ISRAEL JOURNAL OF MATHEMATICS 85 (1994), 203–262

GROUPS DEFINABLE IN LOCAL FIELDS AND PSEUDO-FINITE FIELDS

BY

EHUD HRUSHOVSKI*

Department of Mathematics, The Hebrew University of Jerusalem
Givat Ram 91904, Jerusalem, Israel; e-mail: ehud@math.huji.ac.il
and
Department of Mathematics, Massachusetts Institute of Technology
Cambridge, MA 02139, USA

AND

ANAND PILLAY*

Department of Mathematics, University of Notre Dame
Notre Dame, IN 46556, USA;
and
Department of Mathematics, Wesleyan University
Middletown, CT 06457, USA
e-mail: anand.pillay.1@nd.edu

ABSTRACT

Using model-theoretic methods we prove:

THEOREM A: *If G is a Nash group over the real or p-adic field, then there is a Nash isomorphism between neighbourhoods of the identity of G and of the set of F-rational points of an algebraic group defined over F.*

THEOREM B: *Let G be a connected affine Nash group over $\mathbb{R}$. Then G is Nash isogeneous with the (real) connected component of the set of real points of an algebraic group defined over $\mathbb{R}$.*

THEOREM C: *Let G be a group definable in a pseudo-finite field F. Then G is definably virtually isogeneous with the set of F-rational points of an algebraic group defined over F.*

* Both authors supported by NSF grants.
Received October 1, 1992 and in revised form June 15, 1993

Introduction

In this paper we are concerned with groups which are first order definable in the real and p-adics, or in pseudo-finite fields [Fr-J]. Generally, when we say that a group G is **definable in a structure** M, we mean that the universe of G is a first order definable subset of M^n for some n, and that the graph of the group operation of G is a definable subset of M^{3n}. When we speak of **definability** in a field F we mean definability in the structure $(F, +, .)$.

If F is any field, the group $G(F)$ of F-rational points of an (abstract) algebraic group G defined over F is an example of a group definable in F. Conversely, we show here that for suitable fields F, any group H definable in F is closely related (in a definable fashion) to some group $G(F)$ where G is an algebraic group defined over F.

In fact we start off by showing, that under very general hypotheses on F we have a "generic" definable isomomorphism between H and $G(F)$ for suitable G. Additional arguments in the three cases considered here (Theorems A, B and C) yield sharper results: a definable isomorphism between neighbourhoods of the identity in the real and p-adic case, a definable isogeny between H and the connected component of $G(\mathbb{R})$ when H is a connected **affine** real Nash group, and a definable virtual isogeny between H and $G(F)$ when F is a pseudo-finite field.

The version of these results in the case where F is an **algebraically closed** field, namely that a group definable in F is definably (in F) isomorphic to an algebraic group, is well-known to model theorists. This is essentially a consequence of Weil's theorem [W], stating that an algebraic group can be recovered from birational data. Proofs of this were given by van den Dries and Hrushovski (cf [B1]). One can view the present paper as a further extension of Weil's theorem. In fact we will introduce a general class of (pairs) of structures, which we call geometric substructures of strongly minimal sets, and which will provide a general setting for the results of this paper.

We turn now to a more detailed discussion of the main results. Some of the foundational material on Nash manifolds and pseudo-finite fields will be reviewed in sections 4 and 2, respectively.

THEOREM A: *Let F be $\mathbb{R}$ or $\mathbb{Q}_p$. Let G be a Nash group over F. Then there is an algebraic group H defined over F, and a Nash isomorphism between neighbourhoods of the identity of G and $H(F)$.*

It is known [P2,P3] that any group G definable in $F = \mathbb{R}$ or $\mathbb{Q}_p$ be definably equipped with the structure of a real or p-adic Lie group; we refer to groups with a definable Lie structure as real or p-adic Nash groups. (A Nash function is simply a definable analytic function from an open definable subset of F^n ($F = \mathbb{R}$ or $\mathbb{Q}_p$) into F. Nash manifolds and groups arise just like Lie groups but in a category whose morphism are Nash maps.) So Theorem A is really about groups definable in R or $\mathbb{Q}_p$. Once G is equipped with the structure of a Nash group, it becomes in particular a topological group, and hence the statement of the Theorem makes sense. The content of Theorem A is that even though multiplication on G is given by a Nash function, G is, locally, definably isomorphic to a group in which multiplication is given by a rational function. Jim Madden has informed us that Theorem A is related to (and possibly follows from) work by Perrin [Pe] on henselian groups. We should also mention that Madden and Stanton [M-S] have classified all 1-dimensional Nash groups.

Theorem A is, even in the real case, the best possible general result. Namely it is not always possible to lift the local Nash isomorphism to a global Nash isomorphism between G and $H(F)$ (or even to a Nash "virtual isogeny" between G and $H(F)$). An example is where G is $[0, 1)$ with the group operation taken as addition mod 1. G is equipped with Nash group structure by identifying 0 and 1. The problem here is that G (with this Nash structure) admits no nonconstant Nash maps into $\mathbb{R}$, whereas if H is an algebraic group over $\mathbb{R}$ (even a nonlinear one) then $H(\mathbb{R})$ can be Nash embedded into $\mathbb{R}^n$ for suitable n. Theorem B says that this problem is the only obstacle to obtaining global results. We say that G is an affine (real) Nash group if there is a Nash embedding of G into some $\mathbb{R}^n$. By an isogeny between two groups we mean a surjective homomorphism with finite central kernel.

THEOREM B: *Let G be a (topologically) connected real Nash group. Then there is an algebraic group H defined over $\mathbb{R}$ and a Nash isogeny between G and the connected component of $H(\mathbb{R})$.*

The proof of Theorem B involves passing to universal covers and using some facts on commutative real algebraic groups. Theorem B can be viewed as an equivariant version of a classical result of Artin and Mazur [A-M] which states that a connected affine Nash manifold is Nash diffeomorphic to a connected component of a nonsingular real algebraic variety. We conjecture that an analogous

result to Theorem B holds in the p-adic case.

We should mention that if G is centreless then it is rather easy to definably embed G in $\mathrm{GL}(n, F)$ for suitable n, using the adjoint representation. The image of G will then be an open subgroup of its Zariski closure.

The third case we consider is that of pseudo-finite fields. These fields may be characterized in a number of ways. Model-theoretically they are defined as the infinite models of the theory of finite fields. Algebraically they are defined as perfect pseudo algebraically closed fields, with exactly one field extension of an given degree (namely with absolute Galois group the profinite completion of $\mathbb{Z}$). (Here a field F is called pseudo algebraically closed or PAC if any absolutely irreducible variety defined over F has an F-rational point.)

THEOREM C: *Let G be a group definable in a pseudo-finite field. Then there is an algebraic group H defined over F and a definable (in F) virtual isogeny between G and $H(F)$.*

Here by a virtual isogeny between two groups, say G and H, we mean an isogeny between subgroups G_1 of finite index in G and H_1 of finite index in H. In Theorems A and B, there was an intermediate "geometric" category between definable groups and algebraic groups, namely Nash groups. In the case of pseudo-finite fields there is no such obvious geometric category. The proof of Theorem C (namely obtaining some definable virtual isogeny from a "generic" definable relation) requires the use of *stable group theory*. This sounds rather strange as pseudo-finite fields are unstable. However what we use is "local" stability theory, or stability theory with respect to a fixed collection of formulas. This is reviewed in section 5. The theory as developed there can be used to derive results of Nori [No] on subgroups of $\mathrm{GL}(n, \mathbb{F}_p)$, with applications to "strong approximation theorems". This will appear in a subsequent paper by the authors.

It can be shown that Theorem C also holds for perfect PAC fields whose absolute Galois groups are finitely generated as profinite groups, or more generally "small" [Fr-J, p.185]. To see this one must check that such fields fit into the axiomatic framework which we use in this paper: specifically (i) that they are "geometric substructures" of their algebraic closure (see section 2), and (ii) that their class of definable sets has the "S_1-property" (see again section 2). The verification of these facts was carried out in unpublished notes by the first author. However, in this paper we limit ourselves to the special case of pseudo-finite

fields, and we will cite the paper [Ch-vdD-Mac] for the necessary verifications in this case. (i) and (ii) above are there derived from an extension of the Lang–Weil estimates for the number of points on varieties over finite fields.

One delicate point worth mentioning is the distinction between "definable" objects in F and "interpretable" objects in F. An object X (group or otherwise) is **interpretable** in the structure M if X is a definable subset of M^n/E where E is a definable equivalence relation on M^n. When M has "elimination of imaginaries" (discussed below), any interpretable object X is in definable bijection with an object Y **definable** in M (namely Y is a definable subset of M^k, for some k). The first author has verified that perfect PAC fields with "small" Galois group (in particular pseudo-finite fields) have elimination of imaginaries. ("Small" means that the absolute Galois group of the field F has only finitely many continuous homomorphisms into any given finite group.) This adds considerable force to Theorem C : any **interpretable** group is definably virtually isogeneous with the set of F-rational points of an algebraic group defined over F. This form of Theorem C is easily seen not to generalise to arbitrary PAC fields. For let F be a PAC field of characteristic 0 say, such that the set of nth powers $(F^*)^n$ of F^* has infinite index in F^*. The quotient group $G = F^*/(F^*)^n$ is interpretable in F and is an infinite commutative group of exponent n. This clearly excludes G being even abstractly isomorphic to $H(F)$ for H any algebraic group. However we should point out here, to prevent any confusion, that even when F does not have elimination of imaginaries (for example when $F = \mathbb{Q}_p$) the definable/interpretable distinction does not present problems as far as groups of the form $G(F)$ are concerned, where G is an algebraic group defined over F: Identify G with its points in some algebraically closed field $\widetilde{F}$ containing F. G is a not necessarily affine variety. So G is formed by piecing together finitely many affine varieties (each defined over F) with F-definable identifications of suitable Zariski open sets. As such G is an object interpretable, rather than definable, in $\widetilde{F}$. However, as $\widetilde{F}$ has elimination of imaginaries and quantifier-elimination, there is an F-definable bijection between G and some quantifier-free definable group H which is a subset of $(\widetilde{F})^k$ some k. H is no longer a "geometric" object, but it makes sense to speak of $H(F)$, the points of H whose coordinates are in F, and in F there is a definable bijection between $G(F)$ and $H(F)$. Thus we can (up to definable isomorphism) view $G(F)$ as a group **definable** (rather than just interpretable) in F.

We describe now the organisation of this paper. We will proceed at a rather general model-theoretic level, that of "geometric structures" and "geometric substructures of strongly minimal sets". In section 5, we even make an excursion into general stability theory (which is essential for the results on pseudo-finite fields). So as to make the paper accessible to non model-theorists, we will in section 1, present the required model-theoretic background, together with a lexicon for translating between the language of types, canonical bases etc. and that of varieties, fields of definition etc., in the case where the structure we are working in is an algebraically closed field. In section 2 we present the notions of a geometric structure, and geometric substructure of a strongly minimal set, and verify that the fields we are interested in fall into such classes. Again we provide a suitable lexicon. In section 3, we prove a result which lies behind and provides the thread connecting Theorems A, B and C. The result is proved for geometric structures, but in the language of fields it says that for suitable fields F, if G is a group definable in F then there is an algebraic group H defined over F and a definable finite-to-finite relation between certain "generic" points of G and $H(F)$ which respects the respective group laws.

In section 4, we present the necessary background concerning Nash manifolds and groups, and we prove Theorems A and B. In section 5, we introduce "local" stability theory and equivariant stability theory, and study its interaction with geometric structures under suitable hypotheses.

In section 6 we prove Theorem C (again in a general context).

ACKNOWLEDGEMENT: We wish to thank the referee for his helpful suggestions concerning the organisation of this paper and its style.

1. Model-theoretic background

We now present some background which hopefully should enable the non "model-theory specialist" to read this paper. We refer the reader to [P5] for a more extended introduction to model theory and stability theory. We assume knowledge of the notions : first order language L, L-structure M, satisfaction of formulas and sentences, elementary equivalence, elementary extension, theories. All structures (or, as we say: **models**) are assumed to be infinite. We use M to denote a model. $A, B, \ldots$ denote subsets of a given model M, a, b, c denote elements of M, and $\boldsymbol{a}, \boldsymbol{b}, \ldots$ denote (finite) tuples from M. (Eventually for various reasons we confuse tuples and elements.) If M is an L-structure and A is a subset of M,

then L_A is the language L augmented by names for the elements of A. We write $Th(M)$ for the complete first order theory of M.

1.1 TYPES AND SATURATION Let M be an L-structure, and $A \subset M$. By a (partial) type $\Psi(\boldsymbol{x})$ over A in the sense of M (where $\boldsymbol{x}$ is a finite tuple of variables) we mean a collection of formulas of L_A with free variables $\boldsymbol{x}$, such that for every finite subset Ψ_1 of Ψ, $M \models (\exists \boldsymbol{x})(\wedge \Psi_1(\boldsymbol{x}))$. The compactness theorem implies that if Ψ is such a partial type, then there is an elementary extension N of M, and some $\boldsymbol{a}$ in N which realises Ψ, namely $N \models \psi(\boldsymbol{a})$ for all $\psi \in \Psi$. $\Psi(\boldsymbol{x})$ as above is said to be a complete type over A, if for every $\psi(\boldsymbol{x}) \in L_A$, either ψ or its negation $\neg\psi$ is in Ψ. $S(A)$ denotes the set of complete types over A (this depends on M or rather the theory of M with names for elements of A). Complete types are often denoted p, q etc. If $\boldsymbol{a}$ is in M, then $\mathrm{tp}_M(\boldsymbol{a}/A)$ (or just $\mathrm{tp}(a/A)$ if M is understood) is the set of L_A formulas $\psi(\boldsymbol{x})$ such that $M \models \psi(\boldsymbol{a})$ (which is clearly a complete type over A).

M is said to be **κ-saturated** (where κ is an infinite cardinal), if for every $A \subset M$ with $|A| < \kappa$, and every type $\Psi(\boldsymbol{x})$ over A (in the sense of M), Ψ is already realised by a tuple in M. We will call a model M **saturated** if M is $|M|$-saturated. We will assume that any structure M has saturated elementary extensions of arbitrarily large cardinality. A sufficiently saturated model plays the role of a "universal domain". One of the other benefits of working in a saturated model is that if M is saturated, A is a small subset of M (namely $|A| < |M|$), and $\boldsymbol{a}, \boldsymbol{b}$ are tuples in M (of the same length) then $\mathrm{tp}(\boldsymbol{a}/A) = \mathrm{tp}(\boldsymbol{b}/A)$ iff there is an automorphism of M which fixes A pointwise and takes $\boldsymbol{a}$ to $\boldsymbol{b}$.

A **definable set** in M is a subset X of M^n (some $n < \omega$) such that for some formula $\psi(\boldsymbol{x})$ of L_M, $X = \{\boldsymbol{a} \in M^n : M \models \psi(\boldsymbol{a})\}$. We call the set X **A-definable** if such a formula ψ can be chosen in L_A. In particular X is **$\emptyset$-definable** if it is definable by a formula with no auxiliary parameters. If M is saturated, X is a definable set, and A is a small subset of M, then X is A-definable iff X is fixed setwise by every automorphism of M which fixes A pointwise. We often identify formulas with the sets they define.

Sometimes we are interested in certain special partial types. For example, by $\mathrm{qftp}(\boldsymbol{a}/A)$ we mean the set of quantifier-free formulas of L_A satisfied by $\boldsymbol{a}$ in M.

If a model M is fixed by the context, we use $\models \cdots$ to denote truth in M. If $\Psi(\boldsymbol{x})$ is a partial type over a small subset of M, and $\varphi(\boldsymbol{x})$ is a formula over M, by $\Psi(\boldsymbol{x}) \vdash \varphi(\boldsymbol{x})$ we mean that for any elementary extension N of M and $\boldsymbol{a}$ in N,

if $N \models \Psi(\boldsymbol{a})$, then $N \models \varphi(\boldsymbol{a})$.

1.2 ALGEBRAICITY AND DEFINABILITY If $A \subset M$ and $\boldsymbol{a} \in M$, we say that $\boldsymbol{a}$ is in the **algebraic closure** of A (in M), written $\boldsymbol{a} \in \operatorname{acl}(A)$, if there is a formula $\varphi(\boldsymbol{x})$ over A (namely of L_A) such that $M \models \varphi(\boldsymbol{a})$, and moreover such that $\varphi(\boldsymbol{x})$ has only finitely many solutions in M (the latter is clearly expressed by an L_A-sentence).

We say that $\boldsymbol{a}$ is in the **definable closure** of A, $\boldsymbol{a} \in \operatorname{dcl}(A)$, if for some L_A-formula $\varphi(\boldsymbol{x})$, $\boldsymbol{a}$ is the unique solution of φ in M. Note that both acl(-) and dcl(-) are idempotent operators. A set of tuples $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\}$ from M is said to be **algebraically independent over** A (where $A \subset M$) if for each i, $\boldsymbol{a}_i \notin \operatorname{acl}(A \cup \bigcup\{\boldsymbol{a}_j : j \neq i\})$.

1.3 M^{eq} Knowledge of M^{eq} is not essential to this paper, but is useful anyway. Let M be an L-structure. M^{eq} is a many sorted structure in a language L^{eq} obtained in a canonical fashion from L and M as follows. For each $\emptyset$-definable equivalence relation E on M^n, let S_E be a new sort. The interpretation of the sort S_E in M^{eq} is simply the set M^n/E.

In particular M itself is the interpretation of the sort $S_=$. L sits inside L^{eq}, with all the relations and functions of L restricted to the sort $S_=$. In addition, L^{eq} will contain for each E as above, a function symbol f from n-tuples of sort $S_=$ to sort S_E, the interpretation in M^{eq} being $f(\boldsymbol{a}) = \boldsymbol{a}/E$.

The theory of M^{eq} is determined by the theory of M, $T = \operatorname{Th}(M)$. So $\operatorname{Th}(M^{\mathrm{eq}})$ is denoted T^{eq}. All properties of T pass to T^{eq}. M can be viewed as either an L-structure, or as the interpretation of the sort $S_=$ in the L^{eq}-structure M^{eq}. These amount to the same thing in every possible sense.

M is said to have **elimination of imaginaries** if for any $c \in M^{\mathrm{eq}}$ there is some tuple $\boldsymbol{b}$ from M such that in M^{eq}, $c \in \operatorname{dcl}(\boldsymbol{b})$ and $\boldsymbol{b} \in \operatorname{dcl}(c)$ (we say c and $\boldsymbol{b}$ are interdefinable). This property could also be expressed without passing to M^{eq}: assuming M saturated, M has elimination of imaginaries iff for every definable set X in M there is a tuple $\boldsymbol{a}$ from M such that any automorphism of M fixes X setwise iff it fixes $\boldsymbol{a}$. M has weak elimination of imaginaries, if for every $c \in M^{\mathrm{eq}}$ there is some tuple $\boldsymbol{b}$ from M such that $c \in \operatorname{dcl}(\boldsymbol{b})$ and $\boldsymbol{b} \in \operatorname{acl}(c)$. If M has elimination of imaginaries then any definable set in M^{eq} is in definable bijection with a definable subset of some M^k.

It is known that any algebraically closed field $(K, +, .)$ has elimination of

imaginaries. If A is a subset of M (or even of M^{eq}), by $\mathrm{acl}^{\mathrm{eq}}(A)$ we mean $\{a \in M^{\mathrm{eq}}: a \in \mathrm{acl}(A)\}$.

1.4 STRONGLY MINIMAL SETS A structure M is said to be **strongly minimal** if for any elementary extension N of M, any definable subset X of N is finite or cofinite (in N). (This notion was introduced by Baldwin and Lachlan [BL], but the reader should also see [P5].) If M were already ω-saturated, it would be unnecessary to pass to elementary extensions in the above definition. It is known that algebraic closure behaves very nicely in a strongly minimal structure M: if $A \cup \{a, b\} \subset M$, and $b \in \mathrm{acl}(A \cup \{a\}) \setminus \mathrm{acl}(A)$ then $a \in \mathrm{acl}(A \cup \{b\})$. We say that acl(-) defines a **pregeometry** on M (we already have transitivity). It follows that if $A \subset M$, and $\boldsymbol{a}$ is a tuple from M, then any two maximal A-algebraically independent subsets of $\bigcup \boldsymbol{a}$ have the same cardinality, which we call $\dim(\boldsymbol{a}/A)$. This clearly depends only on $p = \mathrm{tp}(\boldsymbol{a}/A)$, so we also call this number $\dim(p)$. We should remark that if A is a subset of M^{eq} and $a, b \in M$ then still we have that $b \in \mathrm{acl}(A \cup \{a\}) \setminus \mathrm{acl}(A)$ implies $a \in \mathrm{acl}(A \cup \{b\})$ in M^{eq}. Thus if $\boldsymbol{a}$ is a tuple from M and $A \subset M^{\mathrm{eq}}$ then $\dim(\boldsymbol{a}/A)$ still makes sense. Note that $\dim(\boldsymbol{ab}/A) = \dim(\boldsymbol{a}/A\boldsymbol{b}) + \dim(\boldsymbol{b}/A)$. We say that $\boldsymbol{a}$ is **independent** from $\boldsymbol{b}$ over A if $\dim(\boldsymbol{a}/A\boldsymbol{b}) = \dim(\boldsymbol{a}/A)$ (iff $\dim(\boldsymbol{b}/A\boldsymbol{a}) = \dim(\boldsymbol{b}/A)$, by the previous sentence). We will also express this independence by saying that $\mathrm{tp}(\boldsymbol{a}/\boldsymbol{b}A)$ **does not fork over** A. More generally we will say $\mathrm{tp}(\boldsymbol{a}/B)$ **does not fork over** A if $\dim(\boldsymbol{a}/B) = \dim(\boldsymbol{a}/A)$.

Note that if $A \subset M$ (or even M^{eq}) and both $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_n\}$ are A-algebraically independent subsets of M, then

$$\mathrm{tp}(a_1, \ldots, a_n/A) = \mathrm{tp}(b_1, \ldots, b_n/A).$$

(This follows from the definitions, by induction on n.)

This dimension theory can be extended to M^{eq} as follows: let $a \in M^{\mathrm{eq}}$, and let A be some subset of M^{eq}. Then we can clearly find $b_1, \ldots, b_n \in M$, such that $\{b_1, \ldots, b_n\}$ is A-algebraically independent, $a \in \mathrm{acl}(b_1, \ldots, b_n, A)$ and $\{b_1, \ldots, b_n\}$ is minimal such. Without loss of generality $\{b_1, \ldots, b_r\}$ is $A \cup \{a\}$-algebraically independent (and hence a is interalgebraic with $(b_{r+1}, \ldots, b_n)$ over $A \cup \{b_1, \ldots, b_r\}$). We then define $\dim(a/A)$ to be $n - r$. Again we say $\mathrm{tp}(a/B)$ does not fork over A, or a is independent with B over A, if $\dim(a/B) = \dim(a/A)$.

1.5 DIMENSION OF DEFINABLE SETS Let us assume M to be strongly minimal and saturated. From the definitions it follows easily that if $\psi(x, \boldsymbol{y})$ is an L-formula

then there is a L-formula $\delta(\boldsymbol{y})$ such that for any $\boldsymbol{b}$ in M, $\psi(x, \boldsymbol{b})$ defines an infinite subset of M iff $M \models \delta(\boldsymbol{b})$. ($\delta(\boldsymbol{y})$ just says that there are at least k solutions x of $\psi(x, \boldsymbol{y})$, for some suitably large k, depending on the formula ψ.) Iterating this observation, we see that if $\psi(x_1, \ldots, x_n, \boldsymbol{y})$ is an L-formula, then there is again an L-formula $\delta(\boldsymbol{y})$ such that for any $\boldsymbol{b}$ in M, $M \models \delta(\boldsymbol{b})$ if and only if "for infinitely many x_1 (for infinitely many x_2(....(for infinitely many $x_n(\psi(x_1, \ldots, x_n, \boldsymbol{b}))$...))". So clearly $\delta(\boldsymbol{b})$ holds iff for any small set B containing $\boldsymbol{b}$ there is an n-tuple $\boldsymbol{a}$ from M such that $M \models \psi(\boldsymbol{a}, \boldsymbol{b})$ and $\dim(\boldsymbol{a}/B) = n$. We say in this situation that $\dim(\psi(\boldsymbol{x}, \boldsymbol{b})) = n$, or equivalently $\dim(X) = n$, where X is the subset of M_n defined by $\psi(\boldsymbol{x}, \boldsymbol{b})$.

