MODEL THEORY AND GEOMETRY (TUTORIAL)

ELISABETH BOUSCAREN

This paper is based on a series of three lectures that I gave during the LC'2000, in the context of the "tutorials" which have now become a tradition at the European meetings of the ASL. I have kept fairly close to the actual format and style of the talks.

It is always difficult to identify precisely the audience such a tutorial should address. A fair number of broad and ambitious surveys have already been published on the subject of the applications of model theory to algebraic geometry (see section 4.4). I did not, during this tutorial, choose to address the specialists of the subject. The audience I had in mind consisted of both young "inexperienced" researchers in model theory and more "mature" logicians from other parts of logic. Rather than attempting one more broad survey, I tried to present some of the main concerns of "geometrical model theory" by looking at concrete examples and this is what I will try to do also in the present paper.

We will discuss three algebraic examples, algebraically closed fields, differentially closed fields and difference fields (fields with automorphisms). The geometric application we will take up as illustration is Hrushovski's approach to the Manin-Mumford conjecture. This is based on a fine study of the model theory of difference fields and is quite emblematic of the method. Perhaps the key technical notion is that of "local modularity" (or "one-basedness"), which arises in a purely model theoretic setting. We will see that the Diophantine conjectures of the Manin-Mumford type can be rephrased in terms of this notion. Furthermore, as one thinks through the rephrasing process, one realizes the need for the introduction of auxiliary algebraic theories such as the theory of difference fields.

I would like to thank the anonymous referee, despite my temporary shock at the initial suggestion that the paper be totally rewritten and turned into a survey of a completely different type. Fortunately, he/she also provided a long list of detailed comments and less draconian suggestions, in case I did not choose to follow this first drastic piece of advice. I have found these comments very helpful and have followed most of these suggestions.

§1. "Geometric" model theory. Until ten years ago, the most striking applications of model theory to algebra or number theory had typically been

Meeting

obtained using only the most basic tools of model theory, notably the compactness theorem and the technique of quantifier elimination, though the algebraic and analytic ingredients had been considerably deeper and more varied. This applies for example to the work of Ax-Kochen-Ershov on valued fields (1965), with later applications by Denef to the computation of p-adic integrals, to Ax's work on the elementary theory of finite fields (1968), to work of Denef, van den Dries and Macintyre on the p-adics (1970's and 1980's). It applies also to some of the more recent work on o-minimal structures, such as Wilkie's results on the theory of the reals with exponentiation and it's subsequent generalization to broad classes of analytic functions (see [10]).

In parallel pure model theory flourished at the same period, beginning with Morley's characterization of uncountably categorical theories (1965) and then with Shelah's monumental work on classification theory. Applications to algebra of these more sophisticated notions and results were at first rather few: let us mention the existence and uniqueness of the differential closure of a differential field of characteristic zero (Blum 1977), and the applications to the theory of modules (started by Garavaglia around 1978). It was soon apparent that the tools of the theory of stability were particularly well suited to the model theoretic analysis of groups and fields. Around 1980, Poizat introduced the notion of generic of a stable group which was directly inspired by the corresponding notion for algebraic groups and which became one of the main tools in the subject.

Then in the mid-eighties, under the influence of Zilber first and then of Hrushovski, stability theory started evolving and focusing on the study of the fine local behavior of structures of finite dimension. This was the beginning of what has been for some years known as "geometric stability" or more generally "geometric model theory".

Stability theory à la Shelah, developed a theory of abstract independence and dimension. Although this generalized the classical algebraic notions of independence (linear independence, algebraic independence), the methods used were often those of infinite combinatorics. One of the main aspects of the theory for example is the classification of structures according to which infinite combinatorial objects they interpret: orderings, trees...

Geometric stability, as its name indicates, took much of its inspiration from geometry, both in the sense of combinatorial geometries (or matroids) and of algebraic geometry. This relationship turned out to go both ways: the abstract notions developed in model theory were applied to the disciplines of their origins in order to give new proofs or new results there. We will not discuss here combinatorial geometries nor any of the results that were proved in this domain by applying model theoretic tools or ideas (results of Zilber on homogeneous finite geometries for example [46] or results of Evans and Hrushovski about "algebraic matroids"[7], [8]), but we will focus on the relationship with algebraic geometry.

Geometric stability investigates the geometric properties of the abstract independence relation introduced by Shelah. One of the main focus points is the study of the algebraic structures coded via this relation (groups, fields). These questions and the results obtained can be considered to be, at a higher level of generality, in the direct line of two "classical" and well-known theorems:

– the old theorem of geometry which says that a Desarguesian projective geometry of dimension at least 3 is the projective geometry over some division ring;

– the theorem of Weil which constructs an algebraic group from a generically rational associative operation on an algebraic variety.

One of the central notions in the subject is that of "one-basedness" or local modularity, which was introduced into the subject independently from several different points of view. For sets of "dimension one", local modularity corresponds exactly to the cases where the combinatorial geometry associated to the dependence relation is affine, projective or trivial. The *Zilber Trichotomy principle* states that if D is a set of dimension one, there are only three possibilities:

– either the geometry is trivial and there is no group definable in D (the geometry associated to D is then the infinite set with no structure, example (1) in section 3.3);

– or the geometry is affine or projective and every group definable in D is of linear type (see the precise definition in section 2.2). The structure D then behaves very similarly to a vector space (example (2) in section 3.3);

– or there is an algebraically closed field definable in D.

This principle was shown to be false in general by Hrushovski [12]. But it holds with extra assumptions, namely in the context of abstract *Zariski geometries*, defined by Hrushovski and Zilber [20, 21]. This trichotomy, or more precisely this dichotomy in the case of a group of dimension one plays an essential role in the applications to the Manin-Mumford type of conjectures.

The general "abstract" framework in which this material was originally developed, namely stability theory, was eventually seen as part of a broader one, "simplicity theory", which has now become a very active aera in model theory. This is the point of view we will adopt for the presentation of the abstract notions involved.

This ends our introductory sketch of geometric stability theory. In the next section (2) we will discuss the theory of algebraically closed fields, which is the model theoretic context for classical algebraic geometry, and explain how the Manin-Mumford type of conjectures fit within the model theoretic framework.

In the third section, we will give the abstract definition of independence and state the definition and main results about local modularity. These notions will be illustrated by four basic examples, presented at the end of the section (3.3). In the fourth and last section, we present two of the theories of fields which

are used in Hrushovski's proofs of the algebraic geometry results and finish in 4.3 with a brief sketch of the actual strategy for the proof of Manin-Mumford.

§2. Algebraically closed fields and the Mordell-Lang conjecture.

2.1. The theory of algebraically closed fields. We consider fields K as first-order structures in the usual language of rings: $L_R = \{0, 1, +, -, .\}$.

The theory of algebraically closed fields ACF is axiomatized by axioms which say:

(i) K is a field

(ii) K is algebraically closed, that is, every polynomial in one variable with coefficients in K has a solution in K. This can be axiomatized by the following scheme: for every $n > 1$

$$\forall y_1, \ldots \forall y_n \exists x \; x^n + y_1 x^{n-1} + \ldots + y_n = 0.$$

Every field L embeds into an algebraically closed field; there is a smallest such algebraically closed field containing L, the algebraic closure of L, which we denote by L^{alg} and which is unique up to isomorphism over L. The theory ACF is not complete but it suffices to specify the characteristic of the field to obtain a complete theory. For $p \geq 0$, we let ACF_p denote the (complete) theory of algebraically closed fields of characteristic p. In fact the theory ACF_p is categorical in every uncountable cardinality, that is, has a unique model up to isomorphism in every uncountable cardinality. Indeed if K, K' are two models of ACF_p, then K and K' are isomorphic if and only if they have the same transcendence degree over the prime field of characteristic p.

From now on, for the sake of simplification, we consider only the theory ACF_0 of algebraically closed fields of characteristic zero.

2.1.1. DEFINABLE SUBSETS. Let K be a model of ACF_0 of infinite transcendence degree over $\mathbb{Q}$.

In first-order logic, we study the subsets defined by first-order formulas. We start with the basic or atomic subsets, defined using the basic operations and relations in the language. In this particular context, our basic sets will be:

• THE ZARISKI CLOSED SETS: $E \subseteq K^n$ is Zariski closed if E is the zero-set of a finite number of polynomials over K, that is, if $E = \{(a_1, \ldots, a_n) \in K^n; f_1(a_1, \ldots, a_n) = \ldots = f_r(a_1, \ldots, a_n) = 0\}$, for $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$.

The Zariski closed sets define a Noetherian topology on $\bigcup_n K^n$, the classical ZARISKI TOPOLOGY.

• THE ZARISKI CONSTRUCTIBLE SETS: the finite boolean combinations (closure under finite intersection, finite union and complement) of the Zariski closed sets. They are exactly the sets definable by quantifier-free formulas in the language L_R.

• QUANTIFIER ELIMINATION: the theory ACF_0 has quantifier elimination, which means exactly that the projection of a constructible set is also constructible and hence that THE DEFINABLE SETS ARE EXACTLY THE CONSTRUCTIBLE SETS.

REMARK: The model theoretic notion of algebraic closure (see section 3.2) coincides with the usual field notion of algebraic closure.

The theory ACF_0 does not only eliminate quantifiers but it also ELIMINATES IMAGINARIES: for every definable equivalence relation E on $K^n \times K^n$, there is a definable map f_E from K^n to some K^m such that for all a, b in K^n $f_E(a) = f_E(b)$ if and only if a and b are E-equivalent.

2.1.2. VARIETIES AND ALGEBRAIC GROUPS ARE DEFINABLE. For those who already know their way around algebraic varieties and algebraic groups, the aim of this section is to explain how these objects can be considered as definable objects in the theory of algebraically closed fields. Those unfamiliar with the subject can consider them directly as definable subsets and definable groups with some specific properties and this should be sufficient for them to understand the statement of the Mordell-Lang conjecture in the next section.

For a more complete and elaborate introduction to the model theoretic approach to algebraic varieties see [35]. For basic definitions and results in algebraic geometry, see for example [25] and [26].

AN AFFINE VARIETY over K is a Zariski closed subset of K^n, for some $n \geq 1$, endowed with the induced Zariski topology from K^n. A QUASI-AFFINE VARIETY is a Zariski open subset of an affine variety, also endowed with the induced topology. Quasi-affine sets are special cases of Zariski constructible sets.

