

Affine Nash groups over real closed fields

Ehud Hrushovski*

Hebrew University of Jerusalem

Anand Pillay†

University of Leeds

April 28, 2011

Abstract

We prove that a semialgebraically connected affine Nash group over a real closed field R is Nash isogenous to the semialgebraically connected component of the group $H(R)$ of R -points of some algebraic group H defined over R . In the case when $R = \mathbb{R}$ this result was claimed in [5], but a mistake in the proof was recently found, and the new proof we obtained has the advantage of being valid over an arbitrary real closed field. We also extend the result to not necessarily connected affine Nash groups over arbitrary real closed fields.

1 Introduction and preliminaries

The Nash category lies in between the real algebraic and real analytic categories. Nash functions are by definition both semialgebraic and analytic. In so far as Nash manifolds are concerned, the relevant transition functions should be Nash, and one also requires a finite covering by charts which are open semialgebraic subsets of \mathbb{R}^n . A Nash manifold is said to be *affine* if it is Nash embeddable in some \mathbb{R}^n . If X is the set of real points of some nonsingular quasiprojective algebraic variety defined over \mathbb{R} then X is an affine Nash manifold. Conversely the *algebraicity theorem* (see Proposition 8.4.6 of [2]) says that any affine Nash manifold is Nash isomorphic to a connected component of a nonsingular real algebraic variety. There is a considerable

*Supported by ISF

†Supported by EPSRC grant EP/I002294/1

literature on affine Nash manifolds but less on (abstract) Nash manifolds, although the latter were also considered in the pioneering paper of Artin and Mazur [1] and later in Shiota’s comprehensive monograph [7].

A Nash group is a Nash manifold with Nash group structure. In [5] we purported to prove an “equivariant” version of the algebraicity theorem by showing that a connected affine Nash group is Nash isogeneous to the connected component of a real algebraic group. Recently a mistake was pointed out by Elias Baro. We are not sure whether the proof in [5] can be salvaged, but we will give here a somewhat different and more direct proof, which also works over arbitrary real closed fields. This is done in section 2. In section 3 we give a version for not necessarily connected (affine) Nash groups: if G is a Nash group whose connected component is affine then G is Nash isogenous with a subgroup of finite index in a real algebraic group. We also carry this out at the level of real closed fields.

We would first like to thank Elias Baro who pointed out the precise mistake in [5] as well as suggesting that our new proof should work over any real closed field. In this connection we should also mention Margarita Otero who also had pointed out some gaps in the proof in [5] which until recently we thought we could fill easily. Secondly, thanks to Sun Binyong, for asking us about the generalization to the case of non connected affine Nash groups and for his commentary on the proof described to him by the first author.

We now give some definitions and facts, with [2] as a basic reference. We will work over an arbitrary real closed field R , a special case being when $R = \mathbb{R}$. If U is an open semialgebraic subset of R then by a Nash function $f : U \rightarrow R$ we mean a function which is semialgebraic and infinitely differentiable, in the obvious sense. When $R = \mathbb{R}$ this amounts to f being (real) analytic and satisfying a polynomial equation $P(\bar{x}, f(\bar{x})) = 0$ on U . The definition of an abstract Nash manifold over R , of Nash maps between such Nash manifolds, and hence of a Nash group over \mathbb{R} is unproblematic. But there does not seem to be a systematic treatment of “differential geometric” properties of such abstract Nash manifolds when R is not the reals. So we will take as our *definition* of an “affine Nash manifold” that of a *d-dimensional Nash submanifold M of R^n* from [2] (Definition 2.9.9). M should be a semialgebraic subset of R^n with the following property: for every $a \in M$ there is an open semialgebraic neighbourhood U of 0 in R^n and an open semialgebraic neighbourhood V of a in R^n , and a Nash diffeomorphism ϕ between U and V such that $\phi((R^d \times \{0\}) \cap U) = M \cap V$.

A Nash function or mapping f from M to R is by definition a semial-

gebraic function such that for every ϕ as above the map $f \circ \phi$ restricted to $R^d \times \{0\} \cap U$ is Nash (considered as a mapping from a semialgebraic open subset of R^d to R). Note that in particular the coordinate functions on M are Nash. We deduce easily the notion of a Nash mapping from M to N where M, N are affine Nash manifolds.