We in general define $\dim(\psi(x_1, \ldots, x_n, \boldsymbol{b})) = \dim(X)$ to be the greatest $k \leq n$ such that for some projection (existential quantification) Y of the X defined by $\psi(\boldsymbol{x}, \boldsymbol{b})$ onto M^k, $\dim(Y) = k$. Then it can be checked there is again some $\delta(\boldsymbol{y})$ depending on ψ and k such that for any $\boldsymbol{b}$, $M \models \delta(\boldsymbol{b})$ iff $\dim(\psi(\boldsymbol{x}, \boldsymbol{b})) = k$. (We use here that algebraicity over a set is witnessed by a formula.) If X is a definable subset of M^n, then it can be seen that for any $A \subset M$ over which X is defined, $\dim(X) = \max\{\dim(\boldsymbol{a}/A)\colon \boldsymbol{a} \in X\}$.

We will typically say that $\boldsymbol{a}$ is a **generic** point of X over A, if X is A-definable, $\boldsymbol{a} \in X$ and $\dim(X) = \dim(\boldsymbol{a}/A)$. Also the dimension of a finite disjunction of formulas is the maximum of the dimensions of the disjuncts.

If p is a complete n-type over A, $\dim(p)$ is clearly $\min\{\dim(\psi)\colon \psi \in p\}$. By compactness and previous observations, if p is a complete type over A, and $A \subset B$, then there is some $\boldsymbol{a}$ realising p such that $\boldsymbol{a}$ is independent with B over A (i.e. $\dim(\boldsymbol{a}/B) = \dim(\boldsymbol{a}/A) = \dim(p)$).

These considerations also apply to definable sets and types in M^{eq}.

In a similar fashion we can define $\dim(\Psi(\boldsymbol{x}))$ for $\Psi(\boldsymbol{x})$ a partial type.

1.6 MULTIPLICITY AND CANONICAL BASES We continue with the assumptions of 1.5. Let p be a complete type over A. Let $A \subset B$. Then the uniqueness assertion at the end of 1.4 implies that the set $\{\mathrm{tp}(\boldsymbol{a}/B)\colon \boldsymbol{a}$ realises p and $\boldsymbol{a}$ is independent from B over A (namely $\dim(\boldsymbol{a}/B) = \dim(\boldsymbol{a}/A) = \dim(p)$)$\}$ is finite, and moreover has size bounded by some number k, depending on p and not B. The least such number k (as B varies) is called the multiplicity of p, denoted $\mathrm{mult}(p)$. p is said to be stationary if $\mathrm{mult}(p) = 1$.

Multiplicity is witnessed again by a formula:

If X is a definable subset of M^n with $\dim(X) = m$, then by $\mathrm{mult}(X)$ we

mean the greatest k such that X can be partitioned into k definable sets, each of dimension m.

One can then show that, if $\dim(p) = m$, then $\text{mult}(p) = \min\{\text{mult}(\psi(\boldsymbol{x}) : \psi \in p \text{ and } \dim(\psi) = m\}$. Note that if the A-definable set $X \subset M^n$ has dimension m and multiplicity 1, then for any two generic points $\boldsymbol{a}, \boldsymbol{b}$ in X, $\text{tp}(\boldsymbol{a}/A) = \text{tp}(\boldsymbol{b}/A)$.

Now suppose $p \in S(A)$ is stationary, and let $\psi(\boldsymbol{x}, \boldsymbol{b}) \in p$ with $\dim(\psi(\boldsymbol{x}, \boldsymbol{b})) = \dim(p) = m$ say, and $\text{mult}(\psi(\boldsymbol{x}, \boldsymbol{b})) = 1$. Now by the remarks in 1.5, the equivalence relation E defined as

$$\boldsymbol{b}_1 \text{ E } \boldsymbol{b}_2 \quad \text{iff } \dim(\psi(\boldsymbol{x}, \boldsymbol{b}_1) \,\&\, \psi(\boldsymbol{x}, \boldsymbol{b}_2)) = m$$

is $\emptyset$-definable. Thus $\boldsymbol{b}/$ E is an element in M^{eq} (in the sort S_E), and we define the canonical base of p, denoted $\text{Cb}(p)$ to be $\boldsymbol{b}/$ E. This depends formally on the choice of the formula $\psi(\boldsymbol{x}, \boldsymbol{b})$. But if we chose instead $\varphi(\boldsymbol{x}, \boldsymbol{c})$ in p with dimension m and multiplicity 1, then if E′ is the corresponding equivalence relation, we would have that $\boldsymbol{b}/$ E is interdefinable with $\boldsymbol{c}/$ E′. So $\text{Cb}(p)$ is well-defined up to interdefinability. Note $\text{Cb}(p) \in \text{dcl}(A)$. $\text{Cb}(p)$ has the following canonical feature: if C is a subset of M or even M^{eq} then there is some $\boldsymbol{a}$ realising p with $\dim(\boldsymbol{a}/A \cup C) = \dim(\boldsymbol{a}/C) = m(= \dim(p))$, if and only if $\text{Cb}(p) \in \text{acl}(C)$. If also $\text{mult}(\text{tp}(\boldsymbol{a}/C)) = 1$, then even $\text{Cb}(p) \in \text{dcl}(C)$. Now it is a fact that any strongly minimal structure has weak elimination of imaginaries, after naming finitely many parameters (See section 2 of [P7].) In this situation, there is for any complete type p, some tuple $\boldsymbol{c}$ from M such that $\boldsymbol{c} \in \text{acl}(\text{Cb}(p))$, and $\text{Cb}(p) \in \text{dcl}(\boldsymbol{c})$. In addition the "finite equivalence relation theorem" implies that if A is an algebraically closed subset of M, then any $p \in S(A)$ is stationary.

In section 3, we shall be working with a strongly minimal structure M (there called D) which has elimination of imaginaries. In this case $\text{Cb}(p)$ is interdefinable with some tuple from M. Again the considerations in this section also apply to types and defnable sets in M^{eq}.

A group G definable (or even interpretable) in M is said to be (definably) **connected** if $\text{mult}(G) = 1$, or equivalently if G has no definable proper subgroups of finite index.

1.7 ALGEBRAICALLY CLOSED FIELDS, TYPES, AND VARIETIES Let F be an algebraically closed field. The first key fact about F is that $\text{Th}(F)$ has quantifier-elimination in the language $L = \{+, \cdot, -, 0, 1\}$, namely every formula $\varphi(\boldsymbol{x})$ of L is equivalent in F to a quantifier-free formula $\psi(\boldsymbol{x})$. In particular for A a subset of

F and points $\boldsymbol{a}$, $\boldsymbol{b}$, $\mathrm{tp}(\boldsymbol{a}/A) = \mathrm{tp}(\boldsymbol{b}/A)$ iff $\mathrm{qftp}(\boldsymbol{a}/A) = \mathrm{qftp}(\boldsymbol{b}/A)$. Another consequence of quantifier-elimination is that the model- theoretic and field-theoretic algebraic closures coincide, namely if A is a subset of F and $a \in F$ then: $a \in \mathrm{acl}(A)$ in the sense of 1.2 iff a is in the field-theoretic algebraic closure of $F_0(A)$, where F_0 denote the prime field of F, and $F_0(A)$ denotes the field generated by A. If F has characteristic 0 then $a \in \mathrm{dcl}(A)$ (in the sense of 1.2) iff $a \in F_0(A)$. However if $\mathrm{char}(F) = p > 0$ one must also deal with the inverse of the Frobenius, and in this case $\mathrm{dcl}(A) = \{p^{n\text{th}}$ roots of elements of $F_0(A)$: $n < \omega\}$, the "purely inseparable closure" of $F_0(A)$. If κ is an infinite cardinal, then quantifier elimination also implies that F is κ-saturated iff the transcendence degree of F over F_0 is κ.

An affine algebraic variety V included in F^n is of course a definable set, and quantifier elimination means that, conversely, any definable set is a Boolean combination of affine algebraic varieties. In particular every definable subset of F is finite or cofinite, and thus F is strongly minimal. In particular the notions such as dimension, developed in sections 1.4, 1.5 and 1.6 apply. Clearly $\dim(\boldsymbol{a}/A)$ is the same as tr.degree $(F_0(A)(\boldsymbol{a})/F_0(A))$ and so if V is an affine variety, $\dim(V)$ is the same as the algebro-geometric dimension of V.

For V an (affine) variety there is an algebro-geometric notion of V being defined over $K \leq F$. This agrees with the model-theoretic notion in characteristic 0. However in characteristic $p > 0$, V is defined over $K < F$ in the model-theoretic sense iff V is defined over the purely inseparable closure of K in the algebro-geometric sense.

If V is irreducible then V has multiplicity 1. So for any K over which V is defined there is a **unique** type $p(\boldsymbol{x}) \in S(K)$ such that $p(\boldsymbol{x}) \vdash \boldsymbol{x} \in V$ and $\dim(p) = \dim(V)$. In fact $p(\boldsymbol{x})$ is precisely the type of a generic point of V over K, and if F is sufficiently saturated (i.e. has infinite transcendence degree over K) then $p(\boldsymbol{x})$ will be realised in F by some $\boldsymbol{a}$. For such $\boldsymbol{a}$, V in turn is the variety over K generated by $\boldsymbol{a}$, namely the set of points in F_n say, which satisfy all the polynomial equations over K satisfied by $\boldsymbol{a}$. It is well-known that V has a **smallest field of definition** (in the algebro-geometric sense), say K_0. Then K_0 is finitely generated and it turns out that K_0 is precisely the canonical base of $p(\boldsymbol{x})$ in the following sense: let K_0 be generated over the prime field F_0 by the point $\boldsymbol{c}$. Let $d \in F^{\mathrm{eq}}$ be $\mathrm{Cb}(p)$. Then $\boldsymbol{c} \in \mathrm{dcl}(d)$ and $d \in \mathrm{dcl}(\boldsymbol{c})$. In fact F has elimination of imaginaries. This was first observed by Poizat [Po1]. In fact elimination of imaginaries can be deduced from

(i) weak elimination of imaginaries, which holds in any strongly minimal structure in which $\mathrm{acl}(\emptyset)$ is infinite, and

(ii) the fact that unordered sets of tuples can be coded up in fields using symmetric functions.

We will also be considering not necessarily affine varieties and algebraic groups. We assume some familiarity with these objects (and we refer model-theorists to Poizat's expository paper [Po3]). Suffice it to say that an abstract variety is naturally an object interpretable in the algebraically closed field F. The reason we say interpretable rather than definable is because of the equivalence relation which arises from identifying various open subsets of the affine charts of V. The reader should believe that, if V is "defined over" a subfield K of F, then $V(K)$ (the set of K-rational points of V) makes sense and $V(K)$ is interpretable in K. We will often speak of points of V as living in F^n (some n). In this situation we will be working inside some open affine piece of V. On the other hand, by elimination of imaginaries V will be in K-definable bijection with some (quantifier-free) definable subset W of F^m (some m). In this case $W(K)$ is simply $W \cap K^m$, and is (in K) in definable bijection with $V(K)$. For all intents and purposes one could work with W in place of V.

1.8 MODEL-THEORETIC VERSIONS OF WEIL'S THEOREM An important result of André Weil [We] states, roughly speaking, that an algebraic group (over an algebraically closed field), or more generally an algebraic homogeneous space, can be recovered from birational data. There are two related results which have model-theoretic content, and which we will be using. The first is due to Hrushovski [B1] , and we express it here in the strongly minimal case.

PROPOSITION 1.8.1: *Let M be a (saturated) strongly minimal structure. Let A be a small subset of M. Let $p(\boldsymbol{x})$, $q(\boldsymbol{y})$ be two stationary types over A. Let $f(\boldsymbol{x}_1, \boldsymbol{x}_2)$, $g(\boldsymbol{x}, \boldsymbol{y})$ be partial A-definable functions such that*

(i) *for $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, A-independent realisations of $p(\boldsymbol{x})$, $f(\boldsymbol{a}_1, \boldsymbol{a}_2)$ is defined, and if $\boldsymbol{a}_3 = f(\boldsymbol{a}_1, \boldsymbol{a}_2)$ then $\boldsymbol{a}_3$ realises p, and $\boldsymbol{a}_3$ is independent with each of $\boldsymbol{a}_1$, $\boldsymbol{a}_2$ over A,*

(ii) *for $\boldsymbol{a}$, $\boldsymbol{b}$ independent realisations of p, q respectively, $g(\boldsymbol{a}, \boldsymbol{b})$ is defined, realises q, and is independent with $\boldsymbol{a}$ over A,*

(iii) *if $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, $\boldsymbol{a}_3$ are independent realisations of p then $f(f(\boldsymbol{a}_1, \boldsymbol{a}_2), \boldsymbol{a}_3)) = f(\boldsymbol{a}_1, f(\boldsymbol{a}_2, \boldsymbol{a}_3))$,*

(iv) *if* $\boldsymbol{a}_1$, $\boldsymbol{a}_2$ *realise* p, $\boldsymbol{b}$ *realises* q, *and* $\{\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{b}\}$ *is* A*-independent, then* $g(f(\boldsymbol{a}_1, \boldsymbol{a}_2), \boldsymbol{b}) = g(\boldsymbol{a}_1, g(\boldsymbol{a}_2, \boldsymbol{b}))$.

Then there are interpretable in M *a (connected) group* G, *a (multiplicity 1) set* X *and a transitive action of* G *on* X, *all defined over* A, *as well as partial* A*-definable invertible functions* h_1, h_2 *such that*

(v) *for* $\boldsymbol{a}$ *realising* p, $h_1(\boldsymbol{a})$ *realises the generic type of* G, *and for* $\boldsymbol{b}$ *realising* q, $h_2(\boldsymbol{b})$ *realises the generic type of* X,

(vi) *for independent realisations* $\boldsymbol{a}_1$, $\boldsymbol{a}_2$ *of* p, $h_1(f(\boldsymbol{a}_1, \boldsymbol{a}_2)) = f(\boldsymbol{a}_1) \cdot f(\boldsymbol{a}_2)$,

(vii) *for independent realisations* $\boldsymbol{a}$ *of* p *and* $\boldsymbol{b}$ *of* q, $h_2(g(\boldsymbol{a}, \boldsymbol{b})) = h_1(\boldsymbol{a}) \cdot h_2(\boldsymbol{b})$.

The next result takes place in an algebraically closed field. The attribution is unclear: proofs were given by van den Dries in the characteristic 0 case and Hrushovski [B2] in the general case. Strictly speaking this is in any case just a special case of Weil's original theorem (modulo a trick of Serre in the positive characteristic case).

PROPOSITION 1.8.2: *Let* F *be an algebraically closed field. Let* G *be a definably connected group definable in* F. *Then there is an algebraic group* H *(over* F*) and a definable (in* F*) isomorphism* f *between* G *and* H. *If moreover* $\mathrm{char}(F) = 0$ *and* G *is definable with parameters in a subfield* k *of* F, *then both* H *and* f *can be chosen to be* k*-definable.*

(Here we identify H with $H(F)$ the F-rational points of H.) In fact the proof of 1.8.2 proceeds by first observing that, by quantifier elimination, "generically" the group multiplication on G is given by a rational function (or a quasi-rational function in the positive characteristic case). Weil's proof constructs from this generic rational group law an algebraic group H, which then turns out to be definably isomorphic to G. Connectedness (multiplicity 1) plays a crucial role in obtaining this isomorphism.

Our main theorems in this paper can be considered as generalisations of Proposition 1.8.2 to a wider class of fields F, and actually generalisations of Weil's theorem. The problems we will face in more general contexts are

(i) the group operation on G will (even generically) not be given by a rational function, but rather by a function which satisfies an algebraic equation,

(ii) definable sets in F will no longer have any "finite multiplicity" property, and thus obtaining a global definable isomorphism presents problems.

There is actually also a third related model-theoretic result, namely Hrushovski's "group configuration theorem" [B2]. This theorem roughly states that (say in the context of a strongly minimal structure M) one can recover a situation as in the *hypotheses* of Proposition 1.8.1 from a certain "algebraic- dependence-theoretic" configuration of tuples in M. We will neither state nor use this result. However the proof of Proposition 3.1 will be quite closely related to the proof of the group configuration theorem (in fact the proof of 3.1 will basically just consist in checking that certain constructions in the group configuration theorem can be carried out in a suitable substructure of the structure under consideration).

2. Geometric structures, substructures and fields

In this section we present the model-theoretic framework for the main results of this paper.

Definition 2.1: The infinite structure M is said to be a **geometric structure**, if

(i) in any model N of $\mathrm{Th}(M)$, the algebraic closure operation defines a pregeometry, namely the exchange axiom is satisfied: if $a, b \in N$, $A \subset N$ and $b \in \mathrm{acl}(A, a) \setminus \mathrm{acl}(A)$, then $a \in \mathrm{acl}(A, b)$,

(ii) for any formula $\varphi(x, \boldsymbol{y})$ of the language of M there is some $n < \omega$ such that for any $\boldsymbol{b}$ in M $\varphi(x, \boldsymbol{b})^M$ is finite iff $|\varphi(x, \boldsymbol{b})^M| sh \leq n$.

Remarks 2.2: As in sections 1.4 to 1.6 of section 1, clause (i) in Definition 1.1 gives rise to a notion of independence in geometric structures. Similarly clause (ii) yields the existence of "generic points". In these remarks and the subsequent lemma, we summarise the situation. Let M be a geometric structure, $A \subset M$ and $\boldsymbol{a} \in M^n$. The fact that the algebraic closure operation defines a pregeometry implies that $\dim(\boldsymbol{a}/A)$ = the cardinality of any maximal A-algebraically independent subtuple of $\boldsymbol{a}$, is well defined. We will say that $\boldsymbol{a}$ is independent from B over A if $\dim(\boldsymbol{a}/A \cup B) = \dim(\boldsymbol{a}/A)$. We then obtain :

(i) (symmetry) if $\boldsymbol{a}$ is independent from $\boldsymbol{b}$ over A then $\boldsymbol{b}$ is independent from $\boldsymbol{a}$ over A,

(ii) (additivity). $\dim(\boldsymbol{a}, \boldsymbol{b}/A) = \dim(\boldsymbol{a}/\boldsymbol{b}, A) + \dim(\boldsymbol{b}/A)$.

If $A \subset M$, $\Phi(\boldsymbol{x})$ is a partial type over A, and M is $|A|^+$-saturated, then $\dim_A(\Phi)$ is defined to be

$$\max\{\dim(\boldsymbol{a}/A) : \boldsymbol{a} \text{ in } M \text{ and } M \models \Phi(\boldsymbol{a})\}.$$

If M is not saturated, we read $\dim_A(\Phi)$ in an $|A|^+$-saturated elementary extension of M, namely we define $\dim_A(\Phi) = \max\{\dim(\boldsymbol{a}/A)$: $\boldsymbol{a}$ in some elementary extension M' of M, and $M' \models \Phi(\boldsymbol{a})\}$. ∎

LEMMA 2.3: *Let M be a geometric structure.*

(i) *If $A \subset B \subset M$ and $\Phi(\boldsymbol{x})$ is a partial type over A, then $\dim_A(\Phi) = \dim_B(\Phi)$. (Thus we can omit the base set, and just write $\dim(\Phi)$.)*

(ii) *Let $\varphi(\boldsymbol{x}, \boldsymbol{y})$ be a formula, with $\text{length}(\boldsymbol{x}) = n$. Let $m \leq n$. Then there is a formula $\psi(\boldsymbol{y})$ such that for any $\boldsymbol{b}$, $\dim(\varphi(x, \boldsymbol{b})) = m$ iff $\psi(\boldsymbol{b})$ (and this equivalence holds in any model).*

(iii) *Let $X_1, \ldots, X_k$ be definable subsets of M^n. Then $\dim(X_1 \cup \cdots \cup X_k) = \max\{\dim(X_i)$: $i = 1, \ldots, k\}$.*

Proof: (i) and (ii) are proved just like in the special case where M is strongly minimal (see 1.5 above). (iii) is left to the reader. ∎

For M a geometric structure and $\Phi(\boldsymbol{x})$ a partial type over A, if $\boldsymbol{a}$ realises Φ and $\dim(\boldsymbol{a}/A) = \dim(\Phi)$ we call $\boldsymbol{a}$ a **generic point** of Φ (or of Φ^M) over A. The content of Lemma 2.3 (i) is that generic points over arbitrary sets exist. To get a reasonable model theory for a geometric structure M we need a notion of dimension satisfying additional properties. The nicest example of a geometric structure is simply a strongly minimal set. The crucial general feature of strongly minimal sets is the "finite multiplicity" property, which can fail badly in general geometric structures, for example in O-minimal structures — note that an O-minimal structure is also geometric. We will make use of two nice properties which hold in all strongly minimal structures and also in several other interesting geometric structures.

Definition 2.4: Let M be a saturated geometric structure.

(i) M has property (E) if: whenever $X \subset M^n$ is definable and $\dim(X) = m$ then there is no definable equivalence relation E on X infinitely many classes of which have dimension m.

(ii) M has property (S_1) if: whenever $X \subset M^n$ is definable with $\dim(X) = m$, and $\varphi(\boldsymbol{x}, \boldsymbol{y})$ is a formula, then there do not exist $\boldsymbol{b}_i$ for $i < \omega$ such that $\dim(X \cap \varphi(\boldsymbol{x}, \boldsymbol{b}_i)) = m$ for all i but $\dim(\varphi(\boldsymbol{x}, \boldsymbol{b}_i) \,\&\, \varphi(\boldsymbol{x}, \boldsymbol{b}_j)) < m$ for $i \neq j$.

(iii) An arbitrary geometric structure has property (E) (or (S_1)) if: some, equivalently, every saturated model of $\text{Th}(M)$ has the property.

Remarks 2.5:

(i) Clearly (S_1) implies (E).

(ii) We say a structure M has almost weak elimination of imaginaries if every $b \in M^{eq}$ is interalgebraic with some finite tuple from M. (Compare to: (a) weak elimination of imaginaries, which states that for any $b \in M^{eq}$ there is a finite tuple $\boldsymbol{a}$ from M such that $b \in \mathrm{dcl}(\boldsymbol{a})$ and $\boldsymbol{a} \in \mathrm{acl}(b)$, and (b) elimination of imaginaries, which states that any $b \in M^{eq}$ is interdefinable with some tuple $\boldsymbol{a}$ from M.) It is not difficult to prove that a geometric structure with almost weak elimination of imaginaries satisfies (E). ∎

The geometric structures with which we shall be concerned in this paper are certain fields in which algebraic closure equals field-theoretic algebraic closure. The following definition gives a generalisation. For the purposes of this paper, the reader may take D below to be an algebraically closed field; cf. Definition 2.9 below.

Definition 2.6: Let D be a strongly minimal set which has quantifier elimination in a language L. Let F be an infinite substructure of D. We will call F a **geometric substructure of** D if

(i) F (as an L-structure) is a geometric structure,

(ii) F is definably closed in D. Namely, if $b \in D$ and $b \in \mathrm{dcl}(F)$ in the sense of the structure D, then $b \in F$,

(iii) for any model (D_1, F_1) of $\mathrm{Th}(D, F)$, algebraic closure in the structure F_1 equals quantifier-free definable algebraic closure, namely if $A \subset F_1$, $a \in F_1$ and $a \in \mathrm{acl}(A)$ then there is a quantifier-free formula $\psi(x)$ over A such that $F_1 \models \psi(a)$ and ψ has only finitely many solutions in D_1.