Let $V \subseteq K^n$ and $W \subseteq K^m$ be two quasi-affine varieties, a MORPHISM from V to W is a map f from V to W which is locally rational (or regular): for every $a \in V$, there is an open subset U of V containing a and polynomials $P_1, \ldots, P_m, Q_1, \ldots, Q_m$ in $K[X]$ such that on U, the Q_i's are non zero and

$$f(x) = (P_1/Q_1(x), \ldots, P_m/Q_m(x)).$$

By the compactness theorem, f is a definable map from V to W, i.e. the graph of f is definable: there are open subsets $U_1, \ldots, U_k$ of V such that on each U_i f is given by a fixed tuple of rational fractions.

An ISOMORPHISM is a bijective morphism whose inverse is also a morphism.

So far, we can see directly that we are dealing with definable sets and maps. It is a little more difficult in the case of an abstract variety which is obtained by gluing together a finite number of affine varieties.

A VARIETY V over K is a set V covered by a finite number of subsets $V_1, \ldots, V_k$ together with some maps $f_1, \ldots, f_k$, where each f_i is a bijection between V_i and some affine variety U_i, such that:

(i) for each i, j the set $U_{ij} := f_i(V_i \cap V_j)$ is open in U_i

(ii) the map $f_{ij} := f_i \circ f_j^{-1}$ is an isomorphism from U_{ji} into U_{ij}.

The U_i's are called the affine charts of V.

The Zariski topology on V is defined by declaring that $S \subseteq V$ is open if and only if for each i, $f_i(S \cap V_i)$ is open in U_i. A morphism from a variety $V = (V_i, f_i, U_i)$ to a variety $W = (W_j, g_j, Z_j)$ is a map h from V to W which is a morphism when read in the charts, i.e. h is continuous and for any i, j, the map $g_j \circ h \circ f_i^{-1}$ restricted to (the quasi-affine variety) $f_i(h^{-1}(W_j) \cap V_i))$ is a morphism.

There are different possible ways to identify a variety V, given by a fixed system of affine charts, (V_i, f_i, U_i), to a definable set. One way is to consider V to be the disjoint union of its affine charts $U_1, \ldots, U_k$, modded out by the definable equivalence relation which identifies U_{ij} and U_{ji} via the definable maps f_{ij}. By elimination of imaginaries this will indeed be (definably isomorphic to) a definable subset and the morphisms will be definable maps.
Notation: If V is a variety defined over K, we denote by $V(K)$ the set of K-rational points of V, or equivalently, if V is seen as a definable set in K^n, the subset of tuples in K^n which belong to the definable subset V.

We need two more definitions: An ALGEBRAIC GROUP G is a variety G equipped with a group multiplication $. : G \times G \mapsto G$ and an inverse $^{-1} : G \mapsto G$ which are morphisms for the variety structures on G and $G \times G$. So in particular, an algebraic group is a definable group, that is, a group which lives on a definable set and such that the group multiplication is a definable map.

The additive and multiplicative groups of the field K, $(K^n, +)$ and $((K^*)^n, .)$ are affine algebraic groups (algebraic groups which are isomorphic to affine varieties). So are all the linear groups, i.e. all the closed subgroups of $GL_n(K)$.

We will be interested in very different groups, the ones which have no affine subgroup at all. An ABELIAN VARIETY is an algebraic group G which is a complete irreducible variety, where complete means that, for any variety Y, the projection map $\pi : G \times Y \mapsto Y$ is closed (i.e. takes closed sets to closed sets).

The Abelian varieties of dimension one are exactly the elliptic curves, in fact the fundamental examples of Abelian varieties are the Jacobians of curves. Over $\mathbb{C}$ the Abelian varieties are complex tori, that is they are of the form $\mathbb{C}^n/\Lambda$ where Λ is a discrete subgroup of rank $2n$ (but not every complex torus is an Abelian variety).

Abelian varieties are commutative divisible groups. They have a certain number of other rather strong properties of which I will only mention one: in an Abelian variety G, for every $n > 0$, the number of torsion elements of order n is finite but the torsion subgroup of G, $Tor(G)$ is infinite and Zariski dense in G.

So we can consider Abelian varieties over K as a specific class of commutative divisible definable groups with a certain number of additional "nice" properties.

2.2. The Mordell-Lang conjecture. Recall that a commutative group Γ is said to be of *finite rank* if there is a finitely generated subgroup Γ_0 such that for every $\gamma \in \Gamma$, for some integer $n \geq 1$, $n\gamma \in \Gamma_0$. In any commutative group G, the group of torsion elements $Tor(G)$ is of course of finite rank.

We now have all the necessary elements in order to give the statement of the Mordell-Lang conjecture for Abelian varieties over a field of characteristic zero.

THE MORDELL-LANG CONJECTURE. *Let K be an algebraically closed field of characteristic zero, let A be an Abelian variety over K, X a closed irreducible subset of A and Γ a finite rank subgroup of $A(K)$. Then $X \cap \Gamma$ is a finite union of translates of subgroups of Γ, that is, there are $m \geq 1$, $H_1, \ldots, H_m$ subgroups of Γ and elements $b_1, \ldots, b_m$ in Γ, such that*

$$X \cap \Gamma = \bigcup_{i=1}^{m} b_i + H_i.$$

There are two different cases, "the number field case" when K is the algebraic closure of $\mathbb{Q}$, that is when A is in fact defined over a number field (a finite algebraic extension of $\mathbb{Q}$), and "the function field case" when A is not defined over $\mathbb{Q}^{alg}$.

The Mordell conjecture follows from the case when X is a curve defined over a number field k, A is the Jacobian of X and Γ is the (finitely generated) group of k-rational points of A.

The Manin-Mumford conjecture is the particular case when K is the algebraic closure of $\mathbb{Q}$ and the group Γ is the group $Tor(A)$. By taking Zariski closures, one can give the equivalent statement:

THE MANIN-MUMFORD CONJECTURE. *Let K be an algebraically closed field of characteristic zero, let A be an Abelian variety over $\mathbb{Q}^{alg}$ and X a closed irreducible subset of A. Then for some integer $m \geq 0$,*

$$X \cap Tor(A) = \bigcup_{i=1}^{m} b_i + Tor(B_i)$$

where for each i, B_i is an Abelian sub-variety of A (an irreducible closed subgroup of A) and $b_i + B_i$ is contained in X.

The Manin-Mumford conjecture was first proved by Raynaud in 1983, and the full Mordell-Lang conjecture was finally proved by Faltings in 1993. For more history and annotated bibliographies, one can look at [11] or [33].
Hrushovski gave a new proof of the function field case of the Mordell-Lang conjecture in 1994 [15], inspired by a previous proof of Buium's [3]. At the same time he also gave the first full proof of the characteristic $p > 0$ version of the Mordell-Lang conjecture. Then, in 1995, he gave a new proof of Manin-Mumford. One of the interesting aspects of these proofs is that they all fit in a common framework which was developed a priori in model theory, as I hope will become apparent very soon. Another interesting aspect of his Manin-Mumford proof is that it yields rather easily some effective bounds for the number m of translates involved. In fact I believe that at the time, in 1995, this was the first proof giving effective bounds which did not depend on the field of definition of the variety X.

Now let us consider again the statement of the Mordell-Lang conjecture and try to understand its meaning.

The first thing to remark is that it deals with two different kinds of objects: we have on one hand A and X, which are algebraic or from our point of view, definable objects, and the group Γ on the other hand, which is not definable. In algebraic geometry, one has tools to deal with algebraic or geometric objects, like varieties; similarly in model theory we have tools to deal with definable objects. So the first basic idea in the proof is going to be to replace the group Γ by a definable group.

The second remark is that the Mordell-Lang conjecture is usually considered as saying something about curves, or about closed subsets of A, but one can also consider that it is in fact a statement about the group Γ and the topology induced on it by the closed subsets of A. It says that this induced topology is determined by the subgroups and their translates. This is not the case for the topology on A itself: consider for example a curve X of genus strictly bigger than one, and A its Jacobian. It is classical that a curve of genus strictly bigger than one cannot be a group (or the coset of a group). In fact more generally, the topology on an algebraic group is never determined by its closed subgroups (see section 3.2)). In model theory we are familiar with this type of questions about the "induced structure" on a subset. If M is a first-order structure and if $E \subset M^n$ is a definable subset, the *induced structure* on E is the new first-order structure consisting of the set E, together with all relatively definable subsets of M: $(E, D \cap E^m; m \geq 1,\ D$ definable subset of $M^{nm})$.

In the case of definable groups the following notion is crucial. A definable group is of *linear type* if the induced structure on it is similar to a module, precisely:

DEFINITION. Let M be a first-order structure, and $G \subseteq M^n$ be a definable group. We say that G is of **linear type** if for every integer $m \geq 1$ and every definable $D \subseteq M^{nm}$, $D \cap G^m$ is equal to a finite boolean combination of cosets of definable subgroups of G^m.

The Mordell-Lang conjecture fits into this framework. There is a formal equivalence between the Mordell-Lang conjecture and the following statement:

THE MODEL THEORETIC VERSION OF MORDELL-LANG. *Let K be an algebraically closed field of characteristic zero, let A be an Abelian variety over K and Γ a finite rank subgroup of $A(K)$. Let $L_K = \{+, ., S, \{c_a : a \in K\}\}$ be the usual language for rings with an extra unary predicate S (and also constants for each element of K, for technical reasons). Then in the theory of the L_K-structure $(K, +, ., \Gamma, a)_{a \in K}$, where the new predicate S is interpreted by the group Γ, the definable group Γ is of linear type.*

To see that the above statement implies Mordell-Lang, one only needs to check that if X is a Zariski irreducible closed subset of A and if $X \cap \Gamma$ is a finite boolean combination of translates of subgroups of Γ, then in fact it is a finite union of translates of subgroups. This is fairly straightforward, using the properties of the Zariski topology on groups. For the other direction, note first

that Mordell-Lang says something not only about A but also about Cartesian products of A: just consider A^n which is also an Abelian variety hence also satisfies the conclusion of Mordell-Lang. Then there remains only to pass from information about the intersections with Γ^n of all *closed irreducible* subsets of A^n to the intersections with Γ^n of *all* definable subsets of K^n, in the new language.