A Nash submanifold M of R^n has a topology induced from R^n and we call it *semialgebraically connected* if we cannot write M as the disjoint union of two nonempty open semialgebraic subsets. In general an affine Nash manifold is the disjoint union of finitely many definably connected components, each of which is also an affine Nash manifold.

By an *affine Nash group* G we mean an affine Nash manifold with a group structure such that the multiplication and inversion maps, from $G \times G \rightarrow G$ and $G \rightarrow G$ respectively are Nash maps. If G is an affine Nash group then G^0 denotes the semialgebraically connected component of the identity, also an affine Nash group.

The notions of a *real algebraic variety* and *affine real algebraic variety* over R as well as regular maps between them are discussed in detail in section 3 of [2]. We will call these R -algebraic varieties and affine R -algebraic varieties. An R -algebraic group is an R -algebraic variety with group structure (product, inversion) given by regular maps. A key difference with usual algebraic geometry (over an algebraically closed field) is that projective n -space over R , $\mathbb{P}_n(R)$, is (biregularly isomorphic to) an affine R -algebraic variety (Theorem 3.4.4 of [2]). A consequence is that if X is a quasiprojective algebraic variety over R (or defined over R) in the usual sense, then the set $X(R)$ of R -points of X is (naturally) an affine R -algebraic variety. On the face of it $X(R)$ need not be Zariski dense in X , but replacing X by the Zariski closure of $X(R)$ in X , we can always assume Zariski-density of $X(R)$. As algebraic groups are quasiprojective it follows that if G is an algebraic group defined over R then $G(R)$ is an affine R -algebraic group, in particular an affine Nash group over R .

If H is an \mathbb{R} -algebraic group then H^0 as well as finite covers of H , will be affine Nash groups but not necessarily \mathbb{R} -algebraic groups. Likewise over any real closed field R . So the most one can expect to prove is that an affine Nash group G is Nash isogenous to a union of semialgebraic connected components of an R -algebraic group (which is what we prove). Moreover it suffices to prove that there is a Nash homomorphism f with finite kernel from G into some R -algebraic group H , because then $f(G)$ will have finite index in its Zariski closure (an R -algebraic subgroup of H).

Although the role of model theoretic ideas in this paper is somewhat suppressed, we say a few words. A *semialgebraic* subset X of R^n is the same thing as a set which is (first order) definable (with parameters) in the structure $(R, +, \cdot, <)$ (because of quantifier elimination). By a semialgebraic function f between semialgebraic sets we mean simply a function whose graph is semialgebraic, so we make no continuity assumption. (But any semialgebraic function is “piecewise Nash”.) By a semialgebraic group we mean a semialgebraic set with semialgebraic group operation. Nash groups (affine or otherwise) are semialgebraic groups and moreover any semialgebraic homomorphism between Nash groups is Nash. A result in [6] (together with the above-mentioned piecewise Nashness of semialgebraic functions) implies that any semialgebraic group is semialgebraically isomorphic (as a group) to a (not necessarily affine) Nash group. However there are many semialgebraic groups which are not semialgebraically isomorphic to *affine* Nash groups: Fix $a > 0$ in R then the semialgebraic group with universe the interval $[0, a)$ and with group operation addition modulo a is a well-known such example. A rather new kind of example appears in [3], see 2.10 there. It seems not too unreasonable at the current time to aim towards a fairly explicit description of all semialgebraic groups over real closed fields (up to semialgebraic isomorphism), starting from the R -algebraic groups and iterating some basic constructions.

We will be making use of the notion of the *dimension* of a semialgebraic set $X \subseteq R^n$. See section 2.8 of [2] or any model theory text such as [4].

Definition 1.1. *Let M be an affine Nash manifold. By a Nash subset of M we mean the common zero set of finitely many Nash functions $f : M \rightarrow R$.*

So a Nash subset of M is a special case of a semialgebraic subset of M .

An important fact for us will be:

Lemma 1.2. *Let M be an affine Nash manifold. Then we have the descending chain condition on Nash subsets of M : there is no infinite strictly descending chain $X_1 \supset X_2 \supset \dots$ of Nash subsets of M .*

Proof. This is given by Proposition 8.6.2 of [2] that the common zero set in M of an ideal I in the ring of Nash functions on M , is the common zero set of finitely many functions in I . \square

Remark 1.3. *Let $M \subset R^n$ be an affine Nash manifold of dimension d . Then the Zariski closure of M in R^n has dimension d .*

2 Algebraicity of semialgebraically connected affine Nash groups

Remember that R denotes an arbitrary real closed field.