Remarks/Definition 2.7: Let F be a infinite substructure of the strongly minimal set D. We may assume that $D = \mathrm{acl}(F)$. It is not difficult to see that for any model F_1 of $\mathrm{Th}(F)$ there is D_1 such that (D_1, F_1) is elementarily equivalent to (D, F) and moreover $D_1 = \mathrm{acl}(F_1)$ in L. To say that F is a geometric substructure of D means exactly that for any model F_1 of $\mathrm{Th}(F)$, for D_1 as above F_1 is definably closed in D_1, for any $A \subset F_1$, the algebraic closure of A in F_1 in the sense of the L-structure F_1 is precisely $F_1 \cap$(algebraic closure of A in D_1), and that 2.1 (ii) holds for F.

(ii) Let F be a geometric substructure of D, and assume that F is a saturated model of $\mathrm{Th}(F)$. For $\boldsymbol{a} \in F^n$ and $A \subset F$, $\mathrm{tp}(\boldsymbol{a}/A)$ means the type of $\boldsymbol{a}$ over

A in the sense of F. Similarly $X \subset F^n$ will be called A-**definable** if it is definable in the structure F with parameters in A. We say $\boldsymbol{a} \in \mathrm{dcl}(A)$, if $\boldsymbol{a}$ is definable with parameters from A in the structure F.

$\mathrm{qftp}(\boldsymbol{a}/A)$ denotes the set of quantifier-free formulas over A, true of $\boldsymbol{a}$, or equivalently the type of $\boldsymbol{a}$ over A in the sense of D. Similarly $\mathrm{qfdcl}(A)$ is the set of elements of F definable over A by quantifier-free formulas. Note that, as F is definably closed in D, for $A \subset F$, $\mathrm{qfdcl}(A)$ is precisely the definable closure of A in D in the sense of the structure D.

For $\boldsymbol{a} \in F^n$ and $A \subset F$, note that $\dim(\boldsymbol{a}/F)$ is a function of $\mathrm{qftp}(\boldsymbol{a}/A)$ and equals $\dim(\boldsymbol{a}/A)$ in the sense of the strongly minimal set D.

(iii) Let F be a geometric substructure of D, and $X \subseteq D^n$ a set definable in D with parameters from F. Then $X(F) = X \cap F^n$ is definable in F. This is because X is quantifier-free definable in D over F, and so the same quantifier-free formula defines $X(F)$ in F. ∎

LEMMA 2.8: *Let F be a geometric substructure of D. Assume D has weak elimination of imaginaries. Let $A \subset F$ be algebraically closed inside F (namely $\mathrm{acl}(A) \cap F = A$), and let $\boldsymbol{a}$ be a tuple in F. Then $\mathrm{qftp}(\boldsymbol{a}/A)$ is stationary (and thus there is finite $A_0 \subset A$ such that $\mathrm{qftp}(\boldsymbol{a}/A)$ does not fork over A_0, and $\mathrm{qftp}(\boldsymbol{a}/A_0)$ is stationary).*

Proof: By elimination of imaginaries in D and the finite equivalence relation theorem, the canonical base of $\mathrm{stp}(\boldsymbol{a}/A)$ in the sense of D is in $\mathrm{acl}(A) \cap \mathrm{qfdcl}(\boldsymbol{a})$. The latter set equals A as F is definably closed in D. ∎

In the special case of fields we amalgamate Definitions 2.1 and 2.6 as follows:

Definition 2.9: Let F be a field, viewed as an L-structure, where $L = \{+, \cdot, 0, 1, -\}$. We call F a **geometric field** if F is a geometric substructure of $\widetilde{F}$ where $\widetilde{F}$ is the (field-theoretic) algebraic closure of F.

Remark 2.10: As remarked in 1.7, $\widetilde{F}$ has quantifier elimination in L. So to say that F is a geometric field clearly means

(1) F is perfect,

(2) for any model F_1 of $\mathrm{Th}(F)$, and subset A of F_1, the algebraic closure of A in F_1 in the model-theoretic and algebraic senses coincide,

(3) for each L-formula $\varphi(x, \boldsymbol{y})$ there is some $N < \omega$ such that in any model F_1 of $\mathrm{Th}(F)$, and for any $\boldsymbol{b}$ in F_1, if $\varphi(x, \boldsymbol{b})$ defines a finite subset of F_1 then it defines a set with at most N elements. ∎

PROPOSITION 2.11: *The following fields are geometric fields:*

(1) *The real field* $\mathbb{R}$.

(2) *The p-adic field* $\mathbb{Q}_p$.

(3) *Any pseudo-finite field.*

Proof: (1) and (2) follow easily from standard quantifier elimination results of Tarski and Macintyre. In fact Tarski shows that $\mathrm{Th}(\mathbb{R})$ has quantifier elimination after adding a symbol for the ordering (or equivalently for the squares). Macintyre [Mac] shows that $\mathrm{Th}(\mathbb{Q}_p)$ has quantifier elimination after adding predicates for the nth powers, for all n. (3) is more subtle and is proved in [Ch-v.d.D-Mac], Corollary 5.7, using the notion "algebraically bounded". ∎

Remark 2.12: In [Ch-v.d.D-Mac] it is shown that in arbitrary perfect PAC fields, model-theoretic and field-theoretic algebraic closures coincide. So, the only additional property needed for a perfect PAC field F to be a geometric field is property (3) in Remark 2.10. This was shown to hold for "Frobenius fields" by Jarden [Ja]. In fact (3) has been proved for arbitrary perfect PAC fields by the first author in recent unpublished work (and explained to the second author by Zoe Chatzidakis). ∎

Remark 2.13: Let F be a geometric field which we assume to be reasonably saturated. Let F_0 denote the prime field of F. We summarise the translation between the model-theoretic and algebraic language:

(i) If A is a subset of F then $\dim(\boldsymbol{a}/A) = \mathrm{tr.degree}(F_0(A)(\boldsymbol{a})/F_0(A))$ for each $\boldsymbol{a} \in F^n$.

(ii) Let k be a relatively algebraically closed subfield of F, and $\boldsymbol{a} \in F^n$, then the variety over k generated by $\boldsymbol{a}$ is irreducible. (This is obtained from the statement "qftp$(\boldsymbol{a}/k)$ is stationary" in 2.8, using the translation in 1.7).

(iii) Let X be a definable subset of F^n, defined over the finite set A, say. Then $\dim(X)$ = algebro-geometric dimension of $\widetilde{X}$, the Zariski closure of X in $(\widetilde{F})^n$.

The proof of (iii) is quite straightforward: for each $\boldsymbol{a} \in X$, the variety $V(\boldsymbol{a}) \subset (\widetilde{F})^n$ generated by $\boldsymbol{a}$ over $F_0(A)$ has algebro-geometric dimension equal to $\dim(\boldsymbol{a}/A)$ (by (i)). By saturation of F and compactness, there are $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ in X such that $X \subset (V(\boldsymbol{a}_1)(F) \cup \cdots \cup V(\boldsymbol{a}_k)(F))$. So $\widetilde{X} \subset V(\boldsymbol{a}_1) \cup \cdots \cup V(\boldsymbol{a}_k)$. Thus the algebro-geometric dimension of $\widetilde{X}$ is at most $\dim(X)$. The reverse inequality is immediate.

The difference with algebraically closed fields is that in the case of an arbitrary geometric field F, if $V(F)$ is a Zariski closed (hence definable) subset of F^n with $\dim(V(F)) = m$, even if V is absolutely irreducible there may be still be disjoint definable subsets of $V(F)$, say X and Y such that $\dim(X) = \dim(Y) = m$. Or putting it another way, there may be many different types $p(x)$ such that $p(\boldsymbol{x}) \vdash \boldsymbol{x} \in V$ and $\dim(p(\boldsymbol{x})) = m$ (although there will be a unique such quantifier-free type). Or putting it even another way, assuming V is defined over k, there may be several different types over k of generic points $\boldsymbol{a} \in V(F)$ of V over k. ∎

Finally we consider the examples $\mathbb{R}$, $\mathbb{Q}_p$, and pseudo-finite fields in a little more detail. The definable sets in the real and p-adic case are often called **semi-algebraic** sets.

First both R and $\mathbb{Q}_p$ are topological fields (given by the Euclidean topology, and valuation topology respectively). Dimension then has a topological interpretation.

Fact 2.14: See [P2] and [P3]. ($F = \mathbb{R}$ or $\mathbb{Q}_p$). Let X be a definable subset of F^n. Then $\dim(X) = \max\{k \leq n$: some projection of X onto F^k contains an open set$\}$.

Moreover for each of the fields $\mathbb{R}$, $\mathbb{Q}_p$, there is a notion of an analytic function (from say an open subset of F^n into F). In fact a Nash function is precisely a definable analytic function from some open definable subset X of F^n into F.

Fact 2.15: [BCR] and [v.d.D-S]. Again let F be $\mathbb{R}$ or $\mathbb{Q}_p$.

(i) Let X be an open definable subset of F^n and let $f: X \to F$ be a definable function. Then there is some open dense definable subset Y of X such that $f|Y$ is analytic (namely Nash).

(ii) Suppose $k < F$, $a \in F$ and $a \in \operatorname{acl}(k)$. Then $a \in \operatorname{dcl}(k)$. ∎

Concerning the properties (E) and (S_1) we have:

Remark 2.16: $\mathbb{R}$ has (E) but not (S_1). $\mathbb{Q}_p$ does not even have (E).

Proof: The fact that $\mathbb{R}$ (or more generally any O-minimal structure) has property (E) is proved in [P6]. $\mathbb{R}$ does not have (S_1), as we can find infinitely many disjoint intervals in $\mathbb{R}$ (which are clearly defined by the same shape of formula). $\mathbb{Q}_p$ does not have (E), because the equivalence relation $v(x) = v(y)$ is definable and has infinitely many classes, all infinite (and so of dimension 1). ∎

LEMMA 2.17: *Let F be $\mathbb{R}$ or $\mathbb{Q}_p$. Let A be a countable subset of F, and let X be an A-definable subset of F^n. Then X contains a generic point over A, namely there is $\boldsymbol{a} \in X$ such that* $\dim(\boldsymbol{a}/A) = \dim(X)$.

Proof: The point here is that F is not ω_1-saturated, so we cannot just use the definition of $\dim(X)$. However we know from 2.14 that some projection π of X onto F^k contains an open set, where $k = \dim(X)$. Baire category implies that $\pi(X)$ is not contained in a union of A-definable sets of dimension $< k$. So there is $\boldsymbol{b} \in \pi(X)$, such that $\dim(\boldsymbol{b}/A) = k$, and then $\boldsymbol{b}$ extends to $\boldsymbol{a}$ in X such that $\dim(\boldsymbol{a}/A) = k$. ∎

As far as pseudo-finite fields are concerned, the main point is:

Fact 2.18: Let F be a pseudo-finite field. Then F has the (S_1) property.

Proof: This is proved in [Ch-v.d.D-Mac], but we review the situation. Let us suppose F to be an ω-saturated pseudo-finite field. Let $X \subset F^m$ be a definable set in F. We have already pointed out that $d = \dim(X)$ = algebro-geometric dimension of the Zariski closure $\widetilde{X}$ of X in $(\widetilde{F})^m$. Using a generalisation of the Lang–Weil estimates for the number of points on varieties over finite fields, it is shown in [Ch-v.d.D-Mac] that in addition to the dimension d of X, a certain positive rational number $\mu(X)$ can also be assigned to X. It is shown further that

(i) for any formula $\varphi(\boldsymbol{x}, \boldsymbol{y})$ there are a finite number of pairs (d', μ') associated thus to sets defined by $\varphi(\boldsymbol{x}, \boldsymbol{a}')$ as $\boldsymbol{a}'$ varies.

We also have (see 4.10 of [Ch-v.d.D-Mac]):

(ii) if $X \subset Y$ are definable subsets of F^m with $\dim(X) = \dim(Y)$ then $\mu(X) \leq \mu(Y)$.

(iii) Let X and Y be disjoint definable subsets of F^m. If $\dim(X) = \dim(Y)$, then $\mu(X \cup Y) = \mu(X) + \mu(Y)$. If $\dim(X) < \dim(Y)$ then $\mu(X \cup Y) = \mu(Y)$.

The (S_1) property for F follows immediately from (i), (ii) and (iii). ∎

It should be said that all these fields ($\mathbb{R}$, $\mathbb{Q}_p$ and pseudo-finite fields) are unstable (in the sense of model theory). Stability will be formally defined in section 5. For now we remark that if F is a stable field then F^*, the multiplicative group of F, can have no proper definable subgroups of finite index. But each of the fields we are considering clearly does have such multiplicative subgroups.

The first author has (in unpublished notes) defined a PAC-substructure of a strongly minimal set D to be a geometric substructure F of D such that for any

F-definable multiplicity 1 set $X \subset D^n$, $X(F) \neq \emptyset$. In addition he defines F to be bounded if for any model (F_1, D_1) of $\mathrm{Th}(F, D)$, the group G of automorphisms of $\mathrm{acl}(F_1)$ in D_1 which fix F_1 pointwise, is small (in the sense again that any for any finite group H there are only finitely many continuous homomorphisms of G into H). He proves that if F is a bounded PAC-substructure of D and D has elimination of imaginaries, then F has elimination of imaginaries and has the (S_1) property. Using this fact in place of 2.18, all of section 6 of this paper can be carried over to that context.

3. A "group configuration theorem"

In this section we prove the basic common result lying behind Theorems A, B and C. The result can be roughly stated as :

(*) Let F be a geometric substructure of D. Let G be a group which is definable in F. Then there is a connected group H (quantifier-free) definable in D with parameters from F such that G is "generically algebraically equivalent" to $H(F)$.

More precisely, throughout this section we will be working under the following hypotheses:

(1) F is a geometric substructure of the strongly minimal set D, where D has elimination of imaginaries (and of course quantifier elimination).

(2). For any finite subset A of F, and any A-definable subset X of F^n, X has an A-generic point. (The point here is that such an A-generic point of X can be found already in F rather than in some elementary extension of F. Note that this implies that D is ω-saturated.)

(3) G is a group definable in F . (So G is a definable subset of some cartesian power of F, and the group operation of G is definable in F.)

Under these hypotheses we prove:

PROPOSITION 3.1: *There is a finite subset A of F over which G is defined, a connected group H quantifier-free definable in D over A, points $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ of G and points $\boldsymbol{a}'$, $\boldsymbol{b}'$, $\boldsymbol{c}'$ of $H(F)$, such that*

(i) $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{c}$ *(in G) and* $\boldsymbol{a}' \cdot \boldsymbol{b}' = \boldsymbol{c}'$ *(in H).*

(ii) $\mathrm{acl}(\boldsymbol{a}A) = \mathrm{acl}(\boldsymbol{a}'A)$, $\mathrm{acl}(\boldsymbol{b}A) = \mathrm{acl}(\boldsymbol{b}'A)$ *and* $\mathrm{acl}(\boldsymbol{c}A) = \mathrm{acl}(\boldsymbol{c}'A)$.

(iii) $\boldsymbol{a}$ *and* $\boldsymbol{b}$ *are A-generic points of G and* $\boldsymbol{a}$ *is independent with* $\boldsymbol{b}$ *over A.*

(iv) *Similarly* $\boldsymbol{a}'$ *and* $\boldsymbol{b}'$ *are A-generic points of H and are independent with each other over A.*

PROPOSITION 3.1′ (Restatement for fields): *Let F be $\mathbb{R}$, $\mathbb{Q}_p$ or an ω-saturated pseudo-finite field (or more generally a geometric field satisfying (2) above). Let G be a group definable in F over a finite set A_0. Then there is a finite subset A of F containing A_0 and a connected algebraic group H defined over $F_0(A)$ such that there are points $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ of G and points $\boldsymbol{a}'$, $\boldsymbol{b}'$, $\boldsymbol{c}'$ of $H(F)$ satisfying (i) (ii), (iii), (iv) above.*

In the proof we will let a, b, c, a' etc. denote tuples from F (and sometimes also from D). The notation from 2.7 and 1.2–1.6 is in effect. For x, y in some group $x \cdot y$ denotes the product of x and y in that group.

The proof will proceed through a series of lemmas.

Let A_0 be a finite subset of F over which G (and its group operation) are defined. Let $\dim(G) = n$. Let a, b be A_0-independent, A_0-generic points of G. Let $c = a \cdot b$. Note that $\dim(a/A_0) = \dim(b/A_0) = \dim(c/A_0) = n$ and $\dim(a, b/A_0) = \dim(a, b, c/A_0) = 2n$. In F, $c \in \mathrm{dcl}(a, b, A_0)$, $b \in \mathrm{dcl}(a, c, A_0)$ The main point is to modify a, b, and c (staying inside F) in such a way that dcl is replaced by qfdcl (namely definable closure in the sense of D).

LEMMA 3.2: *There are a finite subset A_2 of F, containing A_0, with $\{a, b\}$ and A_2 independent over A_0, and tuples a_1, b_1, c_1 in F such that* $\mathrm{acl}(a, A_2) = \mathrm{acl}(a_1, A_2)$, $\mathrm{acl}(b, A_2) = \mathrm{acl}(b_1, A_2)$, $\mathrm{acl}(c, A_2) = \mathrm{acl}(c_1, A_2)$, $b_1 \in \mathrm{qfdcl}(A_2, a_1, c_1)$ *and* $c_1 \in \mathrm{qfdcl}(A_2, a_1, b_1)$.

Proof: Let (by assumption (2) on F) $x' \in G$ be generic over $A_0 \cup \{a, b\}$. Let $y' = x' \cdot b$ and $z' = x' \cdot a^{-1}$. (So $z' \cdot c = y'$.) Then additivity of dimension yields easily

(1) $\dim(a, c, b, y', z'/A_0) = 3n$, and $\dim(a, c, b/A_0) = \dim(z', c, y'/A_0) = 2n$.

CLAIM: Let c' be any tuple in D such that

$$\mathrm{qftp}(c'/a, z', b, y', A_0) = \mathrm{qftp}(c/a, z', b, y', A_0).$$

Then $c' \in \mathrm{acl}(c, A_0)$.

Proof of the claim: If not then $\dim(c, c'/A_0) \geq n+1$. By (1) $\dim(a, b/c, c', A_0) \leq n - 1$ and also $\dim(z', y'/c, c', A_0) \leq n - 1$. It clearly follows that

$$\dim(a, b, z', y', c, c'/A_0) \leq 2(n-1) + n + 1 = 3n - 1$$

which contradicts (1), and proves the claim.

Let $X = \{c = c_1, c_2, \ldots, c_r\}$ be the set of conjugates in D of c over $\{a, b, z', y', A_0\}$ (namely the set of elements in D whose type in D over $\{a, b, z', y', A_0\}$ is the same as that of c). Note that X is finite as $c \in \mathrm{acl}(a, b, z', y', A_0)$. By the fact that D has elimination of imaginaries, there is a tuple c_1 from D such that c_1 and X are interdefinable in D. It follows that $c_1 \in \mathrm{qfdcl}(a, b, z', y', A_0)$ and thus c_1 is in F. Denote the concatenated sequence (a, z') by a_1, and (b, y') by b_1. Let $A_1 = A_0 \cup \{x'\}$. So we now clearly have a_1, b_1, c_1 in F with

(2) $\mathrm{acl}(a, A_1) = \mathrm{acl}(a_1, A_1)$, $\mathrm{acl}(b, A_1) = \mathrm{acl}(b_1, A_1)$, $\mathrm{acl}(c, A_1) = \mathrm{acl}(c_1, A_1)$ and moreover $c_1 \in \mathrm{qfdcl}(A_1 \cup \{a_1, b_1\})$.

Let $z_1 \in G$ be generic over $A_1 \cup \{a, b\}$. Let $x_1 = z_1 \cdot a$ and $y_1 = z_1 \cdot c$. Then $x_1 \cdot b = y_1$. Moreover by choice of z_1,

(3) x_1 and b are A_0-independent, A_0-generic points of G, and

(4) $\{x_1, b\}$ is independent with x' over A_0.

So exactly as in (2) we can find tuples x_2, y_2 and b_2 in F such that

(5) $\mathrm{acl}(x_1, A_1) = \mathrm{acl}(x_2, A_1)$, $\mathrm{acl}(y_1, A_1) = \mathrm{acl}(y_2, A_1)$, $\mathrm{acl}(b, A_1) = \mathrm{acl}(b_2, A_2)$ and $y_2 \in \mathrm{qfdcl}\{x_2, b_2, A_1\}$.

As $\mathrm{acl}(b, A_1) = \mathrm{acl}(b_1, A_1)$ nothing is lost in (5) in assuming that

(6) b_2 contains b_1.

Note that, by generic choice of z_1 over A_1 we have:

(7) $\dim(a_1, b_2, c_1, x_2, y_2/A_1) = 3n$, $\dim(x_2, y_2, b_2/A_1) = \dim(a_1, c_1, b_2/A_1) = 2n$.

The same computation as in proof of the claim above shows that if b_2' is in D and has the same quantifier free type as b_2 over $A_1 \cup \{a_1, c_1, x_2, y_2\}$ then $b_2' \in \mathrm{acl}(A_1, b_2)$. So, letting A_2 denote $A_1 \cup \{z_1\}$, it follows that if b_2' is in D and has the same quantifier-free type as b_2 over $A_2 \cup \{a_1, c_1, x_2, y_2\}$ then $b_2' \in \mathrm{acl}(A_2, b_2)$. Thus again let b_3 in D be interdefinable in D with the finite set of conjugates in D of b_2 over $A_2 \cup \{a_1, c_1, x_2, y_2\}$. Then

(8) $b_3 \in \mathrm{qfdcl}(A_2 \cup \{a_1, c_1, x_2, y_2\})$.

Again it follows that b_3 is in F. (5) and (2) yield

(9) y_2 and c_1 are both in $\mathrm{qfdcl}(A_2 \cup \{a_1, x_2, b_2\})$.

Thus $y_2 = f(b_2)$ and $c_1 = g(b_2)$ for some quantifier-free $(A_2 \cup \{a_1, x_2\})$-definable functions f and g. So for any b_2' in D satisfying the same quantifier-free type as b_2 over $A_2 \cup \{a_1, x_2, y_2, c_1\}$, also $y_2 = f(b_2')$ and $c_1 = g(b_2')$. By choice of b_3 we then clearly have

(10) y_2 and c_1 are both in $\mathrm{qfdcl}(A_2 \cup \{a_1, x_2, b_3\})$.

Rename (a_1, x_2) as a_1, (y_2, c_1) as c_1 and b_3 as b_1. By (8) and (9), Lemma 3.2 is proved.

Let A denote $\mathrm{acl}(A_2) \cap F$. From now on we work in D.

Remark 3.3: $\mathrm{qftp}(a_1, b_1, c_1/A)$ and $\mathrm{qftp}(b_1, c_1/A, a_1)$ are both stationary.

Proof: $\mathrm{qftp}(a_1, b_1, c_1/A)$ is stationary as a_1, b_1, c_1 are from F and A is relatively algebraically closed in F. (See Lemma 2.8.) Now b_1 is independent from $A \cup \{a_1\}$ over A. Thus also $\mathrm{qftp}(b_1/A, a_1))$ is stationary. But $c_1 \in \mathrm{qfdcl}(A, a_1, b_1)$. Thus $\mathrm{qftp}(b_1, c_1/A, a_1)$ is stationary. ∎

Let the tuple σ from D be the canonical base of $\mathrm{qftp}(b_1, c_1/A, a_1)$. So $\sigma \in \mathrm{qfdcl}(A, a_1)$. By Remark 3.3, σ is in F. Let $r = \mathrm{qftp}(\sigma/A)$, $q_1 = \mathrm{qftp}(b_1/A)$, $q_2 = \mathrm{qftp}(c_1/A)$. So $\dim(q_1) = \dim(q_2) = n$. The next remark is to be understood in the sense of D. In fact from now on D will be the structure we work in, except that we take care that certain points are in F.

Remark 3.4: r is stationary, with $\dim(r) = n$. σ is independent with each of b_1, c_1 over A, $c_1 \in \mathrm{qfdcl}(A, \sigma, b_1)$ and $b_1 \in \mathrm{qfdcl}(A, \sigma, c_1)$.