Model theory has developed abstract criteria in terms of independence which characterize, among the definable groups, those which are of linear type. We will see this in the next section with the definitions of stable and one-based. But the problem is that, with this very brutal way of making the group Γ definable, by just adding a name for it, it is not easier to show that Γ is now of linear type than it was to show the original statement. So the strategy is going to be to add some new structure to the field K, in order to add new definable subsets but in a way we can control, for example in such a way that yields a good dichotomy between groups of linear type and the others. This is what will be achieved, for the group $Tor(A)$, by adding a field automorphism, as we will explain in the last part of this paper. We will not be able to actually make $Tor(A)$ itself definable but will find a new definable subgroup of A, containing $Tor(A)$, and which we will be able to show is of linear type - and this will suffice.

This extension process, in which the original theory of algebraically closed fields is replaced by an enriched theory, is characteristic of the model theoretic approach to such questions. It should be noted that this was also the approach taken by Buium in [3]. As Hrushovski did after him, in the function field case, Buium added a derivation, denoted δ, and confined the group Γ within a δ-closed subgroup of finite rank. He then proceeded to use the tools of differential algebra and jetspaces in order to reach the desired result.

In the case of the model theoretic approach, there are two good reasons that make this extension necessary. This approach is based on the powerful abstract tools that were previously developed around the dichotomy linear type/non linear type for definable (or infinitely definable) groups. In the original theory of algebraically closed fields, the smallest definable group containing $Tor(A)$ is the Zariski closure of $Tor(A)$ in A, that is A itself. Even more relevant is the fact, already mentioned above, that no infinite group definable in an algebraically closed field (in the pure language of fields) is of linear type.

2.3. Independence and rank. We have just seen how to fit the Mordell-Lang conjecture into the model theoretic framework of the theory of algebraically closed fields. But algebraically closed fields, together with vector spaces, are also the main examples which motivated many of the definitions essential to stability theory. Before giving the actual abstract definitions of forking, independence and rank, we will consider them in this concrete context.

We keep the same conventions and K is still an algebraically closed field of characteristic zero and of infinite transcendence degree over the rationals.

The abstract notion of independence from model theory coincides with the classical notion of algebraic independence. Recall that if $K_0 \prec K_1 \prec K$ and $K_0 \prec K_2 \prec K$, we say that K_1 and K_2 are algebraically independent over K_0 if any finite set of elements of K_2 algebraically independent over K_0 remains independent over K_1. When K_0 is algebraically closed, this is equivalent to K_1 and K_2 being linearly disjoint over K_0, i.e. such that every finite set of elements of K_2 which is linearly independent over K_0 remains linearly independent over K_1.

DEFINITION. Let A, B, C be subsets of K; we say that A and B are **independent** over C if the two fields $(\mathbb{Q}(AC))^{alg}$) and $(\mathbb{Q}(BC))^{alg}$) are algebraically independent over $(\mathbb{Q}(C))^{alg}$.

There are many different notions of rank that one uses in model theory. In the case of algebraically closed fields, they all coincide with the classical algebraic notion of dimension.

DEFINITION. Let $E \subseteq K^n$ be a definable subset of K. Let $K_0 \prec K$ be an algebraically closed subfield containing the parameters necessary to define E. We define the **rank** or **dimension** of E over K_0, $Dim(E/K_0)$, to be the maximum of the transcendence degrees of the fields $K_0(e)$ over K_0, when e varies in E.

For $E \subseteq K^n$, the dimension of E is at most equal to n, which is the dimension of K^n itself.

Note that for a finite tuple $e \in K^n$, if $K_0 \prec K_1 \prec K$, then e is independent from K_1 over K_0 if and only if the transcendence degree of $K_1(e)$ over K_1 remains equal to the transcendence degree of $K_0(e)$ over K_0.

The next two properties will tell us that the theory of algebraically closed fields is stable and is not one-based:

Properties: **1.** Let $K_0 \preceq K_1 \preceq K$, be algebraically closed subfields of K. Suppose that a, b finite tuples in K are such that $(K_0(a))^{alg}$ and $(K_0(b))^{alg}$ are K_0-isomorphic and that K_1 is linearly disjoint from each of $(K_0(a))^{alg}$ and $(K_0(b))^{alg}$ over K_0. It is then classical algebra that $(K_1(a))^{alg}$ and $(K_1(b))^{alg}$ are isomorphic over K_1. This is the uniqueness of "independent extensions" over models.

2. There exist K_1, K_2, algebraically closed subfields of K, which are not independent over their intersection. Take a, b, c three transcendental independent elements in K. We claim that $\mathbb{Q}(a,b)^{alg}$ and $\mathbb{Q}(c, ac+b)^{alg}$ are not algebraically independent over $L := \mathbb{Q}(a,b)^{alg} \cap \mathbb{Q}(c, ac+b)^{alg}$. First we check that $L = \mathbb{Q}^{alg}$. Indeed, suppose there is some $d \in L \setminus \mathbb{Q}^{alg}$; then $ac+b \in \mathbb{Q}(d,c)^{alg}$. Let $P(X,Y)$ be an irreducible polynomial with coefficients in $\mathbb{Q}(d)^{alg}$ such that $P(c, ac+b) = 0$. The polynomial $P(X,Y)$ remains irreducible over $\mathbb{Q}(a,b)^{alg}$, hence up to multiplication by an element of $\mathbb{Q}(a,b)^{alg}$ it must be equal to $(Y - aX - b)$. But this implies that both a and b are in $\mathbb{Q}(d)^{alg}$ which is impossible. It is now clear that $\mathbb{Q}(a,b)^{alg}$ and $\mathbb{Q}(c, ac+b)^{alg}$ are not algebraically

independent over $\mathbb{Q}^{alg}$ as $\mathbb{Q}(a,b,c,ac+b)^{alg} = \mathbb{Q}(a,b,c)^{alg}$ has transcendence degree three over $\mathbb{Q}^{alg}$ and each of $\mathbb{Q}(a,b)$ and $\mathbb{Q}(c,ac+b)$ has transcendence degree two.

§3. Independence, simplicity, stability, modularity. We are first going to define what we mean when we talk about an *abstract relation of independence*. In model theory, or more precisely in stability or in geometric model theory, we often explain that we are working in structures where one can define a "good" notion of independence and then proceed directly to classical examples which are particular instances of such an abstract independence, without actually giving the precise abstract definition. I will give here a precise axiomatic definition because I find it quite remarkable that there is a fairly "simple" axiomatic way to define what a relation of independence should be. On the other hand one should be aware that this definition is not a good practical tool: in practice when given a structure, if one wants to see if there is a good relation of independence, one will use other definitions such as the original definition of "forking" of Shelah. One should also be aware that I will present here as definitions (of simplicity and of stability in particular) properties which were in fact theorems established a posteriori from the original definitions.

In section 3.3, I present four easy examples of independence relations which illustrate the various definitions and properties given in sections 3.1 and 3.2.
Conventions: We have a complete theory T in a countable first-order language L. In order to avoid heavy notation, we suppose that we are working inside a *monster model* $\mathfrak{M}$ of T: this means that all sets of parameters we consider, usually denoted $A, B, C \ldots$ are subsets of $\mathfrak{M}$, of cardinality strictly smaller than the cardinality of $\mathfrak{M}$, and all models of T, usually denoted $M, N \ldots$ are elementary sub-models of $\mathfrak{M}$, also of cardinality strictly smaller than the cardinality of $\mathfrak{M}$. Definable sets will be usually denoted $D, E, F \ldots$, for example, E is a definable set in $\mathfrak{M}$ with parameters from A, will mean that $E \subseteq \mathfrak{M}^n$ for some n and that E is the set of n-tuples in M satisfying a particular formula (in n free variables) with parameters from the set A. We do not make any difference in notation between elements and finite tuples.

Furthermore we suppose that this monster model $\mathfrak{M}$ is saturated, which has the following consequences:

- any infinite conjunction of formulas of cardinality strictly smaller than $|\mathfrak{M}|$ which is finitely consistent is realized in $\mathfrak{M}$.

- any two n-tuples a and b satisfy exactly the same formulas over some set C if and only if there is an automorphism of $\mathfrak{M}$ which takes a to b and fixes C point-wise. In that case we write that $a \equiv_C b$ and say that a and b *have the same type over* C.

One brutal way to do this is to suppose that the cardinality of $\mathfrak{M}$ is an inaccessible cardinal. But one should not worry about this, everything that is

done using using these properties of $\mathfrak{M}$, could be done otherwise, with much more cumbersome notation, by constantly changing the model we are working with to an ad hoc sufficiently big one.

3.1. Abstract independence. An *independence relation* in $\mathfrak{M}$ is a relation (or a collection of triples) $\mathfrak{I}(c, B, A)$ where c ranges over finite tuples of $\mathfrak{M}$ and A, B over subsets of $\mathfrak{M}$, with $A \subseteq B \subset \mathfrak{M}$, which satisfies the following conditions:

1. (invariance) $\mathfrak{I}$ is invariant under automorphisms of $\mathfrak{M}$
2. (local character) for any c, B there is some countable $A \subseteq B$ such that $\mathfrak{I}(c, B, A)$
3. (finite character) $\mathfrak{I}(c, B, A)$ if and only if for every finite tuple b from B, $\mathfrak{I}(c, A \cup \{b\}, A)$
4. (extension) for any c, A and $B \supseteq A$, there is some d such that $c \equiv d$ over A and $\mathfrak{I}(d, B, A)$
5. (symmetry) for any b, c, A $\mathfrak{I}(c, A \cup \{b\}, A)$ if and only if $\mathfrak{I}(b, A \cup \{c\}, A)$ also
6. (transitivity) suppose that $A \subseteq B \subseteq C$, then $\mathfrak{I}(e, C, B)$ and $\mathfrak{I}(e, B, A)$ if and only if $\mathfrak{I}(e, C, A)$.

These properties make it legitimate to say, for any B,C and A subsets of $\mathfrak{M}$, that B and C are $\mathfrak{I}$-*independent* over A if for every finite subset c of C, $\mathfrak{I}(c, B \cup A, A)$.