We prove:

Theorem 2.1. *Let G be a semialgebraically connected affine Nash group over R . Then G is Nash isogenous to the semialgebraic connected component of the identity of some R -algebraic group $H(R)$. Equivalent there is a Nash homomorphism with finite kernel of G into some R -algebraic group $H(R)$.*

The strategy is as in the purported proof in [5] in the case $R = \mathbb{R}$.

Step I, which does not make use of affineness, is to find a (connected) algebraic group H over R and a local Nash isomorphism between G and $H(R)$. By a local Nash isomorphism between G and $H(R)$ we mean some Nash diffeomorphism f between open semialgebraic neighbourhoods of the identity, U, V of $G, H(R)$ respectively, such that for any $g, h \in U$, if $g \cdot h \in U$, then $f(g \cdot h) = f(g) \cdot f(h)$.

This is precisely Theorem A from [5] the proof of which goes through with no change for an arbitrary real closed field. Model theory, in the guise of the first author's group configuration techniques, played a role in the proof. The reader is referred to section 3, as well as Lemmas 4.8 and Corollary 4.9 of [5].

Step II replaces the "proof of Theorem B" in section 4 of [5] which made use of universal covers of real Lie groups, but had a mistake (proof of the CLAIM on p. 240, in which we implicitly assumed that the image of a discrete subgroup under a continuous homomorphism of Lie group is also discrete).

Let f be the local Nash isomorphism between G and $H(R)$ given by Step I. Note that $G \times H(R)$ is an affine Nash group (in particular an affine Nash manifold). By Lemma 1.2 we have the DCC on Nash subsets of $G \times H(R)$, so in particular any subset Y of $G \times H(R)$ has a "Nash closure": smallest Nash subset of $G \times H(R)$ containing Y . For each open semialgebraic neighbourhood U of the identity of G contained in $\text{dom}(f)$, let $A_U \subset G \times H(R)$ be the graph of the restriction of f to U , and let $B_U \subset G \times H(R)$ be the Nash closure of A_U .

By Lemma 1.2 again $B = \cap_U B_U$ is a finite subintersection, and so of the form B_{U_0} for fixed U_0 which we may assume to be symmetric (i.e. $U_0 = U_0^{-1}$).

Lemma 2.2. $\dim(B) = d = \dim(G) (= \dim(H(R)))$.

Proof. Note that for each U the dimension of A_U is d , and hence by 1.3 the dimension of the Zariski closure of A_U is d . As $A_U \subset B_U \subseteq$ Zariski closure of A_U , it follows that $\dim(B_U) = d$. \square

Lemma 2.3. *B is a subgroup of $G \times H(R)$.*

Proof. Let $U_1 \subseteq U_0$ be a symmetric neighbourhood of the identity in G such that $U_1 \cdot U_1 \subseteq U_0$. We now work in the group $G \times H(R)$.

Claim 1. For any $a \in A_{U_1}$, and $x \in B$, $a \cdot x \in B$.

Proof. Note that $X_a = \{x \in G \times H(R) : a \cdot x \in B\}$ is a Nash subset of $G \times H(R)$ (as B is a Nash subset and the group operation is Nash). But if $x \in A_{U_1}$ then $a \cdot x \in A_{U_0} \subset B_{U_0} = B$. Hence X_a contains A_{U_1} . But $B_{U_1} = B_{U_0} = B$, so X_a contains B as required.

Using Claim 1 we obtain in a similar fashion:

Claim 2. For any $a \in B$ and $x \in B$, $x \cdot a \in B$.

Likewise we see that B is closed under inversion. Hence the Lemma is proved. \square

So B is a semialgebraic subgroup of $G \times H(R)$ of dimension d ($= \dim(G) = \dim(H(R))$). It follows that B^0 is a semialgebraic subgroup of $G \times H(R)^0$ of dimension d , projecting onto each factor. The “kernel” of B , $\{g \in G : (g, e) \in B\}$ and “cokernel” of B , $\{h \in H(R)^0 : (e, h) \in B\}$ are clearly finite, normal (so central) subgroups of G , $H(R)^0$ respectively. Let C denote the cokernel. As we may assume $H(R)^0$ to be Zariski dense in the connected algebraic group H , C is also a finite central subgroup of H . Then H/C is a connected algebraic group defined over R , and we have a semialgebraic isomorphism between $(H/C)(R)^0$ and $H(R)^0/C$. So the isogeny from G onto $H(R)^0/C$ can be identified with a (Nash) isogeny from G onto the (semialgebraic) connected component of $(H/C)(R)$. The proof of 2.1 is complete.