Proof: The stationarity of r follows from 2.8. Note that $\{a_1, b_1, c_1\}$ is pairwise A-independent. As $\sigma \in \mathrm{acl}(a_1, A)$, $\dim(r) \leq \dim(a_1/A) = n$. For the same reason σ is independent with each of b_1, c_1 over A. The fact that $c_1 \in \mathrm{qfdcl}(A, a_1, b_1)$ and $b_1 \in \mathrm{qfdcl}(A, a_1, c_1)$ is part of $\mathrm{qftp}(b_1, c_1/Aa_1)$, and so is preserved when we replace a_1 by σ. In particular $n = \dim(c_1/A, b_1) \leq \dim(\sigma/A, b_1) = \dim(\sigma/A)$. So $\dim(r) = n$. ∎

Remark 3.4 is rather important. Assuming we are working in say a characteristic 0 geometric field F, this is what is going on: $F_0(A)(\sigma)$ is the field of definition of the variety generated by (b_1, c_1) over $F_0(A)(a_1)$. The variety generated by σ over $F_0(A)$ is absolutely irreducible (and r is the type of a generic point of it, namely of σ). The transcendence degree of $F_0(A)(\sigma)$ over $F_0(A)$ is n. Also, $F_0(A, \sigma, b_1) = F_0(A, \sigma, c_1)$. In the positive characteristic case, the same is true after we replace: "field generated by" by "purely inseparable closure of field generated by".

To return to the general context: Remark 3.4 says that r is the type of a generically defined invertible map from the locus of q_1 to the locus of q_2. To be more precise, as $c_1 \in \mathrm{qfdcl}(\sigma, b_1, A)$ there is some A-definable partial function in the sense of D, say μ, such that $c_1 = \mu(\sigma, b_1)$. We write $\mu(\sigma, b_1)$ as $\sigma.b_1$

(hopefully with no ambiguity), and note that whenever σ' realises r, and b_1' realises q_1 with σ' independent with b_1' over A, $\sigma' \cdot b_1'$ is well-defined, realises q_2 and is independent with each of σ', b_1' over A. Similarly there is an A-definable partial function ν such that $\nu(\sigma, c_1) = b_1$. We write $\nu(\sigma, c_1)$ as $\sigma^{-1} \cdot c_1$, and again for σ', c_1' independent realisations of r, q_2 respectively, $(\sigma')^{-1} \cdot c_1'$ realises q_1 (and clearly $\sigma \cdot ((\sigma')^{-1} \cdot c_1) = c_1$). Note that

Remark 3.5: If σ_1, σ_2 realise r, b' realises q_1, b' is independent with $\{\sigma, \sigma'\}$ over A, and $\sigma_1 \cdot b' = \sigma_2 \cdot b'$, then $\sigma_1 = \sigma_2$.

Proof: Let c' be the common value of $\sigma_1 \cdot b'$ and $\sigma_2 \cdot b'$. Then $\dim(b', c'/A, \sigma_1, \sigma_2) = \dim(b', c'/A, \sigma_1) = \dim(b', c'/A, \sigma_2) = n$. Clearly then each of σ_1, σ_2 is the canonical base of $\mathrm{qftp}(b', c'/A, \sigma_1, \sigma_2)$. From 1.6 we see that σ_1 is interdefinable with σ_2. However, as actually σ_1 and σ_2 have the same quantifier-free type (over A) it follows, by considering in more detail the equivalence relation E in 1.6 that $\sigma_1 = \sigma_2$. ∎

Field theoretic proof of 3.5: With above notation, let V_1 be the variety over $F_0(A, \sigma_1)$ generated by (b', c') and V_2 the variety over $F_0(A, \sigma_2)$ generated by the same point (b', c'). Then (b', c') is a generic point of each of V_1, V_2 over $F_0(A, \sigma_1, \sigma_2)$. So $V_1 = V_2$. There is an automorphism f (of the ambient algebraically closed field) taking σ_1 to σ_2 (as they have the same quantifier-free type). As $F_0(\sigma_1)$ is the field of definition of V_1, and $F_0(\sigma_2)$ the field of definition of V_2, this automorphism takes V_1 to V_2, thus (as $V_1 = V_2$) fixes V_1. So f is the identity on $F_0(\sigma_1)$, in particular $\sigma_2 = \sigma_1$. ∎

Remark 3.5 justifies our calling σ the **germ** of an invertible function from q_1 to q_2. Our aim now is, by "composing" σ with the "inverse" of an independent copy of σ, to find the germ of an invertible function from q_1 to itself. This will then yield a set-up in which we can apply Proposition 1.8.1.

Let σ_1, σ_2 be A-independent realisations of r (note that we can choose σ_1, σ_2 in F if we so wish). Let b_2 realise q_1 independently with $\{\sigma_1, \sigma_2\}$ over A. (Again b_2 can be chosen in F if the σ_i are.) Then $\sigma_1 \cdot b_2$ is defined, realises q_2 and is independent with σ_2 over A. Thus $\sigma_2^{-1} \cdot (\sigma_1 \cdot b_2) = b_3$ is defined and realises q_1. Intuitively we think of "$\sigma_2^{-1}.\sigma_1$" as the germ of an invertible map from q_1 to q_1.

Remark 3.6: $b_3 \in \mathrm{qfdcl}(A, \sigma_1, \sigma_2, b_2)$, $b_2 \in \mathrm{qfdcl}(A, \sigma_1, \sigma_2, b_3)$, each of b_2, b_3 is independent with $\{\sigma_1, \sigma_2\}$ over A. Also $\mathrm{qftp}(b_2, b_3/A, \sigma_1, \sigma_2)$ is stationary.

Proof: Easy and left to the reader. ∎

Let the tuple τ in D be the canonical base of $\mathrm{qftp}(b_2, b_3/A, \sigma_1, \sigma_2)$. Then as in 3.4, $b_3 \in \mathrm{qfdcl}(A, \tau, b_2)$ and $b_2 \in \mathrm{qfdcl}(A, \tau, b_3)$. We write $\tau \cdot b_2 = b_3$ and $\tau^{-1} \cdot b_3 = b_2$. Let $s = \mathrm{qftp}(\tau/A)$. Again s is stationary, and τ can again be viewed as the germ of an invertible map from q_1 to itself. The analogue of 3.5 also holds:

Remark 3.5′: If $\tau \cdot b' = b''$ and $\tau' \cdot b' = b''$ and b' is independent from $\{\tau, \tau'\}$ over A, then $\tau = \tau'$.

LEMMA 3.7: *With the above notation,* $\dim(s) = n$. *Also* τ *is independent with each of* σ_1, σ_2 *over* A.

Proof: We first remark that each of σ_1, σ_2, τ is in the algebraic closure (in fact in the qfdcl) of A together with the other two. This is basically because these elements arise as canonical bases. With this observation we first deduce the dimension part of the lemma from the independence part.

$$\dim(\sigma_1, \sigma_2, \tau/A) = \dim(\sigma_1, \sigma_2/A) = 2n.$$

$$\begin{aligned}\dim(\sigma_1, \sigma_2, \tau/A) &= \dim(\sigma_2/\sigma_1, \tau, A) + \dim(\tau/\sigma_1, A) + \dim(\sigma_1/A) \\ &= 0 + \dim(\tau/A) + n.\end{aligned}$$

So $\dim(\tau/A) = n$. Now we prove independence of each of σ_1, σ_2 from τ over A. As a matter of notation we may as well assume that $\sigma_1.b_1 = c_1$ (i.e. $\sigma_1 = \sigma$). Let $x \in G$ be generic over $A \cup \{a, b\}$. (a, b, c are as chosen at the beginning of the proof of 3.1, and remember that a_1, b_1, c_1 are each interalgebraic over A with a, b, c respectively.) We may suppose that σ_2 is independent with $\{a, b, x\}$ over A. Let $y = x \cdot b$ and $z = y \cdot c^{-1}$ (where $\cdot$ is in the sense of the group G). Then $z = x \cdot a^{-1}$. So σ_2 is independent from $\{x, y, z, a, b, c\}$ over A. As $\sigma_1 \in \mathrm{acl}(a, A)$, σ_1 is clearly independent from $\{z, c_1, y\}$ over A. As r is stationary it follows that σ_1 and σ_2 have the same quantifier-free type over $A \cup \{z, c_1, y\}$. Thus in D we can find elements x_1 and b_2 such that $\mathrm{qftp}(\sigma_1, c_1, b_1, x, y, z/A) = \mathrm{qftp}(\sigma_2, c_1, b_2, x_1, y, z/A)$. It is easily seen that $\tau \cdot b_1 = b_2$. We now make the following claims which imply the desired independence statement:

(A) $\{x, x_1\}$ is independent from each of σ_1, σ_2 over A.

(B) $\tau \in \mathrm{acl}(x, x_1, A)$.

We first discuss (A). Let X be the collection of all points currently considered in the proof of 3.7, namely $X = \{\sigma_1, b, c, b_1, c_1, x, y, z, \sigma_2, x_1, b_2\}$. It is clear that

$\dim(X/A) = 4n$. On the other hand X is clearly contained in $\mathrm{acl}(\sigma_1, x, x_1, b_1, A)$ say, as well as $\mathrm{acl}(\sigma_2, x, x_1, b_1, A)$. But each of the points σ_1, σ_2, x, x_1, b has dimension n over A. This forces $\dim(\sigma_1, x, x_1/A) = \dim(\sigma_2, x, x_1/A) = 3n$, yielding (A).

Now we discuss (B). The argument in the previous paragraph shows that

(i) $\dim(\sigma_1, x, x_1, b_1/A) = 4n$, whereby $\{\sigma_1, x, x_1\}$ is independent from b_1 over A.

But clearly $\sigma_2 \in \mathrm{acl}(\sigma_1, x, x_1, A)$. Thus

(ii) $\{\sigma_1, \sigma_2, x, x_1\}$ is independent from b_1 over A.

By (ii) and the fact that $b_2 \in \mathrm{dcl}(\tau, b_1)$ we see that

(iii) $\tau =$ the canonical base of $\mathrm{qftp}(b_1, b_2/\sigma_1, \sigma_2, x, x_1, A)$.

On the other hand, we have

(iv) $b_2 \in \mathrm{acl}(x, x_1, b_1, A)$

(For $y \in \mathrm{acl}(b_1, x, A)$ and $b_2 \in \mathrm{acl}(y, x_1, A)$). Thus $\mathrm{qftp}(b_1, b_2/\sigma_1, \sigma_2, x, x_1, A)$ does not fork over $\{x, x_1, A\}$. So by (iii) and 1.6, $\tau \in \mathrm{acl}(x, x_1, A)$, proving (B). The Lemma is proved. ∎

We revert now to the notation of 3.6. Clearly $\tau \in \mathrm{qfdcl}(\sigma_1, \sigma_2, A)$ and we write $\tau = \sigma_2^{-1} \cdot \sigma_1$. By 3.6, τ is independent with each of b_2, b_3 over A. We write $\tau \cdot b_2 = b_3$ and $\tau^{-1} \cdot b_3 = b_2$.

LEMMA 3.8: *There is a function f, (quantifier-free) definable in D with parameters in A, such that for independent realisations τ_1 and τ_2 of σ, $f(\tau_1, \tau_2)$ realises s and is independent over A with each of τ_1, τ_2, and moreover for b' realising q_1 independent of $\{\tau_1, \tau_2\}$ over A, $f(\tau_1, \tau_2) \cdot b' = \tau_1 \cdot (\tau_2 \cdot b)$.*

Proof: Let σ_2 realise r such that σ_2 is independent from $\{\tau_1, \tau_2, b'\}$ over A. By Lemma 3.7 there are realisations σ_1, σ_3 of r such that $\tau_1 = \sigma_1^{-1} \cdot \sigma_2$ and $\tau_2 = \sigma_2^{-1} \cdot \sigma_3$. Note that $\tau_2 \cdot b'$ realises q_1 and is independent with τ_1 over A, and thus $\tau_1 \cdot (\tau_2 \cdot b')$ is well-defined, and equals say c'. On the other hand, from Lemma 3.7 it follows that σ_1 and σ_3 are independent over A and $\{\sigma_1, \sigma_3\}$ and b' are independent over A. Thus $\sigma_1^{-1} \cdot \sigma_3 = \tau_3$ realises s and clearly τ_3 is the canonical base of $\mathrm{qftp}(b', c'/A_1, \tau_1, \tau_2)$, and also $\tau_3 \cdot b' = c'$. Thus for some (quantifier-free) A-definable function f, $f(\tau_1, \tau_2) = \tau_3$ and the lemma is proved. ∎

It is now a simple matter to check that s and q_1 satisfy the hypotheses of Proposition 1.8.1. Specifically the function f in 3.8 will correspond to the function

f in 1.8.1 and the function $(\tau, b) \to \tau \cdot b$ will correspond to the function g in 1.8.1. The only thing to check is hypothesis (iii) in 1.8.1, namely associativity. So let τ_1, τ_2, τ_3 be independent realisations of s. Let b realise q_1 independently from $\{\tau_1, \tau_2, \tau_3\}$ over A. Then clearly from 3.8, $\tau_1 \cdot (\tau_2 \cdot (\tau_3 \cdot b)) = f(\tau_1, f(\tau_2, \tau_3)) \cdot b = f(f((\tau_1, \tau_2), \tau_3)) \cdot b$. By 3.5′, $f(\tau_1, f(\tau_2, \tau_3)) = f(f((\tau_1, \tau_2), \tau_3))$, as required.

Let H, X and h_1, h_2 be as given by Proposition 1.8.1. We can assume that h_1, h_2 are both the identity function. Thus already s is the generic type of H, q_1 is the generic type of X, and for τ_1, τ_2 independent realisations of s, the product $\tau_1.\tau_2$ in the group H is exactly $f(\tau_1, \tau_2)$. Also the notation $(\tau, b) \to \tau.b$ for the group action of H on X agrees with the earlier notation when τ and b are independent realisations of s, q_1.

We now complete the proof of Proposition 3.1. Let σ, b_1, c_1 be as fixed prior to Remark 3.4 (so these are all in F). Let $\sigma_1 \in F$ satisfy: $\mathrm{qftp}(\sigma_1/A) = r$ and σ_1 is independent from $\{\sigma, b_1, c_1\}$ over A. (This is easily obtained from assumption (2)). Then $\sigma_1^{-1} \cdot c_1$ is in F, realises q_1 and is independent from σ_1 over A. Similarly $\sigma_1^{-1} \cdot \sigma$ is in $H(F)$, realises s and is independent from σ_1 over A. Let c_2 denote $\sigma_1^{-1} \cdot c_1$ and τ denote $\sigma_1^{-1} \cdot \sigma$. Let $A_1 = \mathrm{acl}(A, \sigma) \cap F$. Then

$$\dim(a, b, c/A_1) = 2n, \ \mathrm{acl}(A_1, \tau) = \mathrm{acl}(A_1, a) \quad \text{and} \quad \mathrm{acl}(A_1, c_2) = \mathrm{acl}(A_1, c).$$

We make a second extension of a similar nature. Let $\tau_1 \in F$ realise s independently from $\{\tau, b_1, c_2\}$ over A_1. Let $\tau_2 = \tau \cdot \tau_1$, $b_2 = \tau_1^{-1} \cdot b_1$ Then $\tau_2 \cdot b_2 = c_2$, and it may be checked that b_2 is independent from $\{\tau, c_2, b_1\}$ over A_1. Let $A_2 = \mathrm{acl}(A_1, b_2) \cap F$. We then clearly have:

$$\dim(a, b, c/A_2) = 2n, \ \mathrm{acl}(A_2, a) = \mathrm{acl}(A_2, T), \ \mathrm{acl}(A_2, b) = \mathrm{acl}(A_2, T_1),$$
$$\mathrm{acl}(A_2, c) = \mathrm{acl}(A_2, \tau_2), \quad \text{and} \quad \tau \cdot \tau_1 = \tau_2.$$

Finally we may shrink A_2 to a finite set over which G and H are defined and with the properties just obtained. This completes the proof of Proposition 3.1. ∎

Proof of 3.1′: In the special case where F is a geometric field, then H is a group definable in $\widetilde{F}$ (algebraic closure of F), defined over $F_0(A)$. In the characteristic 0 case, by 1.8.2 there is an algebraic group H_1 defined over $F_0(A)$ and an $F_0(A)$-definable isomorphism f between H and H_1. But then $f(H(F)) = H_1(F)$, and in the conclusion of 3.1 we may replace H by H_1. In the positive characteristic

case, the proof of 1.8.2 in either [B] or [Po] shows that there is an F-definable isomorphism f between H and an algebraic group H_1 defined over F. Let A_1 be a finite subset of F containing A, such that f and H_1 are defined over the purely inseparable closure of $F_0(A_1)$. By assumption (2) we may assume that the points $\boldsymbol{a}$ and $\boldsymbol{b}$ from the conclusion of 3.1 are generic independent over A_1. This clearly suffices as before.

4. Nash manifolds and groups, and the proofs of Theorems A and B

We first discuss real and p-adic Nash manifolds (although some of this is not really necessary for Theorem A). We consider the real case first. By "definable" we mean definable in the structure $(\mathbb{R}, +, \cdot, 0, 1)$, or equivalently semialgebraic. Recall that a Nash function is an analytic semialgebraic function from an open semialgebraic subset X of $\mathbb{R}^n$ into $\mathbb{R}$. Nash manifolds were introduced in [A-M] and also studied in [Sh]. The latter can be also used as a reference for the definitions below.

Definition 4.1: (i) A (real) n-dimensional Nash manifold is an object $(X, V_1, \ldots, V_k, f_1, \ldots, f_k)$ where

(i) X is a Hausdorff topological space,

(ii) Each V_i is an open subset of X and $X = \bigcup V_i$,

(iii) f_i is a homeomorphism of V_i with an open semialgebraic subset U_i of $\mathbb{R}^n$,

(iv) for each i, j, the homeomorphism induced by $f_i \circ f_j^{-1}$ between $f_j(V_i \cap V_j) \subset U_j$ and $f_i(V_i \cap V_j) \subset U_i$ is Nash (namely each coordinate of the map is a Nash function).

(ii) A Nash map from the Nash manifold $(X, V_1, \ldots, V_k, f_1, \ldots, f_k)$ into the Nash manifold $(Y, W_1, \ldots, W_m, g_1, \ldots, g_m)$ is a continuous map $f\colon X \to Y$ such that for each $1 \leq i \leq k$ and $1 \leq j \leq m$, $U_{ij} = f_i(f^{-1}(W_j) \cap V_i))$ is (open) semialgebraic in U_i and the restriction of $g_j \circ f \circ f_i^{-1}$ to U_{ij} is Nash.

(iii) A Nash manifold X is said to be affine if there is a Nash embedding of X into some $\mathbb{R}^m$.

A few words should be added concerning (iii). If X and Y are Nash manifolds, then by a Nash embedding from X to Y we mean a Nash map f from X to Y which is also an injective immersion (see [S-W]). In this situation $f(X)$ is called a **Nash submanifold** of Y.

If X, Y are Nash manifolds, then the topological space $X \times Y$ has naturally the structure of a Nash manifold.

By a (real) Nash group, we mean a Nash manifold X equipped with a group operation $\bullet$ such that $\bullet$ is a Nash map from $X \times X$ into X and inversion is a Nash map from X into X.

It is not difficult to see that a Nash manifold is in a natural sense interpretable in $\mathbb{R}$, namely think of X as the disjoint union of the U_i, modulo the (definable) equivalence relation E, where $a \in U_i$ is E-equivalent to $b \in U_j$ if $f_i \circ f_j^{-1}(b) = a$. By elimination of imaginaries in $\mathbb{R}$, this interpretable object is in definable bijection with some set Z in some $\mathbb{R}^m$. However, the original topological/Nash structure on X is only reflected "generically" in Z.

On the other hand, in [P2] it is observed that a group G definable in $\mathbb{R}$ can be definably equipped with the structure of a Nash group, or equivalently G is definably isomorphic to a Nash group. This means the following: G begins life as a group interpretable in $\mathbb{R}$, namely (by elimination of imaginaries in $\mathbb{R}$) both G and the graph of the group operation on G are definable sets in $\mathbb{R}^m$, $\mathbb{R}^{3m}$ (some m), and there is a Nash group H, which when viewed as in the above paragraph as definable in $\mathbb{R}$, is definably isomorphic (as a group) to G. So clearly this isomorphism transports the Nash structure on H to a Nash structure on G, with respect to which G is now in particular a topological group. Moreover this Nash structure on G is unique up to Nash isomorphism. It is also remarked in [P2] that G is connected with respect to its Nash group topology if and only if G has no definable subgroup of finite index.

Definition 4.2: A map f from a Nash manifold (X, V_i, f_i) into a Nash manifold (Y, W_j, g_j) is said to be locally Nash if f is continuous and for every $a \in V_i$ there is an open set $V \subset V_i$ containing a, and some j such that $f(V) \subset W_j$, $f_i(V)$ is (open) semialgebraic in U_i and $g_j \circ f \circ f_i^{-1}$ restricted to V is Nash. ∎

Not every locally Nash map between Nash manifolds is Nash. For example we can give the interval $[0, 1)$ the structure of a Nash manifold by identifying 0 and 1. This is exactly what we mean by the Nash manifold $\mathbb{R}/\mathbb{Z}$. The "covering" map π: $\mathbb{R} \to \mathbb{R}/\mathbb{Z}$ is locally Nash but not Nash. (If it were Nash then $\mathbb{Z}$ would be definable in $\mathbb{R}$.)

On the other hand we have ([Sh]):

FACT 4.3: *Let X be a Nash manifold, and X' an affine Nash manifold. Then any locally Nash map from X to X' is Nash.*

The conclusion of 4.3 can also be expressed by saying that any analytic locally

definable map from X to X' is definable.

By Fact 4.3 and the previous remarks, $\mathbb{R}/\mathbb{Z}$ is not an affine Nash group. In fact we can see directly that there are no nonconstant Nash maps of $\mathbb{R}/\mathbb{Z}$ into $\mathbb{R}$. For suppose g is such. Let $\pi\colon \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ be the covering map. Then $g \circ \pi\colon \mathbb{R} \to \mathbb{R}$ is an analytic locally Nash map, such that for some $\pi \in \mathbb{R}$, $X = (g \circ \pi)^{-1}(\pi)$ is an infinite discrete subset of $\mathbb{R}$. As $g \circ \pi$ is locally Nash, there is some open set I in $\mathbb{R}$, and a polynomial $P(x, y)$ such that for all $x \in I$, $P(x, (g \circ \pi)(x)) = 0$. By analytic continuation $P(x, (g \circ \pi)(x)) = 0$ for all $x \in \mathbb{R}$, whereby $g \circ \pi$ is Nash, so X is definable, a contradiction. The reader may be a little confused, imagining that $\mathbb{R}/\mathbb{Z}$ is the circle group, and thus isomorphic to $\mathrm{SO}_2(\mathbb{R})$ (the multiplicative group of complex numbers of norm 1), which is clearly affine. The issue here is that this isomorphism, although analytic, is not Nash or even locally Nash, so is not in our category.

We define a **locally Nash manifold** exactly as in Definition 4.1, except that in (i) we allow there to be infinitely many affine open V_i. A locally Nash manifold is then locally definable, in the obvious sense. The natural class of maps between locally Nash manifolds is then that of locally Nash maps, interpreted as in Definition 4.2. One thus obtains the notion of a locally Nash group. This is useful, as in general the universal covering group of a Nash group will only have the structure of a locally Nash group. In fact Fact 4.3 shows that the universal cover of $\mathrm{SO}_2(\mathbb{R})$ is a locally Nash group which does not have the structure of a Nash group.

Everything we have said above can be done with $\mathbb{Q}_p$ in place of $\mathbb{R}$. One has a notion of p-adic analytic function, and the topology is given by the valuation. Thus we obtain the categories of p-adic Nash manifolds, and p-adic Nash groups. $\mathbb{Q}_p$ does not have elimination of imaginaries. It is nevertheless pointed out in [P3] that if $G \subset \mathbb{Q}_p^n$ is a definable group, then G can be definably equipped with the structure of a p-adic Nash group.