There is a first trivial example, where one puts in $\mathfrak{I}$ all possible triples (c, B, A), $A \subseteq B$. In a (monster) algebraically closed field K, if one sets $\mathfrak{I}$ to be the set of triples (e, K_2, K_1) where $K_1 < K_2$ are algebraically closed subfields of K and e and K_2 are independent over K_1 in the sense of section 2.3, then $\mathfrak{I}$ is an abstract independence relation. We give four more examples in section 3.3. In addition, we will see the two theories of enriched fields presented in section 4, differentially closed fields of characteristic zero and algebraically closed fields with automorphisms.

The independence relations in these different examples do not all behave similarly. For many years, the crucial dividing line was between stable theories and unstable theories. In the past few years, this line has shifted to include a much larger class of theories in which the tools of "geometric stability" apply, the simple theories.

Simple theories were originally introduced by Shelah in 1980, but it was only after work of Hrushovski on specific examples and then of Kim, and Kim and Pillay, that the following property and its consequences was isolated:

THE INDEPENDENCE THEOREM: We say that the independence relation $\mathfrak{I}$ satisfies the **independence theorem** (over models) if,

For any model M, and any a, b, c, d finite tuples such that

- a and b are $\mathfrak{I}$-independent over M,
- c and a (resp. d and b) are $\mathfrak{I}$-independent over M,

- $c \equiv d$ over M,

there is some e such that e and $\{a, b\}$ are $\mathfrak{I}$-independent over M, $e \equiv c$ over $M \cup \{a\}$ and $e \equiv d$ over $M \cup \{b\}$.

The independence theorem says that one can "amalgamate" types in an independent way.

DEFINITION. We say that T is **simple** if there is a notion of independence $\mathfrak{I}$ in T which satisfies the independence theorem over models.

We can already remark (which is rather reassuring) that the first trivial example, that is the relation $\mathfrak{I}$ consisting of all triples, does not satisfy the independence theorem (take $a \neq b, a = c$ and $b = d$).

The independence theorem is in fact a very strong condition, as it forces the independence relation to be uniquely determined:

PROPOSITION 3.1. *If T is simple then the relation $\mathfrak{I}$ for which T satisfies the independence theorem is uniquely determined (and is the notion of non-forking as originally defined by S. Shelah).*

DEFINITION. We say that T is **stable** if there is a notion of independence $\mathfrak{I}$ in T which satisfies the following property (**stationarity over models**): for any model M of T, for any a, b finite tuples such that $b \equiv a$ over M, and for any $C \supseteq M$, if a and C (resp. b and C) are $\mathfrak{I}$-independent over M, then $a \equiv b$ over C.

Stability means that, if $M \subseteq C$, there is (up to isomorphism) only one way C and a can be independent over M.

IF T IS STABLE, THEN T IS SIMPLE: given a, b, c, d and M as in the independence theorem, by the extension property, we know that there is some c' (resp. some d') which looks like c (resp. like d) over $M \cup a$ and is independent from $\{a, b\}$ over M. By stability, as $c \equiv d$ over M , then $c' \equiv d'$ over $M \cup \{a, b\}$, so we also have $c' \equiv d$ over b.

One of the main consequences of stability, which is used in an essential way for example in the group configurations type of constructions, is that certain subsets turn out to be definable: given a model M, a formula $\phi(x, y)$ and some tuple b in $\mathfrak{M}$ (the monster model), the set of tuples a in M such that $\phi(a, b)$ holds is a definable subset of M, definable with parameters from M.

Examples (1) and (2) from section 3.3 are stable, (3) is simple but not stable and (4) is not simple. Algebraically closed fields (ACF_p) are stable, as shown by Property 1 in 2.3. Differentially closed fields of characteristic zero (DCF_0, section 4.1) are stable, algebraically closed fields with an automorphism (ACFA, section 4.2) are simple but not stable.

Finally, we will need an essential notion which was originally introduced by Shelah in the context of stable theories, namely orthogonality:

DEFINITION. Let T be a simple theory, $M \preceq \mathfrak{M}$, and E and F two definable subsets in $\mathfrak{M}$. We say that E and F are **orthogonal** over M if for every finite

sequence of elements e from E, and for every finite sequence of elements f from F, e and f are independent over M.

3.2. Modularity. First we are going to need a local version of stability; there may be stable definable subsets inside a model whose theory is not stable, as we will see in the next section when looking at algebraically closed fields with an automorphism.

From now on we suppose that T is a simple theory, hence that there is a (unique) notion of independence which satisfies the independence theorem.

We also suppose that T has elimination of imaginaries (this is relevant for the definition we give here of modularity). Recall that T has **elimination of imaginaries** if for every definable equivalence relation E on $\mathfrak{M}^n \times \mathfrak{M}^n$, there is a definable map f_E from $\mathfrak{M}^n$ to some $\mathfrak{M}^k$ such that, for all a, b in $\mathfrak{M}^n$, $f_E(a) = f_E(b)$ if and only if a and b are E-equivalent. We mentioned in the previous section that algebraically closed fields had elimination of imaginaries.

DEFINITION. Let $F \subseteq \mathfrak{M}^n$ be a definable subset with parameters from A. We say that F is **stable** if, for all model $M \preceq \mathfrak{M}$, $A \subseteq M$, for all a, b tuples from F and all $C \supseteq M$, if $a \equiv b$ over M, a and C are independent over M and b and C are independent over M, then $a \equiv b$ over $M \cup \{C\}$.

Keeping in mind that we wish to study the induced structure on some definable subsets, we are also going to need:

DEFINITION. Let $F \subseteq \mathfrak{M}^n$ be a definable subset with parameters from A. We say that F is **stably embedded** in $\mathfrak{M}$ if for every k and every definable subset $D \subseteq \mathfrak{M}^{nk}$, there is some definable $D' \subseteq \mathfrak{M}^{nk}$, definable *with parameters from* F, such that $D \cap F^k = D' \cap F^k$. In a stable theory, any definable set is both stable and stably embedded. In an unstable theory, a set can be stably embedded without being stable (it will be the case for example of the fixed field in a model of ACFA_0, see section 4.2.1) or stable without being stably embedded.

THE MODEL THEORETIC ALGEBRAIC CLOSURE: Recall that we say that a is **algebraic** over A ($a \in acl(A)$) if there is a finite set F, definable with parameters from A, such that $a \in F$; equivalently if a has a finite number of conjugates by the automorphisms of $\mathfrak{M}$ which fix A point-wise.

DEFINITION. Let F be a definable subset of $\mathfrak{M}^n$. We say that F is **locally modular** or **one-based** if for all C, all a, b finite tuples of elements from F, a and b are independent over $acl(C \cup \{a\}) \cap acl(C \cup \{b\})$. We say that the theory T is one-based if the formula "$x = x$" (i.e. $F = \mathfrak{M}$) is one-based.

The notion of modularity, in presence of stability, gives information of an algebraic type about the structure. We will not use this result here but in particular, any non trivial relation between three elements has to come from the action of an Abelian group. If we have a stable theory T and a definable

group $(G, .) \subseteq \mathfrak{M}^n$, then there are a, b independent elements of G such that a, b and $a.b$ are pairwise independent but not independent ($a.b$ is not independent from $\{a, b\}$). I am not going to prove this here but it is easy to check that this is true for example in algebraically closed fields for both addition and multiplication (take a, b two algebraically independent transcendental elements over $\mathbb{Q}$). So the existence of three such elements is necessary for the existence of a stable definable group. Local modularity implies that it is also a sufficient condition.

PROPOSITION ([2]). *Suppose that T is stable and one-based and that there are a, b, c finite tuples in $\mathfrak{M}$ which are pairwise independent but not independent, i.e. a and b, c are not independent. Then there is an infinite Abelian group definable in $\mathfrak{M}$.*

In fact one can draw much stronger conclusions from the existence of such a, b, c; the above is just a very weak version of the existing results. We will not be using this "group construction" here anyways but in contrast the following proposition is fundamental for what we are going to do. It is interesting to note that it was proved in 1985, hence long before the relation with Diophantine questions of the Manin-Mumford or Mordell-Lang type was realized.

PROPOSITION ([17]). *Let G be a definable group in $\mathfrak{M}^n$ which is stable, stably embedded and one-based. Then for any m and for any definable set in $\mathfrak{M}^{nm}$, $X \cap G^m$ is a finite boolean combination of cosets of definable subgroups of G^m.*

It follows that G has a definable Abelian subgroup of finite index. In any theory of modules, by the quantifier elimination to positive primitive formulas, it is true that any definable subset is a boolean combination of cosets of (positive primitive) definable subgroups. What the above says is that if G is one-based, then the structure induced by $\mathfrak{M}$ on G reduces to that of a "generalized module", that is a module with predicates for some subgroups.

Property 2, in section 2.3, shows that algebraically closed fields are not one-based. The same argument will be used later in section 4 to show that the two theories of enriched fields we consider there are not one-based either. In fact, more generally, one-basedness rules out the existence of a definable field. But, as we will see, some of the definable subsets inside an enriched field can be one-based and this is at the heart of the applications to algebraic geometry. As we have mentioned earlier, in the theory of (non enriched) algebraically closed fields, this cannot happen, and no definable set can be one-based. This comes from the fact that this theory is "unidimensional", that is, any two definable subsets are not orthogonal.

The three stable examples from section 3.3, are one-based. In order to check this more easily, we will now introduce the notion of strongly minimal sets. This notion and its link to combinatorial geometries was essential to the development of geometrical stability theory.

STRONGLY MINIMAL SETS: As we have mentioned above, the use of imaginary elements in the definition of local modularity is crucial. There is a context though in which one can avoid using imaginaries in the definition (or avoid assuming that the theory eliminates imaginaries) namely that of strongly minimal sets.

We say that a definable set $D \subseteq \mathfrak{M}^n$ is **strongly minimal** if for any other definable $F \subseteq \mathfrak{M}^n$, $F \cap D$ is finite or $D \setminus (F \cap D)$ is finite. We say that the theory T is strongly minimal if the formula "$x = x$" is strongly minimal. The theory ACF_0 of algebraically closed fields of characteristic 0 is strongly minimal: a Zariski closed subset of K is the zero set of a finite number of polynomial equations in one variable, and, by quantifier elimination, any definable subset K is a boolean combination of Zariski closed sets. Our first three examples below in 3.3 are also strongly minimal.

