasonably obvious notions of an algebraic n-valued group. Note that if X is an (irreducible) algebraic variety, then so is $(X)^n = X^n/S_n$ (where S_n is the symmetric group acting naturally on X^n). So we could view an algebraic n-valued group as an algebraic variety, equipped with morphisms $\mu : X \times X \to (X)^n$ and $inv : X \to X$ and distinguished element e such that writing $\mu(x, y)$ as $x * y$, $(X, *, inv, e)$ is an n-valued group. Alternatively we could view the operation $*$ as given by a subvariety Γ of $X \times X \times X$; namely for $a, b \in X$, $\Gamma(a, b, z)$ is a 0-dimensional subvariety of X whose set of points, counted with multiplicities, is precisely $a * b$. In fact even assuming only $*$ to be definable would be enough for our purposes.
We will just consider the case where the underlying X is (absolutely) irreducible.

From now on, $(X, *, inv, e)$ is an irreducible algebraic n-valued group, defined over (in the obvious sense) a field k and we will identify X with its set $X(K)$ of K-points for some algebraically closed field K of infinite transcendence degree over k. Let $m = dim(X)$.

We will also be assuming:
(iv) inv is *generically* finite-to-one, or equivalently the regular map $inv : X \to X$ is dominant (the image of inv is Zariski dense).

For A any finite set of finite tuples from K, by $dim(A/k)$ we mean the transcendence degree of $k(A)$ over k. A point $a \in X(K)$ is said to be generic over k if $dim(a/k) = m$ (the dimension of the algebraic variety X). Similarly for mutually generic etc. By k^{alg} we mean the algebraic closure of k (inside some fixed given algebraically closed field).

We will say that X is generically of type $(k_1, .., k_r)$ if for some, equivalently any, $a, b \in X$, which are mutually generic over k, $a * b = \{k_1x_1, ..., k_rx_r\}$ (with the x_i distinct). Our main result is:

Proposition 1.1. *Suppose that X is generically of type $(1, 1, ..., 1)$ Then there is a connected algebraic group $(G, \cdot, e')$ of dimension m, and a con-*

structible subset R of $X \times G$, such that
(a) R projects dominantly onto both X and G,
(b) for any $x \in X$ there are at most finitely many $g \in G$ such that $(x, g) \in R$ and dually (so in particular the dimension of the Zariski closure of R is m),
(c) $(e, e') \in R$,
(b) for mutually generic (x, g) and (y, h) in R then there is $z \in x * y$ such that $(z, g \cdot h) \in R$,
(c) for generic $(x, g) \in R$, $(inv(x), g^{-1}) \in R$.

Remark 1.2. *(i) So R is the graph of a correspondence between X and G, and is generically closed under inversion and "multiplication". Can one improve this?*
(ii) The proposition is proved in the next section using Lemma 2.1 and the "group configuration theorem". Lemma 2.1 holds trivially if X is of type (n), hence the proposition holds for all algebraic 2-valued groups.
(iii) With appropriate definitions the proposition is valid for stable n-valued groups.
(iv) G will be unique "up to isogeny".
(v) If G is a connected algebraic group and A a finite group of (rational) automorphisms of G of cardinality n then we obtain an algebraic n-valued group structure on $X = G/A$ (called a coset group by Victor Buchstaber) in the obvious way, and note that it is generically of type $(1, .., 1)$. Hence the proposition applies and recovers G, up to isogeny.
(vi) For which other generic types can one prove the Proposition?

We use mainly the naive language of algebraic geometry, but sometimes also model-theoretic terminology for which the reader is referred to [2].

Thanks to Victor Buchstaber for suggesting that these observations be written up for publication.

2 Proofs.

An important ingredient is the following:

Lemma 2.1. *Under the assumptions of the proposition (X is an irreducible m-dimensional algebraic n-valued group over k of type $(1, .., 1)$ satisfying also (iv)) , let $a, b \in X$ be mutually generic over k, and let $c \in a * b$. Then*
(i) $a \in c * inv(b)$, $b \in inv(a) * c$, and
(ii) $dim(a, b, c/k) = dim(a, b/k) = dim(b, c/k) = dim(a, c/k) = 2m$.