Typical examples of Nash groups are objects of the form $G(\mathbb{R})$ where G is an algebraic group defined over $\mathbb{R}$. In fact:

FACT 4.4: *Let G be a connected algebraic group defined over $\mathbb{R}$. Then $G(\mathbb{R})$ is an affine Nash group.*

Proof: We identify G with its set of $\mathbb{C}$-rational points, $G(\mathbb{C})$. It is well-known that G is quasi-projective, as an abstract variety, namely that there is a bira-

tional isomorphism, defined over $\mathbb{R}$, between G and some algebraic group whose underlying variety is quasi-projective (namely a Zariski open subset of a projective variety). So we may assume G to be a locally closed subset of some complex projective space $\mathbb{CP}^n$. Thus $G(\mathbb{R})$ is clearly a Nash submanifold of $\mathbb{RP}^n$. On the other hand, in [BCR] there is given a rational embedding i of $\mathbb{RP}^n$ into some real affine space $\mathbb{R}^m$ (which is basically stereographic projection). The map i then provides a Nash embedding of $G(\mathbb{R})$ into $\mathbb{R}^m$. Thus $G(\mathbb{R})$ is an affine Nash group. ∎

The reader should be aware that there are two notions of connectedness which we will be using, connectedness as an algebraic group (as in Fact 4.4) and connectedeness as a (real) manifold. For example GL_n is a connected algebraic group, but $\mathrm{GL}_n(\mathbb{R})$ is not connected as a Nash group (the connected component of the identity is the group $\mathrm{GL}_n(\mathbb{R})^0$ of matrices with positive determinant).

We now say a few words about covering spaces, especially in the category of (locally) Nash groups. Let M be a connected topological manifold. Recall that a covering space of M is a connected manifold M' and a continuous map $\pi\colon M' \to M$ such that every point $a \in M$ has an open neighbourhood U such that $\pi^{-1}(U)$ is a disjoint union of open sets, the restriction to each of π being a homeomorphism with U. Every M has a universal cover, namely a simply connected covering space, which is unique in the obvious sense. If M also has a continuous group structure, then its universal cover $(\widetilde{M}, \pi)$ can be equipped with continuous group structure in such a way that π is a homomorphism. In this case $\mathrm{Ker}(\pi)$ is a discrete central subgroup of $\widetilde{M}$ (which is isomorphic to the fundamental group of M).

Remark 4.5: Let G be a connected locally Nash group. Let $(\widetilde{G}, \pi)$ be the universal cover of G. Then $\widetilde{G}$ can be equipped (uniquely) with the structure of a locally Nash group, in such a way that π is a locally Nash homomorphism. ∎

Remark 4.6: Let G be a connected locally Nash group and Z a discrete (and thus central) subgroup of G. Then G/Z can be equipped with the structure of a locally Nash group in such a way that the quotient map $\pi\colon G \to G/Z$ is locally Nash.

LEMMA 4.7: *Let G be a Nash group and Z an infinite discrete subgroup of G. Then G/Z is not an affine Nash group.*

Proof: Let $\pi: G \to G/Z$ be the natural locally Nash homomorphism. If G/Z were affine, then by Fact 4.3, p would be Nash (namely definable), and thus $\ker(p) = Z$ would be definable, which is impossible as Z is infinite and discrete. ∎

On the other hand, the quotient of a locally Nash group by an infinite discrete subgroup may very well be an affine Nash group.

We now proceed to the proofs of Theorems A and B.

Proof of Theorem A: We assume F to be $\mathbb{R}$ or $\mathbb{Q}_p$. Let G be a Nash group over F (which just means a group definable in F, equipped with its unique Nash group structure). Proposition 3.1 applies, so let H, A, a, b, c, a', b', c' be as given there. Let k be the subfield of F generated by A. By Proposition 1.8.2 we may assume that H is an algebraic group defined over k. As a, b, c are each generic points of G over k, we may assume that each is a k-independent n-tuple in F^n, an open neighbourhood in F^n of which lies in G. As $H(F)$ is also a Nash group, we may assume the same for a', b', c'. By 2.15 (ii) a and a' are interdefinable over k in F (namely $a \in \mathrm{dcl}(k, a')$ and $a' \in \mathrm{dcl}(k, a)$), and similarly for b, b' and c, c'.

We now work completely in F

LEMMA 4.8: *There are open k-definable neighbourhoods, U, V and W in G of a, b, c respectively, and U', V', W' in $H(F)$ of a', b', c', and k-definable functions f, g, and h such that*

(i) *$f(a) = a'$ and f is a (Nash) homeomorphism between U and U', $g(b) = b'$ and g is a (Nash) homeomorphism between V and V', and $h(c) = c'$ with h a (Nash) homeomorphism between W and W'.*

(ii) *for a'' in U and b'' in V, $f(a'') \cdot g(b'') = h(a'' \cdot b'')$.*

(iii) *for all $x, z \in U$, $x^{-1} \cdot c \in V$ and $z \cdot x^{-1} \cdot c \in W$.*

Proof of Lemma 4.8: (i) We have that a and a' are interdefinable over k. Thus there is a first order formula $\varphi(x, y)$ with parameters in k such that in F: $\varphi(a, a')$ holds and in addition there is unique x' such that $\varphi(a, x')$ holds, and a unique x such that $\varphi(x, a')$ holds. As $a, a' \in F^n$ and $\dim(a/k) = \dim(a'/k) = n$, there are open neighbourhoods U_1 of a and U_2 of a' such that for $x \in U_1$ there is unique y with $\varphi(x, y)$, and for $y \in U_2$ there is unique x with $\varphi(x, y)$. We thus obtain k-definable functions f: $U_1 \to F^n$ and f^{-1}: $U_2 \to F^n$, where e.g. $f(x)$ is the

unique y such that $\varphi(x, y)$ holds. By Fact 2.15 (i), there is an open dense k-definable subset U_3 of U_1 such that $f \restriction U_3$ is analytic. Similarly there is an open dense K-definable $U_4 \subset U_2$ on which f^{-1} is analytic. Again as $\dim(a/k) = n$, $a \in U_3$, and as $\dim(a'/k) = n$, $a' \in U_4$. Thus we clearly obtain some open U containing a on which f is a Nash homeomorphism with an open neighbourhood U' of a' (and $f(a) = a'$). The same thing can be done for b, b' and c, c' to obtain pairs of neighbourhoods V, V' and W, W', so that (i) is satisfied. Now as $\dim(a, b/k) = 2n$, and $f(a) \cdot g(b) = h(a \cdot b)$, there is an open neighbourhood Z in F^{2n} of (a, b) such that for all $(x, y) \in Z$, $f(x) \cdot g(y) = h(x \cdot y)$. We may shrink U and V such that $U \times V \subset Z$, so now also (ii) holds.

We may shrink U, V further so that $U \cdot V \subset W$ (in the group G). Let $U_1 \subset U$ be an open neighbourhood of a such that $U^{-1} \cdot c \subset V$. Replace U by U_1, and clearly (iii) holds.

COROLLARY 4.9: *The map χ from $U^{-1} \cdot a$ to $(U')^{-1} \cdot a'$ defined by $\chi(x^{-1} \cdot a) = f(x)^{-1} \cdot a'$ is a local isomorphism between a neighbourhood of the identity in G and a neighbourhood of the identity in $H(F)$.*

Proof: Clearly χ is a homeomorphism between $U_1 = U^{-1} \cdot a$ and $U_2 = (U')^{-1} \cdot a'$. We must show that $\chi(x \cdot y) = \chi(x) \cdot \chi(y)$ (for $x, y \in U_1$ such that also $x \cdot y \in U_1$). We require:

CLAIM: *Let $x, y, z \in U$ be such that $x \cdot z^{-1} \cdot y = a$. Then $f(a) = f(x) \cdot f(z)^{-1} \cdot f(y)$.*

Proof of claim: Let $b_1 = x^{-1} \cdot c$ and $c_1 = z \cdot b_1$. By the choice of U and Lemma 3.1 (iii), $b_1 \in V$ and $c_1 \in W$. Moreover clearly $y \cdot b = c_1$. Thus we have, by Lemma 4.8 (ii),

(i) $f(y) \cdot g(b) = h(c_1)$,
(ii) $f(z) \cdot g(b_1) = h(c_1)$, and
(iii) $f(x) \cdot g(b_1) = h(c)$.

Thus $f(x) \cdot f(z)^{-1} \cdot f(y) \cdot g(b) = f(x) \cdot g(b_1) = h(c) = f(a) \cdot g(b)$. Thus the claim is established.

Now let $x \in U$, $y \in U$, and suppose that $x^{-1} \cdot a \cdot y^{-1} = z^{-1}$, with $z \in U$. So $(x^{-1} \cdot a) \cdot (y^{-1} \cdot a) = z^{-1} \cdot a$. Then $\chi(z^{-1} \cdot a) = f(z)^{-1} \cdot f(a) =$ (by the claim) $f(x)^{-1} \cdot f(a) \cdot f(y)^{-1} \cdot f(a) = \chi(x^{-1} \cdot a) \cdot c(y^{-1} \cdot a)$. This proves the Corollary.

Theorem A is proved. ∎

We now aim towards the proof of Theorem B. We need the following information on the structure of commutative real algebraic groups. We imagine this to

be well-known, but give a brief proof nevertheless.

LEMMA 4.10: *Let G be the connected component of the real points of a connected commutative algebraic group defined over $\mathbb{R}$. Then $G = G_1 \times G_2 \times G_3$, where G_1 is rationally isomorphic to a product of copies of $(\mathbb{R}, +)$, G_2 is rationally isomorphic to a product of copies of $(\mathbb{R}_{>0}, \cdot)$, and G_3 is closed and compact. (So G_1 and G_2 are semialgebraic, but G_3 need not be.)*

Proof: G is on the one hand a group definable in $\mathbb{R}$ (in fact a Nash group). Let $\dim(G) = n$. On the other hand G is also a connected commutative Lie group of the same dimension n. Thus

(*) G is as a Lie group isomorphic to $\mathbb{R}^m \times \mathbb{T}^k$

where $\mathbb{R}$ is $(\mathbb{R}, +)$ and $\mathbb{T}$ is the 1-dimensional torus (or circle group). (See for example [S-W]). Clearly $n = m + k$. Let H be a connected commutative complex algebraic group, defined over $\mathbb{R}$, such that $G = H(\mathbb{R})^0$. By Chevalley's theorem there is a connected affine algebraic normal subgroup H_1 of H which is defined over $\mathbb{R}$ and such that H/H_1 is an abelian variety. The Jordan decomposition of H_1 yields $H_1 = H_2 \times H_3$ where H_2 is a (connected) commutative unipotent algebraic group defined over $\mathbb{R}$ and H_3 is a connected commutative diagonalisable group defined over $\mathbb{R}$. (see [Bor] Theorem 4.7.) Clearly $H_1(\mathbb{R}) = H_2(\mathbb{R}) \times H_3(\mathbb{R})$.

Now, by [Bor], H_2 is isomorphic, by a rational map defined over $\mathbb{R}$, to some vector group $\mathbb{C}^r$. It follows that $H_2(\mathbb{R})$ is isomorphic, by the same rational map, to $\mathbb{R}^r$.

Now we look at the connected diagonalisable group H_3. By [Bor] (Proposition 8.15) $H_3 = H_4 \cdot H_5$, where H_4, H_5 are connected algebraic subgroups of H_3, defined over $\mathbb{R}$, H_4 is $\mathbb{R}$-split (namely diagonalisable over $\mathbb{R}$), H_5 is anisotropic over $\mathbb{R}$ (namely there is no nontrivial $\mathbb{R}$-rational map of H_5 into $\mathbb{C}^*$), and $H_4 \cap H_5$ is finite. By looking at the $\mathbb{R}$-rational characters of H_3, it is not difficult to see that $H_3(\mathbb{R}) = H_4(\mathbb{R}) \cdot H_5(\mathbb{R})$ (and of course $H_4(\mathbb{R}) \cap H_5(\mathbb{R})$ is finite). Now $H_4(\mathbb{R})$ is isomorphic by a rational map to $(\mathbb{R}^*)^s$ for some s. Thus

(i) $H_4(\mathbb{R})^0$ (the connected component of $H_4(\mathbb{R})$ in the real topology) is isomorphic by the same rational map to $(\mathbb{R}^*_{>0})^s$.

By [Bor] (24.6), $H_5(\mathbb{R})$ is compact and connected, and thus

(ii) $H_5(\mathbb{R})$ is as a Lie group isomorphic to $\mathbb{T}^t$ for some t.

Finally $(H/H_1)(\mathbb{R})$, the set of real points of the abelian variety H/H_1 is a compact Lie group which contains $H(\mathbb{R})/H_1(\mathbb{R})$ as a closed subgroup. Thus $H(\mathbb{R})/H_1(\mathbb{R})$

is a compact Lie group. Now $K = H_2(\mathbb{R}) \times H_4(\mathbb{R})^0 \times H_5(\mathbb{R})$ is connected and thus contained in $G = H(\mathbb{R})^0$. The projection map $H(\mathbb{R})/K \to H(\mathbb{R})/H_1(\mathbb{R})$ is finite to one, and thus $H(\mathbb{R})/K$ is also a compact Lie group. As $H(\mathbb{R})^0/K$ is a closed subgroup of finite index in $H(\mathbb{R})/K$ we obtain

(iii) G/K is as a Lie group isomorphic to $\mathbb{T}^u$ for some u.

Let us put $G_1 = H_2(\mathbb{R})$ and $G_2 = H_3(\mathbb{R})^0$. So $K = G_1 \times G_2 \times H_5(\mathbb{R})$. Note that

(**) $n = \dim(G) = \dim(G_1 \cdot G_2) + t + u$.

Now K is a divisible subgroup of the commutative group G, and is thus a direct summand. Thus (by iii)) $G \cong K \times \mathbb{T}^u$ as an abstract group. So we have

(iv) As an abstract group $G \cong G_1 \times G_2 \times \mathbb{T}^{t+u}$.

On the other hand, by (*) at the beginning of the proof

(v) $G = A \cdot B$ where A, B are closed subgroups, and as Lie groups A is isomorphic to $\mathbb{R}^m$, B is isomorphic to $\mathbb{T}^k$ (and $A \cap B = \{1\}$). Comparing say the number of elements of order 2 in the two expressions in (iv) and (v) for G we see that $k = t + u$. Now clearly $(G_1 \cdot G_2) \cap B = \{1\}$ (as the intersection is a closed and thus compact subgroup of B, so has torsion elements, whereas $G_1 \cdot G_2$ is torsion-free). Thus the Lie subgroup $G_1 \times G_2 \times B$ of G has dimension $\dim(G_1 \cdot G_2) + k$ which equals $\dim(G)$. As G is connected, $G = G_1 \times G_2 \times B$. This completes the proof of the lemma. ∎

Proof of Theorem B: Let G be our connected affine Nash group. Let (by Theorem A) H be the connected component of the real points of an algebraic group defined over $\mathbb{R}$, and f a Nash isomorphism between a neighbourhood U_1 of the identity in G with a neighbourhood U_2 of the identity in H. Let $\widetilde{G}$, $\widetilde{H}$ be the universal covering groups of G, H, respectively, with covering homomorphisms $p_1\colon \widetilde{G} \to G$ and $p_2\colon \widetilde{H} \to H$, where by Remark 4.5 we can take everything to be locally Nash. f lifts to a unique locally Nash isomorphism $\tilde{f}\colon \widetilde{G} \to \widetilde{H}$ (with $p_2 \circ \tilde{f} = f \circ p_1$ on a neighbourhood of identity of $\widetilde{G}$). Let $D_1 = \ker(p_1)$ and $D_2 = \ker(p_2)$.

Let $Z(G)^0$, $Z(H)^0$ be the connected components of the centres of G, H respectively. Easily $Z(H)^0$ is the connected component of the real points of a commutative algebraic group defined over $\mathbb{R}$, so Lemma 4.10 applies, giving us $Z(H)^0 = H_1 \times H_2 \times H_3$, where the H_i are subgroups of $Z(H)^0$ with H_1 definable and isomorphic to a product of copies of $\mathbb{R}$, H_2 definable and isomorphic to a product of copies of $\mathbb{R}^*_{>0}$, and H_3 closed and compact. In particular H_1 and H_2 are affine Nash groups. Then $p_2\colon Z(\widetilde{H})^0 \to Z(H)^0$ is a covering homomorphism.

But $H_1 \times H_2$ is simply connected, and so we can write $Z(\widetilde{H})^0$ as $\widetilde{H}_1 \times \widetilde{H}_2 \times \widetilde{H}_3$ with p_2: $\widetilde{H}_i \to H_i$ an isomorphism for $i = 1, 2$ and p_2: $\widetilde{H}_3 \to H_3$ a covering homomorphism. So clearly

(i) $D_2 \cap Z(\widetilde{H})^0$ is a discrete subgroup of $\widetilde{H}_3$.

Let $\widetilde{G}_1$, $\widetilde{G}_2$, $\widetilde{G}_3$ be the preimages of $\widetilde{H}_1$, $\widetilde{H}_2$, $\widetilde{H}_3$ under $\tilde{f}$. Then $Z(\widetilde{G})^0 = \widetilde{G}_1 \times \widetilde{G}_2 \times \widetilde{G}_3$.

Now $f^{-1}(U_2 \cap H_1)$ is a semialgebraic set in G which generates (as remarked at the end of [P4]), a definable connected subgroup G_1 of G. Moreover $p_1.(\tilde{f})^{-1}.p_2^{-1}$ restricted to H_1 defines a covering map f_1: $H_1 \to G_1$ (agreeing with f^{-1} on $U_2 \cap H_1$). f_1 is locally Nash and G_1, H_1 are affine Nash groups, so by Lemma 4.7, $\ker(f_1)$ is finite, and thus (as H_1 is a product of copies of $\mathbb{R}$), trivial. It follows that p_1: $\widetilde{G}_1 \to G_1$ is an isomorphism. Similarly p_1: $\widetilde{G}_2 \to G_2$ is an isomorphism. Thus again

(ii) $D_1 \cap Z(\widetilde{G})^0$ is a discrete subgroup of $\widetilde{G}_3$.

Now clearly $\tilde{f}$ induces a locally Nash covering homomorphism g: $\widetilde{G}/D_1 \to (\widetilde{H}/D_2)/(\tilde{f}(D_1)/D_2))$, namely g: $G \to H/D_3$, where D_3 is $\tilde{f}(D_1)/D_2$.

CLAIM: *D_3 is finite.*

Proof of claim: Now D_3 is in $Z(H)$, the centre of H, and $Z(H)^0$ has finite index in $Z(H)$. So it suffices to see that $D_3 \cap Z(H)^0 = D_4$ is finite. But by (i) and (ii) D_4 is a discrete subgroup of the compact group H_3. Thus D_4 is finite. The claim is proved.

Let H_4 be a connected algebraic group defined over $\mathbb{R}$ such that H is $H_4(R)^0$. Then H_4/D_3 is a connected algebraic group defined over $\mathbb{R}$, and moreover $H/D_3 = (H_4/D_3)(R)^0$. In particular H/D_3 is an affine Nash group. By Lemma 4.7 $\mathrm{Ker}(g)$ is finite, and by Fact 4.3, g is Nash (definable). Thus g is a Nash isogeny between G and the connected component of the real points of an algebraic group defined over $\mathbb{R}$. This completes the proof of Theorem B. ∎

One can not do without the finite kernel in Theorem B. For example $\mathrm{SL}_2(\mathbb{R})$ has finite covering groups, which can be equipped with the structure of affine Nash groups, but are known to be not even analytically embeddable into algebraic groups.

5. Local stability theory and geometric structures

We will review stability theory and stable group theory in its local form, with outlines of proofs, and we then make some remarks on the interaction of the resulting notion of independence with the dimension-theoretic notion of independence in the case of geometric structures. We divide the section into two subsections, the first giving an exposition of the local stability theory and the second applying this to geometric structures. The more experienced stability-theorist can thus skip the first section.

5S. LOCAL STABILITY THEORY The fact that stability theory can be developed within a Booleanly closed set of stable formulas (rather than in a globally stable theory) was pointed out in [P1]. Here we give a treatment from first principles of this theory, due largely to the first author, but incorporating also the point of view of [P1].

Let T be some complete theory in a language L. We work inside a large saturated model $\mathbb{M}$ of T. M, N etc. denote small elementary submodels of T. x,y, etc. denote tuples of variables. Let $\delta(x, y)$ be some L-formula. By an instance of δ we mean a formula of the form $\delta(x, a)$, for some a in $\mathbb{M}$. By a δ-formula we mean a formula which is equivalent to some Boolean combination of instances of δ. If A is a subset of $\mathbb{M}$ then by a δ-A-formula we mean a formula over A which is also a δ-formula. By a complete δ-type over A we mean a maximal consistent (with $\mathbb{M}$) set of δ-A-formulas. The set of such complete δ-types over A is denoted $S_\delta(A)$. If $p(x) \in S(A)$ (namely $p(x)$ is a complete type over A in the variable x), then $p|\delta$ denotes the set of δ-formulas in p. (So $p|\delta \in S_\delta(A)$.) Note that if $\mathbb{M}$ is a model, and $p(x) \in S_\delta(\mathbb{M})$, then p is determined by the set of instances of δ and $\neg\delta$ which are in p. If $q(x)$ is a (possibly incomplete) type over B and A is a subset of B, then $q|A$ denotes the set of formulas in q which are over A.

Definition 5.1: Let $p \in S_\delta(M)$. p is said to be **definable** if there is a formula $\varepsilon(y)$ over M such that for all a in M, $\delta(x, a) \in p$ iff $\models \varepsilon(a)$. If such a formula ε exists then it is unique up to equivalence. If $p = q|\delta$ where $q(x) \in S(M)$, we call ε the δ-definition of q.

Definition 5.2: The formula $\delta(x, y)$ is said to be **stable** if there do not exist a_i, b_i (in $\mathbb{M}$), for $i < \omega$ such that $\models \delta(a_i, b_j)$ iff $i < j$ (for all $i, j < \omega$). (Note that this definition depends on a fixed division of the variables in δ.) The theory T is said to be **stable** if every formula $\varphi(w, z)$ of L is stable.

Remark 5.3:

(i) If $\delta(x,y)$ is stable, then so is $\delta'(y,x) = \delta(x,y)$.

(ii) If $\delta(x,y)$ is stable, then there is $n < \omega$ such that there do not exist a_i, b_i for $i < n$ such that $\models \delta(a_i, b_j)$ iff $i < j$ $(i,j < n)$.

(iii) If $\delta_1(x,y_1)$ and $\delta_2(x,y_2)$ are stable formulas, and $\delta_3(x,y_1,y_2)$ is some Boolean combination of δ_1 and δ_2, then $\delta_3(x,(y_1,y_2))$ is stable.

We now fix a stable formula $\delta(x,y)$.

LEMMA 5.4: *Let $p(x) \in S(M)$. Then*

(i) *$p|\delta$ is definable.*

(ii) *There are $c_1,\ldots,c_k$ in M such that the δ-definition of p is equivalent to some positive Boolean combination of the $\delta(c_i,y)$.*

(iii) *If A is a subset of M and M is $|A|^+$-saturated, then the elements $c_1,\ldots,c_k$ above can be chosen so that c_i realises $p \vdash (A \cup \{c_1,\ldots,c_{i-1}\})$ for each i.*

Proof: We sketch the proof of (ii), from which the proof of (iii) will also be apparent. Let c^* realise $p(x)$. By 5.3 let n be such that there do not exist a_i, b_i, $i < n$ such that $\models \delta(a_i,b_j)$ if $i < j$, and similarly for $\neg\delta(x,y)$. We define inductively, finite subsets A_i, B_i of M and elements c_i in M (for $i = 0,1,2,\ldots$) such that

(a) Whenever W is a subset of $\{0,\ldots,k-1\}$ and for some a in M, $\models \bigwedge\{\delta(c_j,a)\colon j \in W\}$ but $\models \neg\delta(c^*,a)$, then some such a is in A_k.