In a strongly minimal theory, (model-theoretic) algebraic closure gives rise to the unique independence relation satisfying the independence theorem, which is also stable: e and C are independent over B if e does not belong to $acl(C) \setminus acl(B)$. Moreover, considered as a closure operator, algebraic closure in a strongly minimal set satisfies the exchange principle and gives rise to a pregeometry in the classical sense (see for example [30]). Then one-basedness, or local modularity, corresponds to the local modularity of the associated pregeometry in the usual combinatorial use of the word and can be expressed in the following way:

Let T be a strongly minimal theory (with or without elimination of imaginaries). Then T is locally modular, or one-based, if and only if for all a, b finite tuples of elements from $\mathfrak{M}$ such that $acl(a) \cap acl(b) \neq acl(\emptyset)$, a and b are independent over $acl(a) \cap acl(b)$.

3.3. Some basic examples. We present here four basic examples. In these four examples, as well as in algebraically closed fields, the relation of independence is given by the relation of (model theoretic) algebraic closure. This means that we define A to be independent from B over C if and only if for no $a \in A$, $a \in [acl((A \setminus \{a\}) \cup B \cup C)] \setminus [acl((A \setminus \{a\}) \cup C)]$. There are two important remarks to be made about this: first, this is a special situation, there are many examples where independence is not given directly by the algebraic closure, in particular the two examples of fields we will see in the next section. Secondly, it is not always the case that (model theoretic) algebraic closure gives rise to an independence relation in our sense. In particular the symmetry axiom is not always true (it corresponds to the fact that model-theoretic algebraic closure, considered as a closure operator, satisfies the exchange property, which is not always the case).

(1) Equality. Let L be the language consisting only of equality, and consider the theory in L which says that there are infinitely many distinct elements. This is a totally categorical theory, that is, it has exactly one model (up to isomorphism) in every (infinite) cardinality. It is clearly strongly minimal.

Let E be an infinite set, hence a model. For $A \subseteq B \subset E$, and for $\bar{e} \in E^n$, say that $\bar{e} = (e_1, \dots, e_n)$ is independent from B over A if for every i, $1 \leq n$, $e_i \in B$ iff $e_i \in A$. This is an abstract relation of independence which is stable and one-based (use the characterization of one-basedness in the case of strongly minimal sets at the end of the preceding section as this theory does not strictly speaking have elimination of imaginaries: one cannot eliminate for example the equivalence relation on n-tuples which define the same n element set).

Note that any set of pairwise independent elements is independent, hence (as one might expect) there is no definable group in any model.

(2) Vector spaces. Take a countable division ring S (finite or infinite) and V an infinite dimensional vector space over S. Consider V as an L_S-structure, where L_S is the language with addition, zero, and a unary function f_s for each element s of S, interpreted as scalar multiplication by s in V. The theory of infinite S-vector spaces, which we denote by T_S, is complete and admits quantifier elimination. If S is finite, T_S has one model up to isomorphism in every infinite cardinality; if S is infinite, T_S has countably many countable models and one model in each uncountable cardinality. This theory is strongly minimal. For $C \subseteq B \subset V$, and for $A \subseteq V$, say that A is independent from B over C if A and B are linearly independent over C: for every $a \in A$, a is in the subspace spanned by $B \cup (A \setminus \{a\})$ iff a is already in the subspace spanned by $C \cup \cup (A \setminus \{a\})$. Then again this is a stable one-based theory. The fact that it is one-based corresponds exactly to the fact that vector spaces satisfy the classical dimension equality: for any finitely generated subspaces X, Y of V,

$$\dim(X) + \dim(Y) = \dim(X \cup Y) - \dim(X \cap Y).$$

There is a group of course in V and if v and w are independent, then the set $\{v, w, v + w\}$ is an example of a set which is pairwise independent but not independent.

(3) The random graph. Take the language $L = \{R\}$ with one binary relation R and consider the theory of the random graph E_R which is axiomatized by the following infinite scheme of axioms:

- R is symmetric irreflexive

- for every distinct $a_1, \dots, a_n$ and $b_1, \dots, b_m$, there exists x such that for all $i, 1 \leq i \leq n$, $R(x, a_i)$ and for all $j, 1 \leq j \leq m$, (not $R(x, b_j)$).

The theory of E_R admits quantifier elimination, has only one countable model (but has 2^κ non isomorphic models of power κ for every uncountable cardinal κ). Define independence as in example (1) above, i.e. for $A \subseteq B \subset E$, and for $\bar{e} \in E^n$, say that $\bar{e} = (e_1, \dots, e_n)$ is independent from B over A if for every i, $1 \leq n$, $e_i \in B$ iff $e_i \in A$.

With this notion of independence, this theory is simple, as is easily checked. It follows that this is the unique possible way to obtain a relation of independence satisfying the independence theorem. But the theory is not stable; consider two models $M \prec N$ and two elements a and b such that a is not in

relation via R to any element of N and b is related to exactly one element which is in $N \setminus M$. Then $a \equiv_M b$, a and b are each independent from N over M, but it is not the case that $a \equiv_N b$.

(4) Real closed fields. Consider the theory of the reals $\mathbb{R}$ in the language $L_{ord} = \{0, 1, +, -, ., <\}$ of ordered rings. The theory of $\mathbb{R}$, the theory of real closed fields, admits quantifier elimination and is o-minimal (i.e. every definable subset of $\mathbb{R}$ is a finite union of singletons and open intervals, allowing endpoints from $\mathbb{R} \cup \{\infty, -\infty\}$)). Take the relation of independence given by real closure (= algebraic closure in the model theoretic sense):

For $A \subseteq B \subset E$, and for $\bar{e} \in E^n$, say that $\bar{e} = (e_1, \ldots, e_n)$ is independent from B over A if for every i, $1 \leq n$, e_i is in the real closure of the field generated by $B \cup \{e_1, \ldots, e_{i-1}\}$ if and only if e_i is already in the real closure of the field generated by $A \cup \{e_1, \ldots, e_{i-1}\}$. This defines an independence relation which does not satisfy the independence theorem: in a big non standard model take a, b, c, d, such that $\mathbb{R} \ll c \ll a \ll b \ll d$, (where $x \ll y$ means that y is infinitely bigger than x), everything being independent over $\mathbb{R}$. No e can satisfy both $e \equiv c$ over $\mathbb{R} \cup \{a\}$ and $e \equiv d$ over $\mathbb{R} \cup \{b\}$.

The same kind of argument shows more generally that in the presence of a definable total ordering no independence relation can be simple.

3.4. Some references. Simple theories were first introduced by Shelah in 1980 in [42] as a class strictly containing stable theories. It was not known at the time if in simple theories, as defined there, forking was a symmetric relation. The interest for this class of theories was revived in the past few years for two reasons. First, it was realized by Hrushovski that many very interesting classes of algebraic structures were simple and that in these structures forking seemed to have very good properties (the independence theorem, symmetry etc). This was in particular the case of smoothly approximated structures ([16], for surveys see for example [6], [28]), pseudo-finite fields (see [18]) and of course a little later of algebraically closed fields with an automorphism which we describe in the next section. At around the same time, Kim proved that in simple theories forking was symmetric [22]. This changed the perspective on simple theories and also on what having a good relation of independence should mean. The definitions of independence, simplicity etc. which I gave in the preceding sections come from further work on the subject by Kim and Pillay [23]. For a survey on simple theories with the main results and open questions, there is [24]. A book by F. Wagner has recently appeared on this subject [44]

Concerning geometric stability, the main reference is A. Pillay's book "Geometric Stability" ([34]). More specifically on stable groups, see the books by B. Poizat(the original [37] or the recent english version [38]) and by F. Wagner [43].

§4. Fields with extra structure and the applications. All the present applications of model theory to classical Diophantine geometry questions fit into a common general framework. Each time, one uses a field with more definable sets than just the classical constructible ones and where a good dichotomy theorem is available which enables one to recognize when a group is one-based. Three theories have been used so far:
(1) separably closed fields of characteristic $p > 0$ for the function field Mordell-Lang conjecture in characteristic p [15];
(2) differentially closed fields of characteristic zero for the function field Mordell-Lang conjecture in characteristic 0 [15];
(3) algebraically closed fields with an automorphism, in characteristic zero for the Manin-Mumford conjecture [13] and the Tate-Voloch conjecture [39], as well as in characteristic p for the case of Drinfeld modules [40].

We will present the two theories of fields used in the characteristic zero cases, differentially closed fields and algebraically closed fields with an automorphism, and then finish with a short sketch showing how to apply the model theoretic results in the case of a field with an automorphism in order to obtain the Manin-Mumford conjecture. At the end (section 4.4) we give a selection of references for surveys or introductory papers to all of these applications.

Both the theories we are going to discuss are expansions of algebraically closed fields by a unary function.

4.1. Differentially closed fields of characteristic zero. (see [32] or [1]).

The language is the usual language of rings L_R, which we already used for algebraically closed fields, together with a map δ.
The theory (DCF_0) consists of the following scheme of axioms (i) to (iii):

(i) K is a field of characteristic zero

(ii) (K, δ) is a differential field, that is, δ is a derivation :
$\delta : K \mapsto K$, such that, for all x, y in K, $\delta(x + y) = \delta(x) + \delta(y)$ and $\delta(xy) = x\delta(y) + y\delta(y)$.

Before stating the third set of axioms, we need some definitions. Given a differential field (K, δ), we define the ring $K_\delta[X]$ of differential polynomials (in one variable) over K to be the ring of polynomials in infinitely many variables

$$K[X, \delta(X), \delta^2(X), \ldots, \delta^n(X) \ldots].$$

The *order* of the differential polynomial $f(X)$ in $K_\delta[X]$ is -1 if $f \in K$ and otherwise the largest n such that $\delta^n(X)$ occurs in $f(X)$ with non zero coefficient. For example the differential polynomial equation $\delta(X) = 0$ which defines the *constants* for the derivations δ has order 1.