Proof. Let $a * b = \{c_1, .., c_n\}$. Consider $a * (b * inv(b))$. It contains $a * e = na$ (a with multiplicity n). By associativity a appears with multiplicity at least n in $(a * b) * inv(b)$. So $a \in c_i * inv(b)$ for some $i = 1, .., n$. By assumption (iv), $k(b)^{alg} = k(inv(b)^{alg}$, hence $k(a, b)^{alg} = k(c_i, inv(b))^{alg}$ whereby $dim(c_i, inv(b)/k) = 2m$ from which it follows that c_i and $inv(b)$ are mutually generic (over k) elements of X. So a appears with multiplicity 1 in $c_i * inv(b)$. Hence $a \in c_j * inv(b)$ for some $j \neq i$. Repeating the argument, we conclude that c_j and $inv(b)$ are mutually generic, and a appears with multiplicity 1 in $c_j * inv(b)$. Continuing (using the fact that $na \in (a*b)*(inv(b)))$ we conclude that for each $i = 1, .., n$, $a \in c_i * inv(b)$ and c_i and $inv(b)$ are mutually generic elements of X.
Considering instead $(inv(a) * a) * b$ and repeating the argument, we see that for each $i = 1, .., n$, $b \in inv(a) * c_i$, and c_i and $inv(a)$ are mutually generic.

So we obtain (i), and using also that $k(a)^{alg} = k(inv(a))^{alg}$ and $k(b) = k(inv(b))^{alg}$ we obtain (ii). Lemma 2.1 is proved.

We now prove Proposition 1.1. Let a, b be mutually generic in X over k and let $c \in a*b$. The first step is to recover from X the "group configuration". Let $x \in X$ be chosen generic over $k(a, b)$. By associativity $a * ((x * inv(x)) * b) = (a * x) * (inv(x) * b)$. Now c is in the left hand side. So there are $d \in a * x$ and $f \in inv(x) * b$ such that $c \in d * f$. Our configuration consists of the points a, b, c, x, d, f and the "lines" $\{a, b, c\}$, $\{a, x, d\}$, $\{x, b, f\}$, $\{d, f, c\}$. Note that $k(x)^{alg} = k(inv(x))^{alg}$ (by (iv)).

By Lemma 2.1, we have
(*) each noncollinear triple from $\{a, b, c, x, d, f\}$ is independent over k, and each element of each collinear triple is in the algebraic closure of the other two.

So (*) says precisely that the set of points $\{a, b, c, d, f, x\}$ forms a *group configuration* over k in the algebraically closed field K. We can then apply a fundamental theorem of Hrushovski which produces from this data a definable (and thus algebraic) group closely related to X. We refer to Theorem 5.4.5 of [2] for a statement and proof in the case of arbitrary stable theories. In any case, after possibly replacing k by a larger k_1 algebraically independent from $\{a, b, c, d, f, x\}$ over k) we have:

Lemma 2.2. *There is a connected m-dimensional algebraic group $(G, \cdot, ^{-1}, e')$ defined over k and generic points a', b', c' of G over k such that $a' \cdot b' = c'$ and $k(a)^{alg} = k(a')^{alg}$, $k(b)^{alg} = k(b')^{alg}$ and $k(c)^{alg} = k(c')^{alg}$.*

We now find the R from Proposition 1.1. We may use some model-theoretic language later in the proof. First there is no harm in assuming k to be algebraically closed. We can find an automorphism α of K over k which fixes (c, c') and takes (a, a') to (a_1, a_1') where (a_1, a_1') is independent from (a, a', b, b', c, c') over k.
(Namely $dim(a_1, a_1'/k(a, a', b, b', c, c')) = m$). Let $(b_1, b_1') = \alpha(b, b')$.
So
(a) $a' \cdot b' = c'$ and $a_1' \cdot b_1' = c'$, hence $((a_1')^{-1} \cdot a') \cdot b' = b_1'$.
Put $a_2' = (a_1')^{-1} \cdot a'$.
Also
(b) $c \in a * b$ and $c \in a_1 * b_1$.
By Lemma 2.1, $b_1 \in inv(a_1) * c$, so by associativity there is $a_2 \in inv(a_1) * a$ such that $b_1 \in a_2 * b$.
So we have:
(c) $b_1' = a_2' \cdot b'$ and $b_1 \in a_2 * b$.