(b) Whenever W is a subset of $\{0,\ldots,k-1\}$ and for some b in M, $\models \bigwedge\{\neg\delta(c_j,b)\colon j \in W\}$ but $\models \delta(c^*,b)$, then some such b is in B_k.

(c) For all $\delta \in \bigcup\{A_i\colon i \le k\} \cup \bigcup\{B_i\colon i \le k\}$, $\models \delta(ck,\delta)$ iff $\models \delta(c^*,\delta)$.

The reader is left to check (using our choice of n) that

(I) If $a \in M$ and for some n-element subset W of $\{0,\ldots,2n\}$, $\models \bigwedge\{\delta(c_j,a)\colon j \in W\}$, then $\models \delta(c^*,a)$.

(II) If $a \in M$ and for some n-element subset W of $\{0,\ldots,2n\}$, $\models \bigwedge\{\neg\delta(c_j,a)\colon j \in W\}$, then $\models \neg\delta(c^*,a)$.

It clearly follows from (I) and (II) that for each $a \in M$, $\delta(x,a) \in p(x)$ iff $\models \bigvee\{\bigwedge\{\delta(c_j,a)\colon j \in W\}\colon W$ a subset of $\{0,\ldots,2n\}$ and $|W| = n\}$.

LEMMA 5.5: *Let $p(x)$ be a complete type over A, and $M \supseteq A$ be a model. Then there is some $q(x) \in S_\delta(M)$ such that $p(x) \cup q(x)$ is consistent and the δ-definition of q is over $\mathrm{acl}^{eq}(A)$.*

Proof: Here $\mathrm{acl}^{\mathrm{eq}}(A)$ denotes $\{c \in \mathbb{M}^{\mathrm{eq}}: c \in \mathrm{acl}(A)\}$; and note that $\mathrm{acl}^{\mathrm{eq}}(A)$ is contained in M^{eq}.

First a Lowenheim–Skolem argument allows us to assume that $A = \emptyset$, L is countable and M is countable and recursively saturated. Now every complete δ-type over M is clearly determined by its definition (which exists by Lemma 5.4). Thus $S_\delta(M)$ is countable. In particular $X = \{q(x) \in S_\delta(M)$: $q(x) \cup p(x)$ is consistent$\}$ is countable, and is also a compact Hausdorff space under the usual totally disconnected topology. It is then well-known that every point in X has some Cantor–Bendixon rank, there is a maximal such CB-rank α, and moreover the set X_0 of points in X with CB-rank α is finite and nonempty. Note that $\mathrm{Aut}(M)$ acts on X (as a group of homeomorphisms), and thus X_0 is fixed setwise under $\mathrm{Aut}(M)$. Let $q \in X_0$, and let $\varepsilon(y)$ be the δ-definition of q. If $f \in \mathrm{Aut}(M)$, then $f(q) \in X_0$ and $f(q)$ has definition $f(\varepsilon)$. So $\varepsilon(y)$ has finitely many images (up to equivalence) under $\mathrm{Aut}(M)$. Our saturation assumption on M implies that $\varepsilon(y)$ is almost over $\emptyset$, namely over $\mathrm{acl}^{\mathrm{eq}}(\emptyset)$. ∎

Definition 5.6: If $q(x) \in S_\delta(M)$, A is a subset of M and the δ-definition of q is over $\mathrm{acl}^{\mathrm{eq}}(A)$, we will say that q **does not fork over** A, or that q **is a nonforking extension of** $q|A$. (So Lemma 5.5 gives the existence of nonforking extensions.) If $q(x) \in S_\delta(B)$ and $A \subset B$ we say that q **does not fork over** A if q has some extension $r \in S_\delta(M)$ to a model M, which does not fork over A.

LEMMA 5.7: *Let $\delta'(y, x)$ be the formula $\delta(x, y)$. Let $p(x) \in S_\delta(M)$ and $q(y) \in S_{\delta'}(M)$. Let $\varepsilon(y)$ be the δ-definition of p, and $\sigma(x)$ the δ'-definition of q. Then $\sigma(x) \in p(x)$ iff $\varepsilon(y) \in q(y)$.*

Proof: Let us first remark that $\varepsilon(y)$, the δ-definition of $p(x)$, is by 5.4, a δ'-formula over M, so either ε or $\neg\varepsilon$ is in $q(y)$. Similarly either σ or $\neg\sigma$ is in p.

We may assume that both p, q are definable over some subset A of M and that M is $|A|^+$-saturated. Suppose by way of contradiction that $\neg\sigma(x) \in p$, but $\varepsilon(y) \in q$. Define a_i, b_i in M for $i = 0, 1, 2, \ldots$, as follows: a_i realises $p|(A \cup \{b_0, \ldots, b_{i-1}\})$ and b_i realises $q|(A \cup \{a_0, \ldots, a_i\})$. Then we see that $\models \delta(a_i, b_j)$ iff $i > j$, contradicting the stability of δ. This proves the lemma. ∎

LEMMA 5.8: *Let $p_1(x)$, $p_2(x) \in S_\delta(M)$ both be definable over A, where $A = \mathrm{acl}^{\mathrm{eq}}(A)$ is contained in M^{eq}. Suppose $p_1|A = p_2|A$. Then $p_1 = p_2$.*

Proof: Let $b \in M$. We must check that $(*)$ $\delta(x,b) \in p_1$ iff $\delta(x,b) \in p_2$. Let $q_0(y)$ be the complete δ'-type of b over A. By Lemma 5.5, there is $q(y) \in S_{\delta'}(M)$ which extends $q_0(y)$ and whose δ'-definition is over A. Let $\varepsilon_i(y)$ be the δ-definition of $p_i(x)$, for $i = 1, 2$, and let $\sigma(x)$ be the δ'-definition of q. So ε_1, ε_2 and σ are all over A. By 5.7,

$$\varepsilon_1(y) \in q \quad \text{iff } \sigma(x) \in p_1 \quad \text{iff } \sigma(x) \in p_2 \quad \text{iff } \varepsilon_2(y) \in q.$$

But

$$\varepsilon_i(y) \in q \quad \text{iff } \models \varepsilon_i(b).$$

Thus

$$\models \varepsilon_1(b) \quad \text{iff } \models \varepsilon_2(b)$$

which yields $(*)$. ∎

For the next lemma we use the following notation : $\mathrm{Aut}_A(B)$ is the set of permutations of B induced by elementary maps which fix A pointwise. $\mathrm{FER}_\delta(A)$ denotes the collection of formulas $E(x_1, x_2)$ over A which define an equivalence relation with finitely many classes, and such that for each a, $E(x, a)$ is a δ-formula.

LEMMA 5.9: *Let $p(x) \in S_\delta(A)$, and $M \supseteq A$. Let $X = \{q(x) \in S_\delta(M)$: q is a nonforking extension of $p\}$. Then*

(i) *X is finite,*

(ii) *Assuming M to be sufficiently homogeneous, $\mathrm{Aut}_A(M)$ acts transitively on X,*

(iii) *there is some $E(x_1, x_2) \in \mathrm{FE}_\delta(A)$ such that for all q_1, $q_2 \in X$, $q_1 = q_2$ iff $q_1(x_1) \cup q_2(x_2) \vdash E(x_1, x_2)$.*

Proof: Let $Y = \{q|(\mathrm{acl}^{\mathrm{eq}}(A))$: $q \in X\}$.

CLAIM: $\mathrm{Aut}_A(\mathrm{acl}^{\mathrm{eq}}(A))$ acts transitively on Y.

Proof of Claim: Let $p_1(x)$ be some complete type over A extending $p(x)$. Let $q(x) \in Y$. Then $p_1(x) \cup q(x)$ is consistent: for otherwise $p_1(x) \vdash \neg\psi(x)$ for some ψ in q. Let $\chi(x)$ be the (finite) disjunction of the conjugates of $\psi(x)$ under $\mathrm{Aut}_A(\mathrm{acl}^{\mathrm{eq}}(A))$. So clearly $p_1(x) \vdash \neg\chi(x)$. But $\chi(x)$ is a δ-A-formula, which is in $q(x)$ so also in $p(x)$, and this is a contradiction. So we see that $p_1(x) \cup q(x)$ is consistent. This clearly proves the claim.

The claim, together with Lemma 5.8 proves (ii). For (i) and (iii) we may assume M to be sufficiently homogeneous. Fix $q_0 \in X$. Let $\varepsilon(y)$ be the δ-definition of q_0. Then ε is over $\mathrm{acl}^{\mathrm{eq}}(A)$, so has only finitely many images (up to equivalence) under $\mathrm{Aut}_A(M)$. But if $f \in \mathrm{Aut}_A(M)$, then clearly $f(\varepsilon)$ is the δ-definition of $f(q_0)$ (and clearly $f(q_0) \in X$ too). By (ii) we conclude that X is finite (and moreover X is parameterised by the A-conjugates of $\varepsilon(y)$). So (i) is proved.

For (iii): as X is finite and using again 5.8, there is a finite collection $\Phi(x)$ of δ-formulas over $\mathrm{acl}^{\mathrm{eq}}(A)$, such that for $q_1, q_2 \in X$, $q_1 = q_2$ iff for each $\varphi(x) \in \Phi$, $\varphi(x) \in q_1$ iff $\varphi(x) \in q_2$. We may assume that Φ is closed under A-automorphisms. Let $E(x_1, x_2)$ be the formula $\bigwedge\{\varphi(x_1) \leftrightarrow \varphi(x_2)\colon \varphi \in \Phi\}$. Then E is clearly in $\mathrm{FE}_\delta(A)$ and satisfies (iii). ∎

Definition 5.10: Let $\delta(x, a)$ be an instance of δ. We say that $\delta(x, a)$ **does not fork over** A, if for some model M containing $A \cup \{a\}$, there is $p(x) \in S_\delta(M)$ which contains $\delta(x, a)$ and does not fork over A.

LEMMA 5.11:

(I) *The following are equivalent:*
  (i) $\delta(x, a)$ *does not fork over* A,
  (ii) *some positive Boolean combination of* A*-conjugates of* $\delta(x, a)$ *is consistent and* A*-definable,*
  (iii) *any set of* $\mathrm{acl}^{\mathrm{eq}}(A)$*-conjugates of* $\delta(x, a)$ *is consistent.*

(II) *Moreover, if* $\delta(x, a)$ *forks over* A*, then there is an* A*-indiscernible sequence* $(a_i\colon i < \omega)$ *with* $\mathrm{tp}(a_i/A) = \mathrm{tp}(a/A)$*, such that* $\{\delta(x, a_i)\colon i < \omega\}$ *is inconsistent.*

Proof: We first make some constructions and observations. Let $A_1 = \mathrm{acl}^{\mathrm{eq}}(A)$, and let $q(y) = \mathrm{tp}(a/A_1)$. Let M be some $|A|^+$-saturated model containing $A \cup \{a\}$. By Lemma 5.6 let $q^*(y) \in S_{\delta'}(M)$ be a complete δ'-type over M which is definable over A_1 and is consistent with $q(y)$. Let $\sigma(x)$ be the δ'-definition of q^*. Let a^* realise $q(y) \cup q^*(y)$. By Lemma 5.4 (iii), $\sigma(x)$ is equivalent to a positive Boolean combination of formulas $\delta(x, a')$ where $\mathrm{tp}(a'/A_1) = \mathrm{tp}(a^*/A_1) = q(y)$. Namely

(*) $\sigma(x)$ is equivalent to a positive Boolean combination of A_1-conjugates of $\delta(x, a)$, and $\sigma(x)$ is over A_1.

Now we prove (I).

(i)→(ii): Suppose now that $\delta(x,a)$ does not fork over A. Then there is clearly $p(x) \in S_\delta(M)$ which does not fork over A and contains $\delta(x,a)$. Let $\varepsilon(y)$ be the δ-definition of $p(x)$. By 5.7, $\sigma(x) \in p(x)$ iff $\varepsilon(y) \in q^*(y)$. But, as $\delta(x,a) \in p$, we clearly have that $\models \varepsilon(a)$, and thus (as $\mathrm{tp}(a^*/A) = q(y) = \mathrm{tp}(a/A)$) also $\models \varepsilon(a^*)$. Thus $\varepsilon(y) \in q^*(y)$. So $\sigma(x) \in p(x)$, and $\sigma(x)$ is in particular consistent. Take $\sigma'(x)$ to be the disjunction of the (finite number of) A-conjugates of $\sigma(x)$. Then $\sigma'(x)$ is consistent, and by $(*)$ is also a positive Boolean combination of A-conjugates of $\delta(x,a)$. So (ii) holds.

(iii)→(i): Assuming (iii) is true, we have in particular that $\sigma(x)$ is consistent. So $\sigma(x)$ is a consistent δ-formula over A_1. Let $p(x) \in S_\delta(A_1)$ contain σ, and let (by 5.6) $p^*(x) \in S_\delta(M)$ be a nonforking extension of p. Let $\varepsilon(y)$ be the δ-definition of $p^*(x)$. Again by 5.7, we deduce that $\varepsilon(y) \in q^*(y)$. In particular $\models \varepsilon(a^*)$. Thus also $\models \varepsilon(a)$, whereby $\delta(x,a) \in p^*$. Thus (as p^* does not fork over A), we see that $\delta(x,a)$ does not fork over A.

(ii)→(iii): Assuming (ii), let $\sigma(x)$ be a consistent formula over A which is a positive Boolean combination of A-conjugates of $\delta(x,a)$. Let $p(x) \in S_\delta(A)$ contain $\sigma(x)$, and let $p^*(x) \in S_\delta(M)$ be a nonforking extension of p, where M is sufficiently saturated and homogeneous. As $\sigma(x) \in p^*$ it is clear that some A-conjugate of $\delta(x,a)$, say $\delta(x,a')$ is in p^*. Let f be an A-automorphism of M such that $f(a') = a$. Then $f(p^*) = p^{**}$ is also a nonforking extension of p, and moreover contains $\delta(x,a)$. Now the δ-definition of p^* is over $\mathrm{acl}^{\mathrm{eq}}(A)$, so in particular whenever $a'' \in M$ with $\mathrm{tp}(a''/\mathrm{acl}^{\mathrm{eq}}(A)) = \mathrm{tp}(a/\mathrm{acl}^{\mathrm{eq}}(A))$, then $\delta(x,a'') \in p^*$. Thus any set of conjugates of $\delta(x,a)$ under A-automorphisms of M is consistent. As M is saturated, we can also conclude (iii).

Proof of (II): We slightly modify the construction at the beginning of this proof. M is again a very saturated model of T containing A. $q(y) = \mathrm{tp}(a/A_1)$ and $q^*(y) \in S_\delta(M)$ and a^* realising $q(y) \cup q^*(y)$ are as before. Let $N < M$ be a "small" model containing A. Let $q_1(y) = \mathrm{tp}(a^*/N)$. Then q^* is definable over A_1, so clearly every formula in q^* does not fork over N. Then, using part (I) we see that $q_1(y) \cup q^*(y)$ is finitely satisfiable in N (namely every formula in $q_1(y) \cup q^*(y)$ is satisfied by some element in N). Then easily $q_1(y) \cup q^*(y)$ extends to a complete type $r(y) \in S(M)$ which is finitely satisfiable in N. Let $\sigma(x)$ as before be the δ'-definition of q^* (= the δ'-definition of $r(y)$). By Lemma 5.4 (iii), $\sigma(x)$ is equivalent to some positive Boolean combination of $\delta(x,a_1), \ldots, \delta(x,a_k)$

where a_i realises $r|(N \cup \{a_1, \ldots, a_{i-1}\})$. Let $(a_i : i < \omega)$ extend $a_1, \ldots, a_k$ such that for all $i < \omega$, a_i realises $r|(N \cup \{a_1, \ldots, a_{i-1}\})$. It is easy to see (using the finite satisfiability of r in N) that

$(**)$ $\qquad (a_i : i < \omega)$ is N-indiscernible.

Now assuming that $\delta(x, a)$ forks over A, it follows (as in the proof of (iii)→(i) above) that $\sigma(x)$ is inconsistent. Thus $\{\delta(x, a_1), \ldots, \delta(x, a_k)\}$ is inconsistent. By $(**)$ this proves (II). ∎

Remark 5.12: All the above theory works in the following more general situation. Let T again be a complete theory in language L, and $\mathbb{M}$ a big saturated model (universal domain) of T. Let $\Phi(x)$, $\Psi(y)$ be partial types over $\emptyset$. Let $\delta(x, y)$ be an L-formula. We say $(\delta(x, y), \Phi(x), \Psi(y))$ is **stable** if there do not exist a_i, b_i (in $\mathbb{M}$) for $i < \omega$, such that $\models \Phi(a_i)$ and $\models \Psi(b_i)$ for all i, and $\models \delta(a_i, b_j)$ iff $i < j$. The best way of seeing the generalisation is to now view the variable x as ranging over realisations of Φ, and the variable y as ranging over realisations of Ψ. An **instance** of (δ, Φ, Ψ) is then a **partial type** of the form $\{\delta(x, a)\} \cup \Phi(x)$ where a satisfies $\Psi(y)$. Similarly a (δ, Φ, Ψ)-formula is a partial type of the form $\{\text{Boolean combination of some } \delta(x, a_i)\} \cup \Phi(x)$ where the a_i satisfy $\Psi(y)$. A (δ, Φ, Ψ)-formula is said to be over A if its solution set is fixed setwise by A-automorphisms. $S_{(\delta, \Phi, \Psi)}(A)$ is then the set of maximal consistent sets of (δ, Φ, Ψ)-formulas which are over A. Work with ω-saturated models instead of arbitrary models. Then with these substitutions, the above results 5.4–5.11 remain valid. ∎

The reader should note that the language of forking was also used in earlier sections in connection with strongly minimal structures D. In fact if D is strongly minimal, then D is stable, and for any $A \subset B$ in D and $\boldsymbol{a} \in D^n$, $\dim(\boldsymbol{a}/A) = \dim(\boldsymbol{a}/B)$ iff for all formulas $\delta(\boldsymbol{x}, \boldsymbol{y})$ of the language the complete δ-type of a over B does not fork over A. In fact this will be a consequence of Lemma 5.19 below. In any case it should be noted that there is no contradiction between the current language and that of earlier sections.

The context of 5.12 yields an elegant theory for definable homogeneous spaces, which we will now outline.

Context: In L there are formulas $G(z)$, $S(x)$, $\chi(z_1, z_2, z_3)$, and $\xi(z, x_1, x_2)$ such that the theory T says: "χ defines the graph of a group operation on $G(z)$" and

"ξ defines the graph of a transitive group action of $G(z)$ on $S(x)$". We write both the group operation and group action as $z_1 \cdot z_2$ and $z \cdot x$. We assume all the above formulas are without additional parameters. We sometimes identify $G(z)$ with its locus $G^{\mathbb{M}}$, and similarly for $S(x)$.

Definition 5.13: Let $\delta(x, y)$ be a L-formula such that $\vdash \delta(x, y) \to S(x)$. We say that $\delta(x, y)$ is an **equivariant formula** if for every a in $\mathbb{M}$, and $c \in G^{\mathbb{M}}$ there is b in $\mathbb{M}$ such that $\models \delta(c.x, a) \leftrightarrow \delta(x, b)$.

Note that if X is the subset of S defined by $\delta(x, a)$, and $c \in G$ then $c \cdot X$ is the set defined by $\delta(c^{-1} \cdot x, a)$.

We now assume that $\delta(x, y)$ is a stable, equivariant formula. It follows that if $\varphi(x)$ is a δ-formula (with parameters) then for any $c \in G$, $\varphi(c \cdot x)$ is also a δ-formula. So clearly if $p(x) \in S_\delta(M)$ and $c \in G^M$, then $c \cdot p = \{\varphi(c^{-1} \cdot x)\colon \varphi(x) \in p\} \in S_\delta(M)$. Namely G^M acts on $S_\delta(M)$.

Definition 5.14:

(i) Let $\varphi(x)$ be a δ-formula. We say that φ is generic if finitely many G-translates of $\varphi(x)$ cover S, namely there are $c_1, \ldots, c_n$ in G such that $\models S(x)\varphi(c_1^{-1} \cdot x) \vee \cdots \vee \varphi(c_n^{-1} \cdot x)$.

(ii) For any set A, and $p(x) \in S_\delta(A)$ we say that $p(x)$ is generic if every formula in $p(x)$ is generic.

LEMMA 5.15: *Let $\varphi(x)$ be a δ-formula. Then either $\varphi(x)$ or $\neg\varphi(x)$ is generic.*

Proof: Let $\mathbb{M}_0$ be the following "relativised reduct" of $\mathbb{M}$. $\mathbb{M}_0$ has predicates $G(z)$, $S(x)$, $\lambda(x, z)$, where $\lambda(x, z)$ holds in $\mathbb{M}_0$ iff $\varphi(z^{-1} \cdot x)$ holds in M. Let $T^0 = \mathrm{Th}(\mathbb{M}_0)$. It is clear that $\lambda(x, z)$ is stable for T_0. It is easy to check that

(I) for any $g \in G$, the map which takes $a \in G$ to $g \cdot a$ and $b \in S$ to $g.b$ is an automorphism of $\mathbb{M}_0$.

Thus (by transitivity of the original action of G on S)

(II) In T_0, $S(x)$ determines a unique 1-type.

Let 1 denote the identity element of G. Working in T_0 we have that either $\lambda(x, 1)$ or $\neg\lambda(x, 1)$ does not fork over $\emptyset$. In the first case, by Lemma 5.11, some positive Boolean combination of $\emptyset$-conjugates of $\lambda(x, 1)$ is consistent and $\emptyset$-definable. But any conjugate of $\lambda(x, 1)$ under the action of $\mathrm{Aut}(\mathbb{M}_0)$ has the form $\lambda(x, g)$ for some $g \in G$, so using (II) we see that $\models S(x) \to \lambda(x, g_1) \vee \cdots \vee \lambda(x, g_m)$ for some $g_1, \ldots, g_m$ in G, and thus $\varphi(x)$ is generic in $\mathbb{M}$. Similarly, if $\neg\lambda(x, 1)$ does not fork over $\emptyset$, then $\neg\varphi(x)$ is generic in $\mathbb{M}$. This proves the lemma. ∎

LEMMA 5.16: *Let M be a model. Then*

(i) *The set X of generic $p(x) \in S_\delta(M)$ is finite and nonempty.*

(ii) *G^M acts transitively on X.*

(iii) *There is a G-invariant $E \in \mathrm{FE}_\delta(\emptyset)$ such that for $p_1, p_2 \in X$, $p_1 = p_2$ iff $p_1(x_1) \cup p_2(x_2) \models E(x_1, x_2)$.*

Proof: Essentially we pass to a suitable reduct of T^{eq}, and then directly apply Lemma 5.9. Let $E(y_1, y_2)$ be the formula $\forall x(\delta(x, y_1) \leftrightarrow \delta(x, y_2))$.

Let Δ denote the sort S_E in T^{eq} (see section 1.3). Let $\varepsilon(x, w)$ be the L^{eq}-formula $\exists y(\delta(x, y) \bigwedge w = y/E)$. (So essentially the interpretation of Δ is the set of (sets defined by) instances of δ, and ε is membership.)

Let $\mathbb{M}_1$ be the relativised reduct of $\mathbb{M}$, with predicates $S(x)$, $\Delta(w)$ and $\varepsilon(x, w)$. Let $T_1 = \mathrm{Th}(\mathbb{M}_1)$. Again clearly $\varepsilon(x, w)$ is stable for T_1, and

(I) for any $g \in G$, the permutation $b \to g.b$ of S extends to a (unique) automorphism of $\mathbb{M}_1$.

Thus again

(II) In T_1, the formula $S(x)$ determines a complete type over $\emptyset$.

Fix a model M of T, which we may assume to be reasonably homogeneous, and let M_1 be the corresponding reduct of M to a model of T_1.