(iii) K is existentially closed. In this context, this can be axiomatized by saying (an infinite scheme): for any non-constant differential polynomials $f(X)$ and $g(X)$, where the order of $g(X)$ is strictly less than the order of $f(X)$, there is a z such that $f(z) = 0$ and $g(z) \neq 0$.

BASIC RESULTS: DCF_0 is a complete theory which admits quantifier elimination and elimination of imaginaries. We call the models of DCF_0 the differentially closed fields. It is the model completion of the theory of differential fields of characteristic zero, so, in particular, any differential field (K, δ) embeds into a differentially closed field (L, δ). Differentially closed fields are algebraically closed fields and one can show that they have infinite transcendence degree over $\mathbb{Q}$.

From now on (K, δ) is a monster model of DCF_0.

4.1.1. DEFINABLE SETS IN DCF_0. We saw earlier that in a "pure" algebraically closed field, the basic definable sets are the zero sets of polynomials. Here we start with the zero sets of differential polynomials. For any n let $K_\delta[X_1, .., X_n] = K[X_1, .., X_n, \delta(X_1), .., \delta(X_n), \delta^2(X_1), .., \delta^2(X_n), ..]$.
We say that $F \subseteq K^n$ is a **δ-closed set** if there are $f_1, \ldots, f_r \in K_\delta[X_1, \ldots, X_n]$ such that $F = \{(a_1, \ldots, a_n) \in K^n; f_1(a_1, \ldots, a_n) = \ldots = f_r(a_1, \ldots, a_n) = 0\}$. The ring $K_\delta[X_1, \ldots, X_n]$ is of course not Noetherian but the δ-closed sets (which correspond to radical differential ideals) form the closed sets of a Noetherian topology on K, the δ-topology.

We now consider the δ-constructible sets, that is, the finite boolean combinations of δ-closed sets. The elimination of quantifiers for DCF_0 means that this class is closed under projection hence that all definable sets (we call them δ-definable sets) are δ-constructible.

Examples: First, if $D \subset K^m$ is a set definable in the language L_R, without using δ, as K is algebraically closed, D is constructible. This is a particular case of a δ-constructible set. Exactly as in the case of algebraically closed fields, if V is a variety defined over K, we can consider V as a δ-definable set.

The **field of constants of** K, $Cons(K) = \{a \in K; \delta(x) = 0\}$ is a δ-closed set which is not constructible; it is an algebraically closed subfield of K.

The induced structure on $Cons(K)$ is that of a **pure algebraically closed field**: if D is a δ-definable subset of K^n, $D \cap Cons(K)^n$ is a constructible subset (in the language of rings L_R) of $Cons(K)^n$, definable with parameters from $Cons(K)$.

We define the **δ-algebraic closure** of A, $acl_\delta(A)$, to be equal to the algebraic closure (in the usual sense of fields) of the differential field generated by A, i.e. the algebraic closure of the field $(A)_\delta := \mathbb{Q}(\delta^i(a); a \in A, i \geq 0)$ (this is exactly the algebraic closure of A in the usual model theoretic sense).

4.1.2. INDEPENDENCE AND RANK. If $C \subset A, B \subset K$, we say that A and B are **δ-independent** over C if $acl_\delta(A)$ and $acl_\delta(B)$ are algebraically independent (or equivalently linearly disjoint) over $acl_\delta(C)$. This δ-independence is a notion of independence in the sense of section 3.1 and DCF_0 is stable. One can check the stability easily thanks to the quantifier elimination: let $K_0 < K$ be a sub-model and let a and b be such that $a \equiv b$ over K_0. So in particular, the ideal $I(a/K_0)$ of the differential polynomials f in $K_{0\delta}[X]$ vanishing on a is equal to the corresponding ideal for b, $I(b/K_0)$. By definition of δ-independence, if $K_0 < K_1 < K$ and if a (resp. b) and K_1 are δ-independent

over K_0, then the ideal $I(a/K_1)$ is generated by $I(a/K_0)$, and similarly for b, $I(b/K_1)$ is the ideal generated by $I(b/K_0)$. It follows that $I(a/K_1) = I(b/k_1)$, and by quantifier elimination this implies that $a \equiv b$ over K_1.

In fact the theory DCF_0 is more than stable, it is what is called ω-stable, which means that it is possible to assign a rank (taking possibly infinite ordinal value) to each definable set. We are only going to consider definable sets with finite rank and give the definition of one rank, which will be sufficient for our purpose. The reader should be aware though that there are many different notions of rank available in model theory and that it is now known that no two of them coincide everywhere in DCF_0 (the Lascar rank, the Morley rank, the δ-degree we are going to define below...).

If E is a differential subfield of K and if a is a finite sequence of elements of K, we define the δ-**degree** of a over E, $d_\delta(a/K)$, to be the transcendence degree of the field $(E(a))_\delta$, the differential field generated by E and a, over E. If $D \subseteq K^n$ is a δ-definable set, we define the δ-degree of D to be the maximum of the δ-degrees of the elements of D.

The field $Cons(K)$ has δ-degree equal to one: for any differential subfield E, for any a element of $Cons(K)$, the differential field generated by E and a is equal to the field $E(a)$. Moreover, and this is fundamental for the application to Diophantine geometry, up to definable isomorphism, $Cons(K)$ *is the unique δ-definable field with finite δ-degree* .

In contrast, if V is any variety (of positive dimension) defined over K, as a δ-definable set, V has infinite δ-degree; this is in particular the case of K itself. When it is finite the δ-degree is a good notion of rank, in particular, if $d_\delta(a/E)$ is finite, then a and $B \supset E$ are δ-independent over E if and only if $d_\delta(a/E) = d_\delta(a/B)$.

4.1.3. Modularity and the dichotomy theorem. The results below come from [19] and [15].

The field (K, δ) is not one-based, but neither is the definable subfield $Cons(K)$, by exactly the same argument as for the theory ACFA_0: consider a, b, c in the field $Cons(K)$ which are transcendental over $\mathbb{Q}$ and algebraically independent. In order to be able to do this, we have to suppose that $Cons(K)$ has big enough transcendence degree over $\mathbb{Q}$, but we can always suppose that by going to some big model K' extending K. Then $acl_\delta(a, b) = \mathbb{Q}(a, b)^{alg}$ (the field algebraic closure) and $acl_\delta(c, ac + b) = \mathbb{Q}(c, ac + b)^{alg}$ intersect in $\mathbb{Q}^{alg}$, but they are not algebraically independent over $\mathbb{Q}^{alg}$.

For our purpose, the interesting feature of differentially closed fields of characteristic zero, is that really, the constant field is the "unique" definable set of δ-degree one which is not one-based. Let us make this statement more precise. Let D be a definable set, we have defined in 3.1 the notion of orthogonality. In this particular context, D and $Cons(K)$ are orthogonal if, for every finite sequence of elements d from D, for every finite sequence of elements b from $Cons(K)$, and for every subfield $E = acl_\delta(E)$, $acl_\delta(Ea)$ and $acl_\delta(Eb)$ are algebraically independent over E.

Recall that a δ-definable set $D \subseteq K^n$ is **strongly minimal** if, for any δ-definable $F \subseteq K^n$, $F \cap D$ is finite or cofinite in D. A strongly minimal set has finite δ-degree. The constant field is strongly minimal.

THE DICHOTOMY THEOREM FOR DCF_0. *Let $D \subseteq K^n$ be a strongly minimal δ-definable subset. Then D is one-based if and only if D and the field of constants, $Cons(K)$, are orthogonal.*

Non-orthogonality between two strongly minimal sets is a very strong relation. In particular, if D is a δ-definable group which is non-orthogonal to the field $Cons(K)$, then D will be δ-definably isomorphic to $G(Cons(K))$, where G is an algebraic group defined over the field $Con(K)$. The dichotomy theorem then means that the only strongly minimal groups which are not one-based are exactly the ones arising from algebraic groups over the constants.

Hrushovski's proof of the dichotomy theorem in [15] uses the fact that strongly minimal sets in DCF_0 are abstract Zariski geometries in the sense of Hrushovski-Zilber ([21]). One can then apply their abstract dichotomy theorem which says that if a strongly minimal set D is a non locally modular Zariski geometry, there is a strongly minimal field definable in D. Then one uses the fact that the field $Cons(K)$ is, up to definable isomorphism, the unique strongly minimal field δ-definable in K. For introductory surveys to Zariski geometries, see [20] or [31]. A direct proof of the dichotomy theorem for DCF_0 was given very recently (two years after this tutorial actually took place) in [36].

4.2. Algebraically closed fields with an automorphism. An exposition of the basic properties (axiomatizability, decidability etc.) of ACFA, can be found in Macintyre's introductory paper [27]. The in-depth model theoretic analysis was carried out first by Chatzidakis and Hrushovski in [4], and continued in [5].

The way we are going to present this theory will make it seem very similar to the previous one, differentially closed fields. But although the results are very similar, the actual proofs need not be. One should note though that again in [36], a new proof of the dichotomy theorem for ACFA in characteristic zero is given, along similar lines as the one for the differential case.

A **difference field** is a field K together with an automorphism σ, which we consider as an $L_R \cup \{\sigma\}$-structure.

The class of existentially closed models for difference fields turns out to be axiomatizable (this fact needs a proof of course). Here we restrict ourselves to the case of characteristic zero.

The axioms (ACFA_0) say that:

(i) K is a an algebraically closed field of characteristic zero

(ii) (K, σ) is a difference field, i.e. σ is an automorphism of K.

(iii) K is existentially closed : every difference equation which has a solution in some extension of K has a solution in K.

$ACFA_0$ is not a complete theory and in order to make it complete one needs to describe the action of the automorphism σ on the algebraic closure of $\mathbb{Q}$. This theory does not have elimination of quantifiers, but it does have elimination of imaginaries. Every difference field of characteristic zero embeds into a model of $ACFA_0$.

Let us mention a striking recent result about ACFA [14] answering the long open question: what is the theory of a nonstandard Frobenius automorphism or more precisely, what is the theory of an ultraproduct of the difference fields $(\mathbb{F}_p^{alg},\ \sigma : x \mapsto x^p)$ for all p prime numbers ? The answer is that ACFA is exactly the theory of all nonprincipal ultraproducts of $(\mathbb{F}_p^{alg},\ \sigma_q : x \mapsto x^q)$, when q varies on the set of powers of prime numbers.