3 The non connected case

This section is devoted to a proof of:

Proposition 3.1. *Let G be an arbitrary (not necessarily semialgebraically connected) affine Nash group over R . Then there is a Nash homomorphism with finite kernel from G into some R -algebraic group $H(R)$.*

Let G^0 be the semialgebraically connected component of G . All we will use is that G^0 is affine Nash. Note that we are free to replace G by G/N for N any finite normal subgroup. Hence by Theorem 2.1 we may assume that $G^0 = H_1(R)^0$ where H_1 is a connected algebraic group defined over R . For $g \in G$, let $\alpha_g : G^0 \rightarrow G^0$ be conjugation by g . The basic idea is to extend each α_g to an R -rational automorphism β_g of H_1 , at the expense of replacing H_1 by an isogenous algebraic group defined over R . It will then be easy to construct the required algebraic group H (whose connected component is H_1).

We go through various steps. First we may and will assume that R is of cardinality continuum, by passing to an elementary extension or substructure of R . Hence $R(i)$ is an algebraically closed field of cardinality the continuum, which we can assume to be the field \mathbb{C} of complex numbers. We identify the algebraic group H_1 with its group of complex points $H_1(\mathbb{C})$. Let $\pi : \widetilde{H}_1 \rightarrow H_1$ be the universal cover of H_1 , a simply connected complex Lie group, and Γ the kernel of π , a central discrete subgroup. For $g \in G$, let K_g be the Zariski closure in $H_1 \times H_1$ of the graph of α_g . It is not hard to see that K_g is a connected algebraic subgroup of $H_1 \times H_1$ with finite-to-one projections on each coordinate, and with both “kernel” and “cokernel” being central. Let \widetilde{K}_g be the universal cover of K_g , also a complex Lie group.

Lemma 3.2. (i) \widetilde{K}_g naturally identifies with the graph of an automorphism $\widetilde{\alpha}_g$ of \widetilde{H}_1 , which lifts α_g .

(ii) $\widetilde{\alpha}_g(\Gamma) \cap \Gamma$ has finite index in each of $\widetilde{\alpha}_g(\Gamma)$ and Γ .

(iii) When $g \in G^0$, $\widetilde{\alpha}_g$ acts trivially on $Z(\widetilde{H}_1)$, in particular acts trivially on $\widetilde{\alpha}_h(\Gamma)$ for all $h \in G$.

Proof. (i) The coordinate projections $p_1, p_2 : K_g \rightarrow H_1$ lift to (analytic) isomorphisms p'_1, p'_2 between \widetilde{K}_g and \widetilde{H}_1 , whereby \widetilde{K}_g is the graph of an analytic automorphism of \widetilde{H}_1 .

(ii) By considering $\widetilde{\alpha}_{g^{-1}}$ it suffices to prove that for each g ,

(*) $\widetilde{\alpha}_g(\Gamma) \cap \Gamma$ has finite index in $\widetilde{\alpha}_g(\Gamma)$.

Now $K_g \subset H_1 \times H_1$ has finite cokernel enumerated by \bar{d} say. Let \vec{d} be a lifting of the tuple \bar{d} to a tuple in \widetilde{H}_1 . Let $a \in \Gamma$. Then $\widetilde{\alpha}_g(a) \in \Gamma \cdot \vec{d}$. Hence $\widetilde{\alpha}_g(\Gamma)$ meets only finitely many translates of Γ in \widetilde{H}_1 , yielding (*).

(iii) If $g \in G^0$, then α_g is already a rational map, so the Zariski closure K_g of its graph is still conjugation by g in H_1 . It is easy to see that $\widetilde{\alpha}_g$ is then

conjugation in \widetilde{H}_1 by some (any) lift \widetilde{g} of g , hence acts trivially on $Z(\widetilde{H}_1)$. \square

Corollary 3.3. *Let Γ' be the subgroup of \widetilde{H}_1 generated by the set of $\widetilde{\alpha}_g(\Gamma)$ for $g \in G$. Then Γ is a subgroup of Γ' of finite index.*