We can clearly identify $S_\varepsilon(M_1)$ and $S_\delta(M)$ (although not $S_\varepsilon(A)$ and $S_\delta(A)$ for arbitrary sets A). By (II) there is a unique $p(x) \in S_\varepsilon(\emptyset)$ (in T_1). We apply 5.9 (in T_1) to obtain the finite nonempty set $X_1 = \{q \in S_\varepsilon(M_1)$: q does not fork over $\emptyset\}$, and $E_1 \in \mathrm{FE}_\varepsilon(\emptyset)$ such that the types in X_1 are distinguished by the E_1-classes they contain. Also $\mathrm{Aut}(M_1)$ acts transitively on X_1. As E_1 is $\emptyset$-definable, by (I) E_1 is G-invariant. In particular (by transitivity of the action of G),

(III) G^M acts transitively on the E_1-classes, and thus on X_1.

All that remains to be seen is that X_1 is precisely the set of generic complete δ-types over M. This is given by

CLAIM: Let $\varphi(x)$ be a δ-formula over M (and thus equivalent to a ε-formula over M_1). Then $\varphi(x)$ is generic iff $\varphi(x) \in q$ for some $q \in X$.

Proof of Claim: If $\varphi(x)$ is generic, clearly any $q \in S_\varepsilon(M)$ contains some G^M-translate $g.\varphi(x)$ of $\varphi(x)$. Taking $q \in X_1$, then $g^{-1}.\varphi(x) \in g^{-1}.q \in X_1$. Conversely, suppose $\varphi(x) \in q$, with $q \in X_1$. By (III), some finite union of G-translates of $\varphi(x)$, say $\psi(x)$, is contained in every type in X_1. Thus $\neg\psi(x)$ is contained in

no type in X_1. By the first part of the proof of the claim, $\neg\psi(x)$ is not generic. By 5.15, $\psi(x)$ is generic. So clearly $\varphi(x)$ is also generic. The claim is proved, and so also the lemma. ∎

Remark 5.17:

(i) Let $\varphi(x)$ be a δ-formula. Then φ is generic iff for all $g \in G$, $\varphi(g.x)$ does not fork over $\emptyset$.

(ii) Let $p(x) \in S_\delta(M)$, where M is sufficiently saturated. Then p is generic iff for all $g \in G^M$, $g.p$ does not fork over $\emptyset$.

Proof: (i) We make use of the proofs of 5.16 and 5.15. Suppose $\varphi(x)$ is generic. Then for each $g \in G$, $\varphi(g \cdot x)$ is generic, so by the proof of 5.16, is contained in some $q \in S_\delta(M)$ which does not fork over $\emptyset$ in the sense of the theory T_1. This means that the δ-definition of q is over $\mathrm{acl}^{\mathrm{eq}}(\emptyset)$ in the sense of T_1, so also in the sense of T. Thus q does not fork over $\emptyset$ in T, so $\varphi(g \cdot x)$ does not fork over $\emptyset$.

Conversely, suppose $\varphi(x)$ is not generic. Let $\mathbb{M}_0$, $T_0 = \mathrm{Th}(\mathbb{M}_0)$ and $\lambda(x, z)$ be as in the proof of 5.15. ($\lambda(z, x)$ is equivalent to $\varphi(z^{-1} \cdot x)$.) Then $\lambda(x, 1)$ forks over $\emptyset$ in T_0. By 5.11 (II) (for T_0) there is an indiscernible sequence $(g_i\colon i < \omega)$ such that $\{\lambda(x, g_i)\colon i < \omega\}$ is inconsistent. We may extend this sequence to an indiscernible sequence $(g_i\colon i < \kappa)$ where $\kappa > 2^{|T|}$. Let M be a model of T containing all the g_i. Note $\lambda(x, g_i)$ is precisely $\varphi(g_i^{-1} \cdot x)$. If by way of contradiction all the $\varphi(g_i^{-1} \cdot x)$ did not fork over $\emptyset$, then we could choose, for each $i < \kappa$, some $p_i \in S_\delta(M)$ containing $\varphi(g_i^{-1} \cdot x)$ such that p_i does not fork over $\emptyset$. But by Lemma 5.8, each p_i is determined by $p_i|\mathrm{acl}^{\mathrm{eq}}(\emptyset)$, so among the p_i there are at most $2^{|T|}$ different types. But indiscernibility of the g_i (in T_0) implies that every k-subset of $\{\varphi(g_i^{-1} \cdot x)\colon i < \kappa\}$ is inconsistent, giving κ different types among the p_i. This contradiction shows that some $\varphi(g_i^{-1} \cdot x)$ forks over $\emptyset$ in T, completing the proof. (ii) follows from (i). ∎

Remark 5.18: Again the homogeneous space theory works in the more general context where $G(z)$ and $S(x)$ are partial types over $\emptyset$ instead of formulas. We still assume that the group operation on G and the transitive action of G on S are given by formulas over $\emptyset$ (restricted to $G \times G \times G$ and $G \times S \times S$). This set-up is called an **∞-definable homogeneous space** (over $\emptyset$). Then $\delta(x, y)$ is called **equivariant**, if for any a, and $g \in G$, there is b such that the partial type $\delta(g \cdot x, a) \bigwedge S(x)$ is equivalent to $\delta(x, b) \bigwedge S(x)$ (or in terms of solution sets $\delta(g \cdot x, a)^{\mathbb{M}} \cap S^{\mathbb{M}} = \delta(x, b)^{\mathbb{M}} \cap S^{\mathbb{M}}$). (We could also restrict the variable y to some

partial type Ψ as in 5.12, but in the applications this is not needed). A complete δ, S-type over A is a type of the form $p(x) \bigwedge S(x)$ where $p(x) \in S_\delta(A)$, and the set of such types is denoted $S_{\delta,S}(A)$. If $\varphi(x)$ is a δ-formula then φ is said to be **generic** if finitely many G-translates of $\varphi(x)^{\mathbb{M}} \cap S^{\mathbb{M}}$ cover $S^{\mathbb{M}}$, and $q(x) \in S_{\delta,S}(A)$ is **generic** if every δ-formula in q is generic. Lemma 5.16 is then valid in this context: If M is reasonably saturated then the set X of generic $q \in S_{\delta,S}(M)$ is finite and nonempty, and G^M acts transitively on X. The analogue of 5.17 (ii) is also true: if M is sufficiently saturated and $q(x) \in S_{\delta,S}(M)$ then q is generic iff for all $g \in G^M$, $g \cdot q$ does not fork over $\emptyset$. This observation will be used below. ∎

The reader should note that in this paper the word generic has been used in two different contexts: geometric structures, and stability theory for homogeneous spaces. We shall see below that in geometric structures satisfying (E) the notions essentially coincide.

5G. GEOMETRIC STRUCTURES AND STABILITY Our aim now is to study the interaction of the local stability theory developed above with geometric structures.

LEMMA 5.19: *Let M be a (sufficiently saturated) geometric structure. Let $p \in S_n(A)$, with $\dim(p) = m$. Let $\delta(x, y)$ be stable. Let $B \supset A$.*

(i) *There is an extension $q \in S_n(B)$ of p with $\dim(q) = m$, and such that $q|\delta$ does not fork over A.*

(ii) *If moreover F has property (E), then for every extension $q \in S_n(B)$ of p with $\dim(q) = m$, $q|\delta$ does not fork over A.*

Proof: If (i) fails then by compactness there are formulas $\theta(\boldsymbol{x}) \in p$, $\psi(\boldsymbol{x}, \boldsymbol{b})$ over B and $\chi(\boldsymbol{x}, \boldsymbol{b})$ a δ-B-formula, such that $\dim(q) = m$, $\psi(\boldsymbol{x}, \boldsymbol{b}) \to \theta(\boldsymbol{x}) \,\&\, \chi(\boldsymbol{x}, \boldsymbol{b})$, $\dim(q(\boldsymbol{x}) \,\&\, \neg\psi(\boldsymbol{x}, \boldsymbol{b})) < m$, and $\chi(\boldsymbol{x}, \boldsymbol{b})$ forks over A. But then, by 5.11, some finite set of A-conjugates of $\chi(\boldsymbol{x}, \boldsymbol{b})$ is inconsistent, whereby clearly $\theta(\boldsymbol{x})$ is the union of finitely many conjugates of $\theta(\boldsymbol{x}) \,\&\, \neg\psi(\boldsymbol{x}, \boldsymbol{b})$, contradicting Lemma 2.3 (iii).

(ii) Let $q \in S_n(B)$ be an extension of p with $\dim(q) = m$. Suppose by way of contradiction that $q|d$ forks over A. Without loss of generality B is a model M_0. Let M_1 be an $|M_0|^+$-saturated elementary extension of M_0. By part (i), let $r(\boldsymbol{x}) \in S_n(M_1)$ be an extension of $q(\boldsymbol{x})$ such that $\dim(r) = m$ and $r|\delta$ does not fork over M_0. So the δ-definition of r is over M_0, and is also the δ-definition of q.

Write this δ-definition as $\psi(\boldsymbol{y}, \boldsymbol{c})$ with $\boldsymbol{c}$ in M_0. As $q|\delta$ forks over A, $\psi(\boldsymbol{y}, \boldsymbol{c})$ is not over $\mathrm{acl}^{\mathrm{eq}}(A)$. By Lemma 5.4 (iii) there are $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ in M_1 such that $\boldsymbol{a}_i$ realises $r|(M_0 \cup \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{i-1}\})$ and $\psi(\boldsymbol{y}, \boldsymbol{c})$ is over $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k\}$. Then (as $\dim(p) = m$, and $\mathrm{tp}(\boldsymbol{a}_i/A) = p$)

(a) $\dim(\boldsymbol{a}_i/M_0\boldsymbol{a}_1 \cdots \boldsymbol{a}_{i-1}) = \dim(\boldsymbol{a}_i/A\boldsymbol{a}_1 \cdots \boldsymbol{a}_{i-1}) = \dim(\boldsymbol{a}_i/A) = m$ for all $i \leq k$, whereby, by Remarks 2.2,

(b) $\dim(\boldsymbol{a}_1 \cdots \boldsymbol{a}_k/M_0) = \dim(\boldsymbol{a}_1 \cdots \boldsymbol{a}_k/A)$.

Let E be the definable equivalence relation:

$$\boldsymbol{c}_1 \, \mathrm{E} \, \boldsymbol{c}_2 \quad \text{iff } \psi(\boldsymbol{y}, \boldsymbol{c}_1) \leftrightarrow \psi(\boldsymbol{y}, \boldsymbol{c}_2).$$

Let C be the E-class of $\boldsymbol{c}$, and let $\boldsymbol{c}'$ be in $C \cap M_0$ with $\dim(\boldsymbol{c}'/A, \boldsymbol{c}) = \dim(C) = t$ say. As $\psi(\boldsymbol{y}, \boldsymbol{c})$ is over $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k\}$, C is $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k\}$-definable and thus $\dim(\boldsymbol{c}'/A \cup \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k\}) \leq t$. On the other hand, by (b) and symmetry (2.2 i) $\dim(\boldsymbol{c}'/A \cup \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k\}) = \dim(\boldsymbol{c}'/A) \geq t$. Thus $\dim(\boldsymbol{c}'/A) = t$. Let X be a A-definable set of dimension t containing $\boldsymbol{c}'$. Then as C is $\boldsymbol{c}$-definable and $\dim(\boldsymbol{c}'/A, \boldsymbol{c}) = t$, also $\dim(X \cap C) = t$. On the other hand, as $\psi(\boldsymbol{y}, \boldsymbol{c})$ is not defined almost over A, C has infinitely many A-conjugates. Thus infinitely many distinct E-classes of X have dimension t, contradicting property (E). This contradiction proves (ii). ∎

COROLLARY 5.20: *Let M be a saturated geometric structure satisfying property (E). Let $G \subset M^k$ be a group which is ∞-definable over $\emptyset$, with $\dim(G) = n$. Identify G with the partial type $G(\boldsymbol{x})$ defining it. Let $\delta(\boldsymbol{x}, \boldsymbol{y})$ be a L-formula which is stable and equivariant for the action of G on itself by left multiplication. Then $p(\boldsymbol{x}) \in S_{\delta,G}(M)$ is generic (in the stability-theoretic sense) iff $p(\boldsymbol{x})$ extends to a complete $q(\boldsymbol{x}) \in S(M)$ with $\dim(q) = n$ (iff $\dim(p) = n$).*

Proof: Suppose $p(\boldsymbol{x}) \in S_{\delta,G}(M)$ is generic. Let $\varphi(\boldsymbol{x})$ be a δ-formula in p. Then finitely many G-translates of $\varphi(\boldsymbol{x}) \bigwedge G(\boldsymbol{x})$ cover G. But clearly $\dim(\varphi(\boldsymbol{x}) \bigwedge G(\boldsymbol{x})) = \dim(\varphi(\boldsymbol{g} \cdot \boldsymbol{x}) \bigwedge G(\boldsymbol{x}))$ for any $\boldsymbol{g} \in G$. By Lemma 2.3 (iii) (for partial types) and the fact that $\dim(G) = n$, we conclude that $\dim(\varphi(\boldsymbol{x}) \bigwedge G(\boldsymbol{x})) = n$. Thus $\dim(p) = n$, so $p(\boldsymbol{x})$ extends to some complete $q(\boldsymbol{x}) \in S(M)$ with $\dim(q) = n$.

Conversely, suppose $p(\boldsymbol{x}) \in S_{\delta,G}(M)$ extends to some $q(\boldsymbol{x}) \in S(M)$ with $\dim(q) = n$. Then $\dim(q) = \dim(q|\emptyset)$ (as $G(\boldsymbol{x}) \in q(\boldsymbol{x})$, G is a partial type over $\emptyset$ and $\dim(G(\boldsymbol{x})) = n$). By 5.19 (ii), $q|\delta$ does not fork over $\emptyset$, and thus clearly $p(\boldsymbol{x})$ does not fork over $\emptyset$. But clearly for any $\boldsymbol{g} \in G^M$, $\dim(\boldsymbol{g} \cdot q) = n$ too, and

$g.p \in S_{\delta,G}(M)$. Thus for all $g \in G^M$, $g \cdot p$ does not fork over $\emptyset$. By Lemma 5.17 (see also Remark 5.18), $p(x)$ is generic in the stability sense. ∎

We now point out how stable formulas arise naturally in geometric structures satisfying (S_1).

LEMMA 5.21: *Let M be a geometric structure satisfying (S_1). Let $\varphi(x,y)$, $\psi(x,z)$ be formulas such that for all a, b in M, we have:* $\dim(\varphi(x,a)) \leq n$ *and* $\dim(\psi(x,b)) \leq n$. *Let $\delta(y,z)$ be the formula such that for all a', b', $\delta(a',b')$ iff* $\dim(\varphi(x,a') \,\&\, \psi(x,b')) = n$. *Then δ is stable.*

Proof: We assume M to be saturated. Ramsey's theorem states that if X is an infinite set, and the collection of unordered k-element subsets of X is partitioned into 2 sets Y_1 and Y_2, then there is $i = 1$ or 2 and an infinite subset X_0 of X such that every k-element subset of X_0 is contained in Y_i. If by way of contradiction δ is not stable then a standard model-theoretic argument using Ramsey's theorem and compactness enables us to find an indiscernible sequence $\langle (a_i, b_i) \colon i \in \mathbb{Z} \rangle$ such that $\delta(a_i, b_j)$ iff $i \leq j$.

CASE (i): $\dim(\varphi(x,a_1) \,\&\, \varphi(x,a_2) \,\&\, \psi(x,b_3)) = n$. Then

$$\dim(\varphi(x,a_1) \,\&\, \varphi(x,a_i) \,\&\, \psi(x,b_{i+1})) = n \quad \text{for all } i > 1,$$

whereas

$$\dim(\varphi(x,a_i) \,\&\, \psi(x,b_{i+1}) \,\&\, \varphi(x,a_j) \,\&\, \psi(x,b_{j+1})) < n \quad \text{for all } 1 < i+1 < j.$$

This contradicts the fact that $\dim(\varphi(x,a_1)) = n$ and the property (S_1).

CASE (ii): *Otherwise.* Then $\dim(\varphi(x,a_i) \,\&\, \varphi(x,a_j) \,\&\, \psi(x,b_3)) < n$ for all $i < j < 3$. As $\dim(\psi(x,b_3)) = \dim(\varphi(x,a_i) \,\&\, \psi(x,b_3)) = n$ for all $i < 3$ we again contradict (S_1). ∎

LEMMA 5.22: *Let M be a saturated geometric structure. The following are equivalent:*

(i) *M has property (S_1),*

(ii) *(The Independence Theorem over a model.) Let M_0 be a small elementary submodel of M. Let a, b be tuples from M such that a is independent from b over M_0 (in the dimension-theoretic sense). Let c_1, c_2 be tuples from M such that* $\mathrm{tp}(c_1/M_0) = \mathrm{tp}(c_2/M_0) = r$, *$c_1$ is independent from a*

over M_0, and $\boldsymbol{c}_2$ is independent from $\boldsymbol{b}$ over M_0. Then there is $\boldsymbol{c}$ in M such that $\mathrm{tp}(\boldsymbol{c}/M_0, \boldsymbol{a}) = \mathrm{tp}(\boldsymbol{c}_1/M_0, \boldsymbol{a})$, $\mathrm{tp}(\boldsymbol{c}/M_0, \boldsymbol{b}) = \mathrm{tp}(\boldsymbol{c}_2/M_0, \boldsymbol{b})$ *and* $\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$ *is M_0-independent.*

Proof: (ii)→(i). Assume M satisfies (ii). Suppose by way of contradiction that for some formulas $\theta(\boldsymbol{x})$ and $\varphi(\boldsymbol{x}, \boldsymbol{y})$ (maybe with parameters), there are $\boldsymbol{b}_i$ for $i < \omega$ such that

$$(*) \qquad \begin{aligned} &\dim(\theta(\boldsymbol{x})) = \dim(\theta(\boldsymbol{x}) \,\&\, \varphi(\boldsymbol{x}, \boldsymbol{b}_i)) = n \quad \text{for all } i, \\ &\text{but } \dim(\varphi(\boldsymbol{x}, \boldsymbol{b}_i) \,\&\, \varphi(\boldsymbol{x}, \boldsymbol{b}_j)) < n \quad \text{for } i \neq j. \end{aligned}$$

It is then easy to obtain some model M_0 containing the parameters from θ and φ, and $\boldsymbol{b}^1$, $\boldsymbol{b}^2$ such that $\mathrm{tp}(\boldsymbol{b}^1/M_0) = \mathrm{tp}(\boldsymbol{b}^2/M_0)$, $\boldsymbol{b}^1$ is independent from $\boldsymbol{b}^2$ over M_0, $\dim(\theta(\boldsymbol{x}) \,\&\, \varphi(\boldsymbol{x}, \boldsymbol{b}^i)) = n$ for $i = 1, 2$, and $\dim(\varphi(\boldsymbol{x}, \boldsymbol{b}^1) \,\&\, \varphi(\boldsymbol{x}, \boldsymbol{b}^2)) < n$.

Indeed, choose M_0 containing the parameters from θ and φ. By Ramsey's Theorem and definability of dimension, without loss of generality $\langle \boldsymbol{b}_i \colon i < \omega \rangle$ is an indiscernible sequence over M_0. If $\boldsymbol{b}_0$ is independent from $\boldsymbol{b}_1$ over M_0 we are finished. Otherwise, we can again by Ramsey, find a model M_1 containing $M_0 \cup \boldsymbol{b}_0$, and an indiscernible sequence $\langle \boldsymbol{b'}_1, \boldsymbol{b'}_2, \ldots \rangle$ over M_1 with $\mathrm{tp}(\boldsymbol{b'}_i/M_0 \cup \boldsymbol{b}_0) = \mathrm{tp}(\boldsymbol{b}_i/M_0 \cup \boldsymbol{b}_0) = p$ for all i, and with $(*)$ holding for the $\boldsymbol{b'}_i$ in place of the $\boldsymbol{b}_i$. If $\boldsymbol{b'}_1$ is independent from $\boldsymbol{b'}_2$ over M_1, we are again finished. Otherwise continue to find M_2 and $\langle \boldsymbol{b''}_2, \boldsymbol{b''}_3, \ldots \rangle$ as before. As dimension is finite, this process must eventually stop.

Now let $\boldsymbol{c}_1$ be a generic point of $\theta(\boldsymbol{x}) \& \varphi(\boldsymbol{x}, \boldsymbol{b}^1)$ over $M_0 \cup \boldsymbol{b}^1$. Thus $\boldsymbol{c}_1$ is independent from $\boldsymbol{b}^1$ over M_0. Let $\boldsymbol{c}_2$ be such that $\mathrm{tp}(\boldsymbol{c}_2, \boldsymbol{b}^2/M_0) = \mathrm{tp}(\boldsymbol{c}_1, \boldsymbol{b}^1/M_0)$. Let $\boldsymbol{c}$ be as given by the Independence Theorem, namely $\mathrm{tp}(\boldsymbol{c}/M_0 \cup \boldsymbol{b}^i) = \mathrm{tp}(\boldsymbol{c}_i/M_0 \cup \boldsymbol{b}^i)$ for $i = 1, 2$, and $\{\boldsymbol{b}^1, \boldsymbol{b}^2, \boldsymbol{c}\}$ is M_0-independent. The existence of the tuple $\boldsymbol{c}$ contradicts the fact that $\dim(\varphi(\boldsymbol{x}, \boldsymbol{b}^1) \,\&\, \varphi(\boldsymbol{x}, \boldsymbol{b}^2)) < n$.

(i)→(ii). Assume M satisfies (S_1). Let M_0, $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}_1$, $\boldsymbol{c}_2$ and r be as in the hypotheses of (ii). Let $\dim(r) = n$. It clearly suffices, by compactness, to show that for every $\varphi_1(\boldsymbol{x}, \boldsymbol{a}) \in \mathrm{tp}(\boldsymbol{c}_1/M_0, \boldsymbol{a})$ and $\varphi_2(\boldsymbol{x}, \boldsymbol{b}) \in \mathrm{tp}(\boldsymbol{c}_2/M_0, \boldsymbol{b})$ (where φ_1, φ_2 may have additional parameters from M_0)

$$(*) \qquad \dim(\varphi_1(\boldsymbol{x}, \boldsymbol{a}) \,\&\, \varphi_2(\boldsymbol{x}, \boldsymbol{b})) = n.$$

Let $\delta(\boldsymbol{y}, \boldsymbol{z})$ be a formula (over M_0) defining the set of $(\boldsymbol{a'}, \boldsymbol{b'})$ for which $(*)$ holds with $\boldsymbol{a'}$ replacing $\boldsymbol{a}$, and $\boldsymbol{b'}$ replacing $\boldsymbol{b}$. Let $\boldsymbol{a}_1$ be such that $\mathrm{tp}(\boldsymbol{a}_1, \boldsymbol{c}_2/M_0) =$

$\mathrm{tp}(\boldsymbol{a}, \boldsymbol{c}_1/M_0)$ and $\boldsymbol{a}_1$ is independent from $\{\boldsymbol{b}, \boldsymbol{c}_2\}$ over M_0. Then $\{\boldsymbol{a}_1, \boldsymbol{b}, \boldsymbol{c}_2\}$ is M_0-independent, whereby clearly

$(**)$ $\qquad \delta(\boldsymbol{a}_1, \boldsymbol{b})$ holds.

By Lemma 5.21, δ is stable. By Lemma 5.8 above there is a unique complete δ-type over $M_0 \cup \boldsymbol{b}$, say q, such that q does not fork over M_0 and $q|M_0 = \mathrm{tp}_\delta(\boldsymbol{a}/M_0)$. By Lemma 5.19 (ii), $\mathrm{tp}_\delta(\boldsymbol{a}/M_0 \cup \boldsymbol{b}) = \mathrm{tp}_\delta(\boldsymbol{a}_1/M_0 \cup b) = q$. By $(**)$, $\delta(\boldsymbol{a}, \boldsymbol{b})$. So $(*)$ holds, completing the proof. ∎

6. Groups in pseudo-finite fields

In this final section we prove Theorem C. We start with a lemma on ∞-definable subgroups of definable groups in geometric structures satisfying (S_1).