From now on (K, σ) is a monster model of $ACFA_0$.

4.2.1. DEFINABLE SETS IN $ACFA_0$. Here the basic sets are the zero sets of difference polynomials: for any n let
$K_\sigma[X_1, .., X_n] = K[X_1, .., X_n, \sigma(X_1), .., \sigma(X_n), \sigma^2(X_1), .., \sigma^2(X_n), ..]$.
We say that $F \subseteq K^n$ is a **σ-closed set** if there are $f_1, \ldots, f_r \in K_\sigma[X_1, \ldots, X_n]$ such that $F = \{(a_1, \ldots, a_n) \in K^n; f_1(a_1, \ldots, a_n) = \ldots = f_r(a_1, \ldots, a_n) = 0\}$. The σ-closed sets form the closed sets of a Noetherian topology on K, the σ-topology. Consider now the σ-constructible sets. It is not true that every σ-definable set is σ-constructible (the theory does not eliminate quantifiers). Here is one example of a σ-definable set which is not σ-constructible: pick a in some extension of K, and extend σ to the field $K(a)$ by setting $\sigma(a) = a$. In order to extend σ to the algebraic closure of $K(a)$, there are choices to be made, in particular one can either choose to have σ fix point-wise the two square roots of a , or to have σ exchange them. This means that the set $\{x; \sigma(x) = x \ \wedge \ \exists t \ (t^2 = x \ \wedge \ \sigma(t) \neq t)\}$ is not σ-constructible.

The class of σ-definable sets is the closure under finite boolean operations and projections of the σ-closed sets.

The field $Fix(K) = \{a \in K; \sigma(a) = a\}$, the fixed field of σ in K, is σ-closed. It is not algebraically closed but it is pseudo-finite, i.e. it is an infinite model of the theory of all finite fields. It is also a "pure" field : if D is any σ-definable subset of K^n, $D \cap Fix(K)^n$ is a definable subset (in the language L_R) of $Fix(K)^n$ definable with parameters from $Fix(K)$.

We define the **σ-algebraic closure** of A, $acl_\sigma(A)$, to be equal to the algebraic closure (in the usual sense of fields) of the difference field generated by A, i.e. the algebraic closure of the field $(A)_\sigma := \mathbb{Q}(\sigma^i(a); a \in A, i \in \mathbb{Z})$.

4.2.2. INDEPENDENCE, STABILITY AND MODULARITY. If $C \subset A \subset K$ and $C \subset B \subset K$, we say that A and B are **σ-independent** over C if $acl_\sigma(A)$ and $acl_\sigma(B)$ are algebraically independent (or equivalently linearly disjoint) over $acl_\sigma(C)$. We define the **σ-degree** of a definable set exactly like the δ-degree; if $D \subseteq K^n$ is a σ-definable set, the σ-degree of D is the maximum of the transcendence degrees of the difference fields generated by elements of D. The fixed field of σ, $Fix(K)$ has σ-degree one.

This gives a notion of independence which satisfies the independence theorem over models, which we will not prove here. Hence the theory is simple. But it is not stable, because the field $Fix(K)$ is not stable: one can find $E = acl_\sigma(E) \subset K$ and $a, b, c \in Fix(K) \setminus E$, such that a and c on the one hand, b and c on the other hand, are σ-independent over E, but such that $\sqrt{a-c} \in Fix(K)$ and $\sqrt{b-c} \notin Fix(K)$ (note that this is the same example which shows that quantifier elimination does not hold). This contradicts the uniqueness of independent extensions.

Exactly as in the case of the field of constants in DCF_0, the field $Fix(K)$ is not one-based and there is also a very powerful dichotomy theorem.

THE DICHOTOMY THEOREM FOR ACFA_0. *Let $D \subseteq K^n$ be a σ-definable subset of finite σ-degree. Then D is stable, stably embedded and one-based if and only if D and the fixed field, $Fix(K)$, are orthogonal.*

4.3. Application to the Manin-Mumford conjecture. Recall the statement of the conjecture from section 2.2. Let A be an Abelian variety defined over $\mathbb{Q}^{alg}$ and let X be a sub-variety of A; then $Tor(A) \cap X$ is a finite union of translates of subgroups of $Tor(A)$.

We have explained already that this is the same as showing that $Tor(A)$ is of linear type (section 2.2), and hence, by section 3.2 "stable, stably embedded and one-based", except that $Tor(A)$ is not definable in the algebraically closed field K. Indeed, as we remarked earlier, there are *no* definable one-based subsets in a "pure" algebraically closed field , so to make this approach work one must put additional structure on the field.

So the strategy is going to be: go to some bigger algebraically closed field L and add new structure on L, hence getting new definable sets, in such a way that there is some new definable subgroup of A, denoted H, which contains $Tor(A)$, and which we can prove is stable, stably embedded and one-based.

It is not immediately obvious that this is enough: this would say that $Tor(A) \cap X$ is contained in $H \cap X$, which itself is a boolean combination of translates of subgroups of H (definable in the bigger field with the extra structure). But it is then fairly straightforward to check, using the fact that X is Zariski closed, that this does imply that $X \cap Tor(A)$ is a finite union of translates of subgroups of $Tor(A)$.

Let $k < \mathbb{Q}^{alg}$ be a finite extension of $\mathbb{Q}$ such that A is defined over k.

We want to find an algebraically closed field L and an automorphism σ of L such that (L, σ) is a model of ACFA_0 and such that there is some σ-definable subgroup of $A(L)$ (the group of L-rational points of the Abelian variety A) containing $Tor(A)$ and which is stable, stably embedded and one-based.

What kind of group H are we looking for in (L, σ)? How can we be sure that this H will indeed be stable, stably embedded and one-based, i.e. by the dichotomy theorem, will be orthogonal to $Fix(\sigma)$? Let us consider groups defined by rather simple difference equations. First $H_1 = \{a \in A(L); \sigma(a) - a = 0\}$. This is $A(Fix(\sigma))$, so of course H_1 is not orthogonal to $Fix(\sigma)$ and hence

is not stable one-based. Similarly if $H_n = \{a \in A(L); \sigma^n(a) - a = 0\}$, this is $A(Fix(\sigma^n))$. The field $Fix(\sigma^n)$ is a finite extension of $Fix(\sigma)$ and it follows that there is a σ-definable map (with finite fibers) from $(Fix(\sigma))^r$ (for some $r > 0$) onto H_n which is hence also not orthogonal to $Fix(\sigma)$.

Now these groups are particular cases of groups defined by polynomial equations. Let $P(T) = m_n T^n + \ldots + m_1 T + m_0$, where the m_i's are in $\mathbb{Z}$. Then define

$$H_P = \{a \in A(L); m_n \sigma^n(a) + \ldots + m_1 \sigma(a) + m_0 a = 0\}$$

where $+$ denotes addition in A, and for $a \in A(L)$ and $m \in \mathbb{N}$, ma denotes as usual $a + ... + a$, m *times*.

Then H_P is a σ-definable subgroup of $A(L)$ of finite σ-degree. If, for some $n \geq 1$, the polynomial $P[T]$ is not prime to $X^n - 1$, i.e. if $P[T]$ has a root which is also a root of unity, then H_P is contained in $Ker(\sigma^n - 1)$ and the argument given just above implies that H_P is not stable one-based. The remarkable result at the heart of Hrushovski's proof of the Manin-Mumford conjecture for number fields is that the converse is true:

PROPOSITION 4.1. *The group H_P is orthogonal to the field $Fix(\sigma)$ if and only if $P[T]$ has no root which is also a root of unity.*

The proof of this result goes through an analysis of the ring of σ-definable endomorphisms of $A(L)$ when A is a simple Abelian variety and then various reductions to minimal cases, using in particular the following fact: if $0 \mapsto A_1 \mapsto A_2 \mapsto A_3 \mapsto 0$ is an exact sequence of σ-definable homomorphisms, where the A_i's are σ-definable groups, then A_2 is one-based if and only if both A_1 and A_3 are one-based.

So from the dichotomy theorem for ACFA_0 one now knows that if $P[T]$ has no root which is also a root of unity, then H_P is stable, stably embedded and one-based.

Now in order to apply this, one needs to show that there is an automorphism σ of $\mathbb{Q}^{alg}$, fixing the number field k, and a polynomial $P[T]$ with integer coefficients such that no root of $P[T]$ is a root of unity and H_P contains $Tor(A)$. This part of the proof involves no model theory and consists of two steps. First, one fixes a prime p (of good reduction for A) and one considers only the p'-torsion of A, denoted $Tor_{p'}(A)$, that is, the torsion elements of order prime p. By applying a classical result of Weil ([45]) one gets such an automorphism σ_1 and a polynomial $P_1(T)$ with H_{P_1} containing $Tor_{p'}(A)$. Then using two different primes p and q, and a result of Serre ([41], pages 33-34 and 56-59), one gets the required automorphism working for the full torsion subgroup.

Fix such an automorphism σ, and extend the difference field $(\mathbb{Q}^{alg}, \sigma)$ to a model (L, σ) of ACFA_0. In (L, σ), the group H_P is of linear type, hence $X \cap H_P$ is a finite boolean combination of translates of (σ-definable) subgroups of H_P. And we can conclude that $X \cap Tor(A)$ is a finite union of translates of subgroups of $Tor(A)$.

An important remark: this sketch of the proof is correct but does not yield effective bounds for the number of translates involved in the representation of $X \cap Tor(A)$ as a finite union. In fact Hrushovski shows that one can bound the number of translates involved by a function of the degree of the polynomial $P[T]$ and of the size of its coefficients. But if one is not careful, one looses track of any effective bounds on the degree and coefficients of the polynomial $P[T]$ during the passage from the p'-torsion to the full torsion via the Serre result.

So Hrushovski in fact, in order to deal with the full torsion group, gives a more complicated proof, which uses model theory and yields sharper information. What I have described above is exactly his proof for the case of the elements of p'-torsion , $Tor'_p(A)$. In that case, the classical result of Weil mentioned above, (a result about the characteristic polynomial of the Frobenius in an Abelian variety defined over $\mathbb{F}_p$), provides directly a polynomial $P(T)$ such that its degree and the size of its coefficients are bounded by a function of p, and of invariants of A (dimension, degree). In order to deal with the full torsion and keep effective bounds, one needs to work simultaneously with two different automorphisms, σ and τ, hence two distinct models of ACFA_0, and two different polynomials, $P[T]$ and $Q[T]$, such that in $(\mathbb{Q}^{alg}, \sigma)$, H_P contains the torsion elements of order prime to p, and in $(\mathbb{Q}^{alg}, \tau)$, H_Q contains the torsion elements of order a power of p.