Lemma 2.3. *$dim(a_2/k) = dim(a_2'/k) = dim(a_2, a_2'/k) = m$, and (a_2, a_2') is independent from each of (b, b') and (b_1, b_1') over k.*

Proof. It is clear from Lemma 2.1 that $dim(a_2/k) = dim(a_2'/k) = m$. Now $(a_2, a_2') \in k(a, a', a_1, a_1')^{alg}$ and (a, a', a_1, a_1') is independent from (b, b') over k. So (a_2, a_2') is independent from (b, b') over k. But $(a_2, a_2') \in k(b, b', b_1, b_1')^{alg}$, and $dim(b_1, b_1'/k(b, b')) = m$. This forces $dim(a_2, a_2'/k)$ to be at most m, so exactly m. The rest of the lemma follows.

Let $V \subseteq X \times G$ be the irreducible algebraic variety over k whose generic point is (b, b'). So (as $(b_1, b_1') = \alpha(b, b')$) (b_1, b_1') is also a generic point of V over k. Note that $dim(V) = m$. Using model-theoretic notation let $p = tp(b, b'/k)$, the "generic type" of V, and so a "realization" of p is precisely a generic point (over k) of V. R will be a kind of "stabilizer" of V or p.

More precisely let $R \subset X \times G$ be the set of (y, y') such that for some (any) realization (d, d') of p independent from (y, y') over k there is (d_1, d_1') realizing p such that $d_1' = y' \cdot d'$, $d_1 \in y * d$, $d \in inv(y) * d_1$ and $y \in d_1 * inv(d)$. Then R is definable (or constructible) over k.

Lemma 2.4. *(i) $(a_2, a_2') \in R$.*
(ii) For any $y \in X$ there are at most finitely many $y' \in G$ such that $(y, y') \in R$, and dually. (Hence using (i) R has dimension m.)
(iii) If $(y, y') \in R$ is generic over k, namely $dim(y, y'/k) = m$, then $(inv(y), y'^{-1}) \in$

R,
(iv) If $(y,y') \in R$ *and* $(y_1,y_1') \in R$ *are mutually generic over* k*, then there is* $z \in y * y_1$ *such that* $(z, y' \cdot y_1') \in R$.

Proof. . (i) is clear by Lemma 2.3 and Lemma 1.1.
(ii) Suppose for a contradiction that $(y,y') \in R$ and $y \notin k(y')^{alg}$. So $dim(y,y'/k) > dim(y'/k)$. Let (d,d') realize p, independently from (y,y') over k. So
(**) $dim(y,y',d/k) > m + dim(y'/k)$.
Let (d_1,d_1') be a realization of p given by the definition above of (y,y') being in R. Hence $dim(y',d,d',d_1,d_1'/k) = m + dim(y'/k)$. But $y \in k(d,d_1)^{alg}$, so $dim(y,y',d,d',d_1,d_1'/k) = m + dim(y'/k)$, contradicting (**).
(iii) follows from Lemma 1.1.
(iv). Let (y,y') and (y_1,y_1') be mutually generic generic elements of R. This means that $dim(y,y',y_1,y_1'/k) = 2m$. Let (d,d') realize p independently of (y,y',y_1,y_1') over k. Let (d_1,d_1') be a realization of p witnessing that $(y,y') \in R$ (namely $d_1' = y' \cdot d'$, $d_1 \in y * d$ etc.). Then (d_1,d_1') is independent of (y,y',y_1,y_1') over k so again we find (d_2,d_2') realizing p witnessing that $(y_1,y_1') \in R$ (namely $y_2' = y_1' \cdot d_1'$ etc..). It is easy to see that (d,d') and (d_2,d_2') are independent over k. Note that $(y_1' \cdot y') \cdot d' = d_2'$. Also by associativity of $*$, there is $z \in y_1 * y$ such that $d_2 \in z * d$. The same argument as in the proof of Lemma 2.3 shows that $(z, y_1' \cdot y')$ is independent from (d,d') over k. Hence $(z, y_1' \cdot y') \in R$, as required.

Lemma 2.4 finishes the proof of Proposition 1.1. Note that as a_2, a_2' are generic points of X, G respectively over k, then part (i) of Lemma 2.4 gives that R projects dominantly to both X and G. Also it is immediate that $(e,e') \in R$.

References

[1] V.M. Buchstaber, n-valued groups: theory and applications, Moscow Math. Journal, vol. 6, no. (2006), 57-84,

[2] A. Pillay, Geometric Stability Theory, OUP, 1996.