LEMMA 6.1: *Let M be a saturated geometric structure with property (S_1). Let G be a group definable in M, and let H be an ∞-definable subgroup of G (namely H is a subgroup of G which is the solution set of a partial type over a small set). Then H is an intersection of definable subgroups of G.*

Proof: Let M_0 be a small elementary submodel of M over which G and H are defined. Let $\dim(H) = n$. Let U_i for $i \in I$ be M_0-definable subsets of G such that $\dim(U_0) = n$, $U_i \subset U_0$ for all i, $\{U_i\colon i \in I\}$ is closed under finite intersections, and $H = \cap\{U_i\colon i \in I\}$. We work in G. For $i \in I$, let $\delta_i(x, y)$ be the formula (over M_0):

$$G(x) \wedge G(y) \wedge \dim(x \cdot U_i \cap y \cdot U_i) = n.$$

(We may at this point add names for the elements of M_0 to the language if we wish. In any case from now on all sets and models we consider will contain M_0.)

By Lemma 5.20, $\delta_i(x, y)$ is stable. Moreover $\delta_i(x, y)$ is also equivariant for the action of H on itself by left translation. For if $a \in G$ and $b \in H$ then $\delta_i(b.x, a) \wedge H(x)$ is equivalent to $\delta_i(x, b^{-1}.a) \wedge H(x)$.

As in Remark 5.18, $S_{\delta_i, H}(M)$ denotes the set of types of the form $p(x) \wedge H(x)$, where $p(x) \in S_{\delta_i}(M)$.

For $i \in I$, let $Q_i = \{b \in U_0\colon$ for every generic (in the stability-theoretic sense) $p(x) \in S_{\delta_i, H}(M)$, $\delta_i(x, b) \in p(x)\}$. By Lemma 5.16, or more precisely Remark 5.18, for each $i \in I$ there are only finitely many generic $p(x) \in S_{\delta_i, H}(M)$. Each of these does not fork over M_0 (by 5.17 (ii)) and thus the δ_i-definition of each is a formula over M_0. This shows that Q_i is an M_0-definable set.

CLAIM 1:

(i) For each $i \in I$, $Q_i = \{b \in U_0$: for any $a \in H$ such that $\dim(a/b, M_0) = n$, $\delta_i(a, b)$ holds$\}$.

(ii) $H = \cap\{Q_i : i \in I\}$.

Proof of Claim 1: (i) Now whenever $\dim(a/b, M_0) = n$, then $\mathrm{tp}(a/b, M_0)$ has an extension to some complete $q(x) \in S(M)$ with $\dim(q) = n$. Thus the right hand side in (i) is precisely $\{b \in U_0 : \delta_i(x, b) \in q(x)$ for all $q(x) \in S(M)$ with $\dim(q) = n\}$. By Corollary 5.20 this set equals Q_i.

(ii) If $b \in H$ and $a \in H$ then $a \cdot U_i \cap b \cdot U_i$ contains H, thus has dimension n, so $\delta_i(a, b)$, thus $b \in Q_i$. Conversely, let $b \in Q_i$ for all i. Let $a \in H$ be such that $\dim(a/M_0, b) = n$. By (i) $\dim(a \cdot U_i \cap b \cdot U_i) = n$ for all i, thus $\dim(b^{-1} \cdot a \cdot U_i \cap U_i) = n$ for all i. As $H = \cap U_i$, by compactness $b^{-1} \cdot a \cdot H \cap H$ is nonempty, which clearly implies $b \in H$.

As H is a group, and $\{U_i : i \in I\}$ is closed under finite intersections, it is clear from Claim 1 (ii) that for any $i \in I$ there is $i(0) \in I$ such that $Q_{i(0)} \subset Q_i$ and $Q_{i(0)} \cdot Q_{i(0)} \subset U_0$. Thus we may assume that for every $i \in I$, $Q_i \cdot Q_i \subset U_0$.

CLAIM 2: For any $i \in I$, $H \cdot Q_i \subset Q_i$.

Proof of Claim 2: First note that $H \cdot Q_i \subseteq Q_i \cdot Q_i \subseteq U_0$ (as by Claim 1, $H \subset Q_i$). Now let $a \in H$, $b \in Q_i$, and let c be a (dimension-theoretic) generic point of H over $M_0 \cup \{a, b\}$. We have to show (by Claim 1 (i)) that $\delta_i(c, a \cdot b)$, namely $\dim(c \cdot U_i \cap a \cdot b \cdot U_i) = n$, or equivalently $\dim(a^{-1} \cdot c \cdot U_i \cap b \cdot U_i) = n$. But, by dimension considerations $a^{-1} \cdot c$ is a generic point of H over $M_0 \cup b$, so as $b \in Q_i$, this follows by Claim 1 (i) again.

Now for $i \in I$, let $Q'_i = \{x \in Q_i : x \cdot Q_i, x^{-1} \cdot Q_i \subseteq Q_i\}$. By Claim 3 and the fact that $H \subset Q_i$, Q'_i contains H and is a subgroup of G. Thus $H = \cap\{Q'_i : i \in I\}$. This completes the proof of Lemma 6.1. ∎

Note that if R is a saturated (so non Archimedean) real closed field, then Lemma 6.1 fails in R. Take $H(x)$ to be $\{-a < x < a : a \in Q\}$ for example.

A slight extension of the proof of 6.1 yields: if M is a (saturated) geometric structure with property (S_1) and H is an ∞-definable group in M then H is the intersection of definable groups. This will not be needed here.

The next proposition is fundamental, and will yield Theorem C. We work in a geometric substructure F of D where F has the property (S_1). The problem is to pass from the algebraic relation between generics of G and $H(F)$ given in

2.1 to a virtual isogeny between G and $H(F)$. We now give a rough description of what goes on. Let $a \in G$, $a' \in H(F)$ be as given by 2.1, and let K be the group $G \times H(F)$. Suppose the base set of parameters is $\emptyset$. We will consider the set S of pairs (c, c') in K such that for some (a_1, a'_1) realising $\mathrm{tp}(a, a')$ and independent with (c, c'), $(c, c') \cdot (a_1, a'_1)$ also realises $\mathrm{tp}(a, a')$. If F happened to be a strongly minimal set say then (by uniqueness of generic types) S would be definable and would basically be the graph of the required isogeny. However in the situation here, S is only ∞-definable (rather than definable), and is not necessarily a group. However the Independence Theorem will allow us to show that $S.S$ is an ∞-definable subgroup of K. An application of 6.1 then yields the desired definable virtual isogeny.

PROPOSITION 6.2: *Let F be a geometric substructure of D, where D has elimination of imaginaries. Assume that F is sufficiently saturated and has property (S_1) (so by Lemma 5.22 satisfies the Independence Theorem). Let G be a group definable in F. Then there are: a group H definable in D with parameters in F, a definable (in F) subgroup G_0 of finite index in G; a definable (in F) subgroup H_0 of finite index in $H(F)$; and a definable (in F) homomorphism from G_0 onto H_0 with finite central kernel.*

Proof: Suppose $\dim(G) = n$. Let A, H, and a,a',b,b',c,c' be as given by Proposition 2.1. We may easily replace A by a small elementary submodel of F such that 2.1 still holds. We still call this submodel A. Note that $\dim(H(F)) = n$.

We will be working in the definable group $K = G \times H(F)$ (in particular inside F). We make no more use of stability-theoretic notation, so the word generic is always used in the dimension- theoretic sense.

Let $q = \mathrm{tp}(b, b'/A)$. So $\dim(q) = n$. Let (a_1, a'_1) realise $\mathrm{tp}(a, a'/c, c', A)$ with (a_1, a'_1) is independent with $\{a, a', b, b', c, c', A\}$ over A, c, c' (and so also over A, as (a, a') and (c, c') are independent over A). Let (b_1, b'_1) be such that $\mathrm{tp}(a_1, a'_1, b_1, b'_1, c, c'/A) = \mathrm{tp}(a, a', b, b', c, c'/A)$. In particular $\mathrm{tp}(b_1, b'_1/A) = q$, and $(a_1, a'_1) \cdot (b_1, b'_1) = (c, c')$. Let $a_2 = a_1^{-1} \cdot a$, and $a'_2 = (a'_1)^{-1} \cdot a'$.

CLAIM 1: $(a_2, a'_2) \cdot (b, b') = (b_1, b'_1)$, $\dim(a_2/A) = \dim(a_2, a'_2/A) = n$, and (a_2, a'_2) is independent with (b, b') over A.

Proof of Claim 1: The first statement is immediate. $\dim(a_2/A) = n$, because $a_2 = a_1^{-1}.a$ and a_1 and a are independent generic points of G over A. Now $\dim(a_2, a'_2, a_1, a'_1, a, a', b_1, b'_1, b, b'/A) = 3n$, $\dim(a_2, a'_2, a_1, a'_1, a, a'/A) = 2n$ and

$\dim(a_2, a_2', b_1, b_1', b, b'/A) = 2n$. By subadditivity of dimension it follows that $\dim(a_2, a_2'/A) = n$, and that (a_2, a_2') is independent with (b, b') over A.

Let us define

$$\mathrm{St}(q) = \{x \in K: \quad \text{for some } y \text{ realising } q, \text{ with } x \text{ independent from } y \text{ over } A, \\ x.y \text{ realises } q\}.$$

CLAIM 2: $\mathrm{St}(q)$ is ∞-definable over A, namely defined by a partial type over A. Moreover $\mathrm{St}(q) = \mathrm{St}(q)^{-1}$ and $\dim(\mathrm{St}(q)) = n$.

Proof of Claim 2: For U a definable set in q, with $\dim(U) = n$, let

$$\mathrm{St}(U) = \{x \in K: \dim(x \cdot U \cap U) = n\}(= \{x \in K: \dim(x^{-1} \cdot U \cap U) = n\}).$$

By 2.3 (ii) $\mathrm{St}(U)$ is A-definable. Then $\mathrm{St}(q) = \cap\{\mathrm{St}(U): U \text{ in } q\}$. For example, if x is in the right hand side, then by compactness $\dim(q \cap x^{-1} \cdot q) = n$, so choose y satisfying $q \,\&\, x^{-1} \cdot q$, with y independent from x. Then $x \cdot y$ satisfies q.

Clearly, if x is independent with y over A, y realises q and $x \cdot y$ realises q, then also x is independent with $x \cdot y$ over A, whereby $x^{-1} \in \mathrm{St}(q)$.

By Claim 1, $(a_2, a_2') \in \mathrm{St}(q)$. As $\dim(a_2, a_2'/A) = n$, $\dim(\mathrm{St}(q)) \geq n$. On the other hand if $x \in \mathrm{St}(q)$ and y is independent from x, and both y and $x \cdot y$ realise q, then $\dim(x/A) = \dim(x/y, A) \leq \dim(x \cdot y/y, A) \leq \dim(x.y/A) = n$. Thus $\dim(\mathrm{St}(q)) = n$.

CLAIM 3:

(i) For any $x_1, x_2 \in \mathrm{St}(q)$ with x_1 independent from x_2 over A, $x_1 \cdot x_2 \in \mathrm{St}(q)$.

(ii) $\mathrm{Stab}(q) =_{\mathrm{def}} \mathrm{St}(q) \cdot \mathrm{St}(q) (= \{x \cdot y, x, y \in \mathrm{St}(q)\})$ is an ∞-definable (over A) subgroup of K, of dimension n. If $x \in \mathrm{Stab}(q)$ is generic ($\dim(x/A) = n$) then $x \in \mathrm{St}(q)$.

(iii) $\mathrm{Stab}(q)$ is "connected", namely contains no ∞-definable subgroup of finite index.

Proof of Claim 3: (i). Let x_1, x_2 be A-independent realisations of $\mathrm{St}(q)$. Then $x_2^{-1} \in \mathrm{St}(q)$. Let y_2 realise q independently with x_2 over A such that $x_2^{-1} \cdot y$ realises q and let $r_2 = \mathrm{tp}(y_2/A, x_2)$. Let y_1 realise q independently with x_1 over A such that $x_1 \cdot y_1$ realises q. Let $r_1 = \mathrm{tp}(y_1/A, x_1)$. By the Independence Theorem 5.22 there is y realising $r_1 \cup r_2$ such that $\{x_1, x_2, y\}$ is A-independent. Then it is clear that $x_2^{-1} \cdot y$ is independent with $\{x_1, x_2\}$ over A (as it realises q) and thus, as $(x_1 \cdot x_2) \cdot (x_2^{-1} \cdot y) = x_1 \cdot y$ realises q, $x_1 \cdot x_2 \in \mathrm{St}(q)$.

(ii) As $\mathrm{St}(q)$ is closed under inverses, so is $\mathrm{Stab}(q)$. Clearly $\mathrm{Stab}(q)$ is ∞-definable over A, since $\mathrm{Stab}(q) = \cap\{\mathrm{St}(U) \cdot \mathrm{St}(U)\colon U \text{ in } q\}$. To show $\mathrm{Stab}(q)$ is a subgroup it is sufficient to show that if

$$a, b, c \in \mathrm{St}(q) \quad \text{then } a \cdot b \cdot c \in \mathrm{Stab}(q).$$

So let $a, b, c \in \mathrm{St}(q)$. Let b_1 be generic in $\mathrm{St}(q)$ over $\{a, b, c, A)$, namely $b_1 \in \mathrm{St}(q)$ and $\dim(b_1/A, a, b, c) = n$. By (i)

$$a \cdot b_1 \in \mathrm{St}(q) \quad \text{and} \quad b_1^{-1} \cdot b \in \mathrm{St}(q).$$

Moreover

$$\dim(b_1^{-1} \cdot b/A, a, b, c) = \dim(b_1/A, a, b, c) = n \geq \dim(b_1^{-1} \cdot b/A).$$

Thus $b_1^{-1} \cdot b$ is independent with c over A, so by (i) again $(b_1^{-1} \cdot b) \cdot c \in \mathrm{St}(q)$. Thus $a \cdot b \cdot c = (a \cdot b_1) \cdot (b_1^{-1} \cdot b \cdot c) \in \mathrm{Stab}(q)$.

Finally we show $\dim(\mathrm{Stab}(q)) = n$. Clearly $\dim(\mathrm{Stab}(q)) \geq n$. Let $e = a \cdot b \in \mathrm{Stab}(q)$ with $a, b \in \mathrm{St}(q)$. Let $c \in \mathrm{St}(q)$ with $\dim(c/A, a, b) = n$. Then again $b \cdot c \in \mathrm{St}(q)$ and is independent with a over A. Thus $a \cdot b \cdot c \in \mathrm{St}(q)$, and hence $\dim(a \cdot b \cdot c/A, c) \leq n$. But $\dim(e/A) = \dim(e/A, c) = \dim(a \cdot b/A, c) = \dim(a \cdot b \cdot c/A, c)$. Thus $\dim(e/A) \leq n$. Thus $\dim(\mathrm{Stab}(q)) = n$.

The last part of (ii) is proved in a similar way: if $a, b \in \mathrm{St}(q)$ and $\dim(a \cdot b/A) = n$, choose c generic in $\mathrm{St}(q)$ over A, a, b. Then $a \cdot b = (a \cdot c) \cdot (c^{-1} \cdot b)$, $\dim(a \cdot c/A) = \dim(c^{-1} \cdot b/A) = n$, and as $\dim(a \cdot b/A) = n$, this forces $a \cdot c$ to be independent with $c^{-1} \cdot b$ over A. As both are in $\mathrm{St}(q)$, so is their product, by (i) again.

(iii) Suppose by way of contradiction that C is an ∞-definable subgroup of $\mathrm{Stab}(q)$ of finite index in $\mathrm{Stab}(q)$. Clearly (as A is a model) C is A-definable, and $\dim(C) = n$. Let $c \in C$ be generic over A. By (ii) $c \in \mathrm{St}(q)$. So let a realise q independently with c over A such that $c \cdot a$ realises q. Clearly a is independent with $c \cdot a$ over A. Let $d \in \mathrm{Stab}(q) \setminus C$ be generic in $\mathrm{Stab}(q)$ over A such that d is independent with a over A and $d \cdot a$ realises q. Again $d \cdot a$ and a are independent over A. By the Independence Theorem there is e such that $\mathrm{tp}(a, e/A) = \mathrm{tp}(a, d \cdot a/A)$ and $\mathrm{tp}(c \cdot a, e/A) = \mathrm{tp}(c \cdot a, a/A)$. So a and e are in different cosets modulo C, whereas $c \cdot a$ and e are in the same coset modulo C, contradicting the fact that a and $c \cdot a$ are in the same coset modulo C.

At this point it is clear that $\mathrm{Stab}(q)$ induces an "isogeny" between a "large" ∞-definable subgroup of G and a "large" ∞-definable subgroup of $H(F)$. To be

more precise: first the projection of $\mathrm{Stab}(q)$ on G, say G^0, is ∞-definable and of dimension n (as it contains a_2). Similarly the projection $H(F)^0$ of $\mathrm{Stab}(q)$ on $H(F)$ is ∞-definable of dimension n. Moreover $K_0 = \{x \in G^0 \colon (x,0) \in \mathrm{Stab}(q)\}$ is finite, as is $K_1 = \{x \in H(F)^0 \colon (0,x) \in \mathrm{Stab}(q)\}$ (as $\dim(\mathrm{Stab}(q)) = n$). As $\mathrm{Stab}(q)$ is connected, both $K_0 \times \{0\}$ and $\{0\} \times K_1$ are in the center of $\mathrm{Stab}(q)$, and thus K_0 is central in G^0 and K_1 is central in $H(F)^0$. So $\mathrm{Stab}(q)$ is the graph of an isomorphism between G^0/K_0 and $H(F)^0/K_1$. We want to replace G^0 and $H(F)^0$ by definable supergroups. This can be done using Lemma 6.1.

By 6.1 there is a definable subgroup Q of $G \times H(F)$, such that $\mathrm{Stab}(q) \subset Q$, $\dim(Q) = n$, $\{x \colon (x,0) \in Q\} = K_0$ and $\{x \colon (0,x) \in Q\} = K_1$. Let G_0 be the projection of Q on the first coordinate, and H_0 the projection of Q on the second coordinate. Clearly G_0 is definable with $\dim(G_0) = n$, whereby as (E) holds, G_0 has finite index in G. Similarly H_0 has finite index in $H(F)$. By choice of Q, K_0 is in the center of G_0, K_1 is in the center of H_0, and Q defines an isomorphism between G_0/K_0 and H_0/K_1. To complete the proof of Proposition 6.2 we need to replace H_0/K_1 by a definable group of finite index in the F-rational points of some group definable in D over F. First let H_1 be the centraliser of K_1 in H. So H_1 is a group living in D and definable (in D) over F. Moreover K_1 is in the centre of H_1 and $H_1(F) = H(F)$. By elimination of imaginaries in D, H_1/K_1 is (in D) F-definably isomorphic by some map f to some group H_2 in D. Clearly $\dim(H_2(F)) = n$. On the other hand f embeds H_0/K_1 in $H_2(F)$, and $\dim(f(H_0/K_1)) = n$. Thus by (S_1) $f(H_0/K_1)$ has finite index in $H_2(F)$. So altogether we now have in F a definable isomorphism of G_0/K_0 with a subgroup of finite index in $H_2(F)$, completing the proof of Proposition 6.2. ∎

Proof of Theorem C: Let F be a pseudo-finite field, which we may assume to be saturated. Let D be an algebraically closed field containing F with D the field-theoretic algebraic closure of F. By 2.11 and 2.18, F is a geometric substructure of D and F has property (S_1). Let G be a group definable in F. Let H be the (connected) group given by Proposition 6.2: namely H is definable in D with parameters in F, and there is a (definable in F) subgroup G_0 of finite index in G, and a subgroup H_0 of finite index in $H(F)$ and a definable (in F) homomorphism g from G_0 onto H_0 with finite central kernel. As in the proof of 3.1′ (using 1.8.2 and its proof in [B1] or [Po2]) there is an F-definable isomorphism f between H and an algebraic group H_1 defined over F. Composing g with f yields Theorem C. ∎

References

[A-M] M. Artin and B. Mazur, *On periodic points*, Ann. of Math. **81** (1965), 82–99.

[BaL] J. T. Baldwin and A. H. Lachlan, *On strongly minimal sets*, J. Symbolic Logic **36** (1971), 79–96.

[B1] E. Bouscaren, *Model theoretic versions of Weil's theorem on pregroups*, in *Model Theory of Groups* (A. Nesin and A. Pillay, eds.), Notre Dame Press, 1989, pp. 177–185.

[B2] E. Bouscaren, *The group configuration—after E. Hrushovski*, in*Model Theory of Groups* (A. Nesin and A. Pillay, eds.), Notre Dame Press, 1989, pp. 199–209.

[Bor] A. Borel, *Linear Algebraic Groups*, Springer-Verlag, Berlin, 1991.

[BCR] J. Bochnak, M. Coste and M-F. Roy, *Geometrie algebrique reelle*, Springer-Verlag, Berlin, 1987.

[Ch-v.d.D-Mac] Z. Chatzidakis, L. van den Dries and A. Macintyre, *Definable sets over finite fields*, J. Reine Angew **427** (1992), 107–135.

[v.d.D] L. van den Dries, *Algebraic theories with definable Skolem functions*, J. Symbolic Logic **49** (1984), 625–629.

[v.d.D-S] L. van den Dries and Ph. Scowcroft, *On the structure of semialgebraic sets over p-adic fields*, J. Symbolic Logic **53** (1988), 1138–1164.

[Fr-J] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Heidelberg, 1986.

[Hr1] E. Hrushovski, *Contributions to stable model theory*, Ph.D. thesis, Berkeley, 1986.

[Ja] M. Jarden, *Algebraic dimension over Frobenius fields*, preprint, 1992.

[Mac] A. Macintyre, *On definable sets of p-adic fields*, J. Symbolic Logic **41** (1976), 605–610.

[M-S] J. Madden and C. Stanton, *One dimensional Nash groups*, Pacific J. Math. **154** (1992), 331–344.

[No] M. V. Nori, *On subgroups of* $\mathrm{GL}_n(Fp)$, Inventiones Mathematicae **88** (1987), 257–275.

[Pe] Perrin, *Groupes henseliens*, Publications d'Orsay, Universite Paris-Sud, 1975.

[P1] A. Pillay, *Forking, normalisation and canonical bases*, Ann. Pure Appl. Logic **32** (1986), 61–81.

[P2] A. Pillay, *Groups and fields definable in O-minimal structures,* J. Pure Appl. Algebra **53** (1988), 239–255.

[P3] A. Pillay, *On fields definable in* $\mathbb{Q}_p$, Arch. Math. Logic **29** (1989), 1–7.

[P4] A. Pillay, *An application of model theory to real and p-adic algebraic groups,* J. Algebra **126** (1989), 139–146.

[P5] A. Pillay, *Model theory, stability theory and stable groups,* in *Model Theory of Groups* (A. Nesin and A. Pillay, eds.), Notre Dame Press, 1989, pp. 1–40.

[P6] A. Pillay, *Some remarks on definable equivalence relations in O-minimal structures,* J. Symbolic Logic **51** (1986), 709–714.

[P7] A. Pillay, *Some remarks on modular regular types,* J. Symbolic Logic **56** (1991), 1003–1011.

[Po1] B. Poizat, *Cours de Theorie des modeles,* Nur al-Mantiq Wal-Marifah, Paris, 1985.

[Po2] B. Poizat, *Groupes stables,* Nur al-Mantiq Wal-Marifah, Paris, 1987.

[Po3] B. Poizat, *An introduction to algebraically closed fields and varieties,* in *Model Theory of Groups* (A. Nesin and A. Pillay, eds.), Notre Dame Press, 1989, pp. 41–67.

[S-W] A. Sagle and R. Warner, *Introduction to Lie Groups,* Academic Press, New York, 1973.

[Sh] M. Shiota, *Nash manifolds,* Lecture Notes in Math. 1269, Springer-Verlag, Berlin, 1987.

[We] A. Weil, *On algebraic groups of transformations,* Am. J. Math. **77** (1955), 355–391.