One last remark: in fact Hrushovski's result in [13] is more general than the one I quoted. He proves the result for all commutative algebraic groups, and not only Abelian varieties.

4.4. A selection of references on the model theory of fields and the applications to Algebraic Geometry. Some general surveys on geometric model theory and applications:

- A. Pillay, *Model Theory, Differential Algebra and Number Theory*, in Proceedings of the ICM 94, Zurich, Birkhauser 1996.
- A. Pillay, *Model Theory and Diophantine geometry*, Bull. Am. Math. Soc. 34 (1997), 405-422.
- D. Marker, *Strongly minimal sets and geometries*, Tutorial, LC '95, in [29].
- E. Hrushovski, *Geometric model theory*, in Proceedings of the ICM 98, Berlin, Vol. I,, Doc. Math., 281–302, 1998.
- A. Pillay, *Geometric Model Theory*, Tutorial, LC '99, preprint.
- T. Scanlon, *Diophantine geometry from model theory*, o Bulletin of Symbolic Logic 7 (2001), 37–57.

For surveys on algebraically closed fields with an automorphism (ACFA) and the Manin-Mumford conjecture or on the Mordell-Lang conjecture:

- J.B. Goode (B. Poizat) *H.L.M. (Hrushovski-Lang-Mordell)*, Séminaire Bourbaki, exposé 811, Février 1996.

- Z. Chatzidakis *A survey on the model theory of difference fields*, in Model Theory, Algebra and Geometry, D. Haskell and C. Steinhorn ed., MSRI Publications 2000, 65-96 ([10]).
- E. Bouscaren *Théorie des Modèles et Conjecture de Manin-Mumford [d'après E. Hrushovski]*, Séminaire Bourbaki, Exposé 870, Mars 2000.

BOOKS:

- One can find an introduction to the model theory of fields with special emphasis on differentially closed fields of characteristic zero and a survey on separably closed fields in *Model theory of fields*, D. Marker, M. Messmer and A. Pillay, Lecture Notes in Logic 5, Springer 1996 ([32]). (The Lecture Notes in Logic are now published by the ASL; a new edition of this book is planned).

- For a reasonably self-contained introduction to Hrushovski's proof of the Mordell-Lang conjecture, based on the lectures given at a summerschool held in Manchester in 1994, see *Model Theory and Algebraic Geometry*, Lecture Notes in Mathematics 1696, E. Bouscaren Ed., Springer, 1998 ([1]).

- In *Algebraic Model Theory*, B. Hart, A. Lachlan and M. Valeriote eds., NATO ASI Series, Kluwer Academic Publishers 1997 ([9]), one can find introductory lectures with proofs (by Z. Chatzidakis and A. Pillay) to Hrushovski's proof of the Manin-Mumford Conjecture .[9]

- In *Model Theory, Algebra and Geometry*, D. Haskell, A. Pillay and C. Steinhorn Eds., MSRI Publications 2000, one can find the proceedings of the introductory workshop of the MSRI semester on "Model theory of fields" (January 98 - June 98) ([10]).

REFERENCES

[1] E. Bouscaren (editor), *Model theory and algebraic geometry*, Lecture Notes in Mathematics, no. 1696, Springer, 1998.

[2] E. BOUSCAREN and E. HRUSHOVSKI, *One-based theories*, ***The Journal of Symbolic Logic***, vol. 59 (1994), pp. 579–595.

[3] A. BUIUM, *Intersections in jet spaces and a conjecture of Serge Lang*, ***Annals of Mathematics***, vol. 136 (1992), pp. 583–593.

[4] Z. CHATZIDAKIS and E. HRUSHOVSKI, *The model theory of difference fields*, ***Transactions of the American Mathematical Society***, vol. 351 (1999), pp. 2997–3071.

[5] Z. CHATZIDAKIS, E. HRUSHOVSKI, and K. PETERZIL, *The model theory of difference fields II: periodic ideals and the trichotomy in all characteristics*, ***Proceedings of the London Mathematical Society***, vol. 85 (2002), pp. 257–311.

[6] G. CHERLIN, *Large finite structures with few type*, In Hart et al. [9].

[7] D. EVANS and E. HRUSHOVSKI, *Projective planes in algebraically closed fields*, ***Proc. London Math. Soc.***, vol. 62 (1991), pp. 1–24.

[8] ———, *The automorphisms group of the combinatorial geometry of an algebraically closed field*, ***J. London Math. Soc.***, vol. 52 (1995), pp. 209–225.

[9] B. Hart, A. Lachlan, and M. Valeriote (editors), *Algebraic model theory*, NATO ASI Series, Kluwer Academic Publishers, 1997.

[10] D. Haskell, A. Pillay, and C. Steinhorn (editors), *Model theory, algebra and geometry*, MSRI Publications, 2000.

[11] M. Hindry, *Introduction to abelian varieties and the Mordell-Lang conjecture*, In Bouscaren [1].

[12] E. Hrushovski, *A new strongly minimal set*, ***Annals of Pure and Applied Logic***, vol. 62 (1993), pp. 147–166.

[13] ———, *The Manin-Mumford conjecture and the model theory of difference fields*, to appear in the Annals of Pure and Applied Logic, preprint, 1995.

[14] ———, *The first-order theory of the Frobenius*, preprint, 1996.

[15] ———, *The Mordell-Lang conjecture for function fields*, ***Journal of the American Mathematical Society***, vol. 9 (1996), pp. 667–690.

[16] E. Hrushovski and G. Cherlin, *Finite structures with few types*, to appear in the Annals of Mathematical Studies, Princeton.

[17] E. Hrushovski and A. Pillay, *Weakly normal groups*, ***Logic Colloquium '85***, North-Holland, 1987, pp. 233–244.

[18] ———, *Groups definable in local fields and pseudofinite fields*, ***Israel Journal of Mathematics***, vol. 85 (1994), pp. 203–262.

[19] E. Hrushovski and Z. Sokolovic, *Minimal subsets of differentially closed fields*, to appear in the Transactions of the American Mathematical Society.

[20] E. Hrushovski and B. Zilber, *Zariski geometries*, ***Bulletin of the American Mathematical Society***, vol. 28 (1993), pp. 315–323.

[21] ———, *Zariski geometries*, ***Journal of the American Mathematical Society***, vol. 9 (1996), pp. 1–56.

[22] B. Kim, *Forking in simple unstable theories*, ***Journal of the London Mathematical Society***, vol. 57 (1998), pp. 257–267.

[23] B. Kim and A. Pillay, *Forking in simple unstable theories*, ***Annals of Pure and Applied Logic***, vol. 88 (1997), pp. 149–164.

[24] ———, *From stability to simplicity*, ***The Bulletin of Symbolic Logic***, vol. 4 (1998), pp. 17–36.

[25] S. Lang, ***Introduction to algebraic geometry***, Interscience tracts in pure and applied mathematics, Interscience Publishers, 1958.

[26] ———, ***Abelian varieties***, Interscience tracts in pure and applied mathematics, Interscience Publishers, 1959.

[27] A. Macintyre, *Generic automorphisms of fields*, ***Annals of Pure and Applied Logic***, vol. 2-3 (1997), pp. 165–180.

[28] D. Macpherson, *Homogeneous and smoothly approximated structures*, In Hart et al. [9].

[29] J. A. Makowsky and E. V. Ravve (editors), *Logic Colloquium '95, Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Haifa, Israel*, Lecture Notes in Logic, Springer, 1998.

[30] D. Marker, *Strongly minimal sets and geometry*, In Makowsky and Ravve [29].

[31] ———, *Zariski geometries*, In Bouscaren [1].

[32] D. Marker, M. Messmer, and A. Pillay, ***Model theory of fields***, Lecture Notes in Logic, vol. 5, Springer, 1996.

[33] B. Mazur, *Abelian varieties and the Mordell-Lang conjecture*, In Haskell et al. [10].

[34] A. Pillay, ***Geometrical stability theory***, Oxford Logic Guides, vol. 32, Oxford University Press, 1996.

[35] ———, *Algebraically closed fields*, In Bouscaren [1].

[36] A. Pillay and M. Ziegler, *Jet spaces of varieties over differential and difference fields*, to appear in Selecta Math.

[37] B. Poizat, ***Groupes stables***, Nur al-matiq wal ma'rifah, 1987.

[38] ———, ***Stable groups***, Mathematical Surveys and Monographs, vol. 87, American Mathematical Society, 2001.

[39] T. Scanlon, *The conjecture of Tate and Voloch on p-adic proximity to torsion*, ***International Mathematical Research Notices Journal***, vol. 17 (1999), pp. 909–914.

[40] ———, *Diophantine geometry of the torsion of a Drinfeld module*, ***Journal of Number Theory***, vol. 97 (2002), pp. 10–25.

[41] J.P. Serre, ***Oeuvres, collected works 1985-1998***, vol. IV, Springer, 2000.

[42] S. Shelah, *Simple unstable theories*, ***Annals of Mathematical Logic***, vol. 19 (1980), pp. 177–203.

[43] F. Wagner, ***Stable groups***, London Math. Soc. Lecture Notes, vol. 240, Cambridge University Press, 1997.

[44] ———, ***Simple theories***, Mathematics and its applications, vol. 503, Kluwer Academic Publishers, 2000.

[45] A. Weil, ***Courbes algébriques et variétés abéliennes***, Hermann, 1971.

[46] B. Zilber, *Finite homogeneous geometries*, ***Proceedings of the sixth easter conference on model theory (Wendisch-Rietz 1988)***, Humboldt Univ., Berlin, 1988, pp. 186–208.

CNRS-UNIVERSITÉ PARIS 7
UFR DE MATHÉMATIQUES, CASE 7012
2 PLACE JUSSIEU, 75251 PARIS CEDEX 05, FRANCE
E-mail: elibou@logique.jussieu.fr