Proof. Clearly $\Gamma \subset \Gamma'$, as by Lemma 3.2(iii) $\widetilde{\alpha}_g(\Gamma) = \Gamma$ for $g \in G^0$. Also by 3.2(iii) again, $\widetilde{\alpha}_g(\Gamma)$ depends only on the coset of g modulo G^0 . So, as G^0 has finite index in G , $\{\widetilde{\alpha}_g(\Gamma) : g \in G\}$ is finite, so by Lemma 3.2(ii), Γ has finite index in Γ' . \square

By the Corollary $N = \Gamma'/\Gamma$ is a finite (central) subgroup of H_1 , and the quotient of H_1 by N is a connected algebraic group H_2 , say (which also equals \widetilde{H}_1/Γ'). Let $\tau : H_1 \rightarrow H_2$ be the canonical surjective homomorphism.

Lemma 3.4. (i) *For each $g \in G$, the automorphism $\widetilde{\alpha}_g$ of \widetilde{H}_1 induces an automorphism β_g of $H_2 = \widetilde{H}_1/\Gamma'$.*

(ii) *For any $g \in G$, β_g is a rational automorphism of the algebraic group H_2 , and $(\beta_g \circ \tau)|_{G^0} = (\tau \circ \alpha_g)|_{G^0}$.*

Proof. (i) is clear as Γ' is invariant under each $\widetilde{\alpha}_g$.

(ii) The graph of β_g is clearly the image of K_g under the projection $\tau \times \tau : H_1 \times H_1 \rightarrow H \times H$, hence β is a rational automorphism of H . The second part follows as $K_g|(G^0 \times G^0)$ is the graph of α_g \square

We now use the β_g 's to build a (complex) algebraic group H whose connected component is H_2 . Let g_1, \dots, g_n be representatives of the cosets of G^0 in G . Let $g_i \cdot g_j = h_{ij} \cdot g_r$ where $r = r(i, j)$ and $h_{ij} \in G^0$. Note that the group (G, \cdot) is isomorphic to the set $G^0 \times \{g_1, \dots, g_n\}$ equipped with the group operation $(h, g_i) * (h', g_j) = (h \cdot (\alpha_{g_i}(h')) \cdot h_{ij}, g_{r(i,j)})$, via the map taking $h \cdot g_i$ to (h, g_i) . Let us now *define* the group H to be the set $H_2 \times \{g_1, \dots, g_n\}$ with group operation $(h, g_i) * (h', g_j) = (h \cdot (\beta_{g_i}(h')) \cdot \tau(h_{ij}), g_{r(i,j)})$. Note that H is definable with parameters in $(\mathbb{C}, +, \cdot)$, hence is definably isomorphic to a complex algebraic group (whose connected component is clearly H_2).

Let us now map G to H by the map $f(h \cdot g_i) = (h, g_i)$, and we note that this is a homomorphism with finite (central) kernel (contained in G^0).

At this point we can conclude the proof of Proposition 3.1 in two possible ways.

(A): We have already said that H can be identified with a complex algebraic group. Identifying \mathbb{C} with $R \times R$, we identify H with an R -algebraic group, and we note that f is semialgebraic (hence Nash)

(B): Alternatively we can analyse H_2 and the construction of H to see that H is actually a (complex) algebraic group defined over R and that the homomorphism $f : G \rightarrow H$ is also defined over R , whereby $f : G \rightarrow H(R)$ is the required semialgebraic (in fact Nash) homomorphism with finite central kernel.

The proof of Proposition 3.1 is complete.

References

- [1] M. Artin and B. Mazur, On periodic points, *Annals of Math.*, 81 (1965), 82-99.
- [2] J. Bochnak, M. Coste, M.-F. Roy, *Real Algebraic Geometry*, Springer, 1998.
- [3] A. Conversano and A. Pillay, Connected components of definable groups and o -minimality I, preprint 2011. <http://www.maths.leeds.ac.uk/pillay/>
- [4] L. van den Dries, *Tame topology and o -minimal structures*, LMS Lecture Note Series 248, Cambridge Univ. Press, 1998.
- [5] E. Hrushovski and A. Pillay, Groups definable in local fields and pseudofinite fields, *Israel J. Math.* 85 (1994), 203-262.
- [6] A. Pillay, On groups and fields definable in o -minimal structures, *Journal of Pure and Applied Algebra*, 53 (1988), 239-255.
- [7] M. Shiota, *Nash Manifolds*, Lecture Notes in Mathematics 1269, Springer, 1987.