MODEL THEORY OF DIFFERENCE FIELDS
LECTURE NOTES
NOTRE DAME, SEP 2000

ZOÉ CHATZIDAKIS

Introduction. This is the set of notes of a special topics course I gave at Notre Dame in the Fall 2000 (September 20-October 13). I develop here some of the model theory of difference fields (a difference field is simply a field with a distinguished automorphism σ), at a fairly elementary level. I reproduce many of the classical proofs of stability theory in the particular context we are working in, my feeling being that a proof in a concrete situation is much easier to understand than in a more general context. I tried to avoid using results from stability theory, and succeeded except at one or two places (where the neophyte is asked to just accept the result). I also inserted some comments for people with a working knowledge of stability theory, and these are enclosed by the symbols □□□. These comments can simply be skipped.

The notes are organized as follows. Chapter 1 gives some preliminary algebraic results and definitions (difference fields, varieties, Zariski topology, etc.). Chapter 2 introduces the theory ACFA of generic difference fields, and proves elementary results about it. Chapter 3 introduces the notions of independence and SU-rank, and shows various results about them. In chapter 4 we study the fixed field, and in chapter 5 the notions of orthogonality and modularity. Chapter 6 introduces generics and stabilizers of groups. Finally, chapter 7 contains some of the hard results in the area, and the applications by Hrushovski to problems in number theory. At the end of the notes, you will find some references and "further reading" on difference fields, with comments.

I would like to thank A. Berenstein for his careful reading of the notes and many helpful suggestions.

Notation

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$	the natural numbers, the integers, the rational and complex numbers
$\mathbb{F}_q$	the field with q elements
$\mathcal{L}(E)$	language obtained by adjoining to $\mathcal{L}$ constant symbols for elements of E
AB	subfield of Ω generated by A and B
$A[B]$	subring of Ω generated by A and B
A^{alg}	algebraic closure of the field A
$K[X_1, \dots, X_n]_\sigma$	$= K[X_1, \dots, X_n, X_1^\sigma, \dots, X_n^\sigma, \dots, X_i^{\sigma^j}, \dots]$ = difference polynomial ring in $X_1, \dots, X_n$
$I(S)$	ideal of polynomials vanishing on the set S
$I_\sigma(S)$	ideal of difference polynomials vanishing on the set S
$I(\bar{a}/K)$	ideal of polynomials over K vanishing at $\bar{a}$
$I_\sigma(\bar{a}/K)$	ideal of difference polynomials over K vanishing at $\bar{a}$
$cl_\sigma(A)$	smallest difference field containing A = field generated by $\{\sigma^i(A) \mid i \in \mathbb{Z}\}$, with the action of σ
$acl_\sigma(A)$	$cl_\sigma(A)^{alg}$
U^σ	variety conjugate of U under σ
$U(K)$	points of the algebraic set U with their coordinates in K
$qfdiag(E)$	set of quantifier-free $\mathcal{L}(E)$-sentences which hold in some $\mathcal{L}$-structure containing E
$qftp$	quantifier-free type
tp_{ACF}	type in the reduct to the language of fields $\{+, -, \cdot, 0, 1\}$
$tr.deg$	transcendence degree
dim	dimension of an algebraic set
$\perp$	orthogonal
$Tor(A)$	torsion points of the group A
$Tor_{p'}(A)$	torsion points of the group A of order prime to p
□□□	The text enclosed by these symbols is meant as comments for those with a working knowledge of stability theory

§1. Definitions, preliminary results.

1.1. **Definition**. A *difference field* is a field K with a distinguished endomorphism σ. An *inversive difference field* is a difference field where the endomorphism is onto (and therefore an automorphism). Given a difference field K, there is a "smallest" inversive difference field extending K, which is unique up to K-isomorphism. Therefore we will adopt the following

CONVENTION: In what follows, all difference fields will be assumed to be inversive

Consider the language $\mathcal{L} = \{+, -, \cdot, 0, 1, \sigma\}$, where $+, -, \cdot$ are binary operations, $0, 1$ are constants and σ is a unary function symbol. Then every difference field is naturally an $\mathcal{L}$-structure. Inclusion of difference fields corresponds to inclusion of $\mathcal{L}$-structures, and similarly for morphisms of difference fields. A good reference for basic results on difference fields is R.M. Cohn's book, Difference algebra [1].

1.2. **Difference polynomials, difference equations**. Let (K, σ) be a difference field, and $\bar{X} = (X_1, \dots, X_n)$ a tuple of indeterminates. The difference polynomial ring in $\bar{X}$ over K, denoted $K[\bar{X}]_\sigma$, is defined as follows:

As a ring, $K[\bar{X}]_\sigma$ is simply the polynomial ring in the indeterminates $X_1, \dots, X_n$, $X_1^\sigma, \dots, X_n^\sigma, \dots, X_1^{\sigma^m}, \dots$.

The action of σ on $K[\bar{X}]_\sigma$ is the one suggested by the names of the indeterminates. Then $K[\bar{X}]_\sigma$ is also an $\mathcal{L}$-structure.

Remarks. (1) A *difference ring* is a ring with a distinguished injective endomorphism. So, $K[\bar{X}]_\sigma$ is a difference ring.

(2) This map σ is injective, but is not surjective. One could instead take $K[X_j^{\sigma^i}]_{j=1,\dots,n, i\in\mathbb{Z}}$.

The elements of $K[\bar{X}]_\sigma$ are called *difference polynomials*. If $f(\bar{X}) \in K[\bar{X}]_\sigma$, then $f(\bar{X}) = 0$ is called a *σ-equation*, and the set $\{\bar{a} \in K^n \mid f(\bar{a}) = 0\}$ is called a *σ-closed set*.

1.3. **Definitions**. (1) Let T be a theory, M a model of T. Then M is *existentially closed* (among models of T) if whenever N is a model of T containing M, then every existential sentence with parameters in M which is satisfied in N is already satisfied in M.

(2) A *generic difference field* is a difference field K such that every finite system of σ-equations (over K) which has a solution in some difference field extending K, has already a solution in K.

1.4. **Exercise 1**. Show that if K is a generic difference field, then K is an existentially closed difference field. [Hint: recall that in a field $x \neq 0 \iff \exists y\, xy = 1$].

1.5. Our first goal is to show that the generic difference fields form an elementary class (with axiomatization called ACFA). We will then study some easy properties of this theory. We first need however to recall some definitions of basic algebraic geometry and of field theory. Proofs and details can be found in S. Lang's book, Introduction to algebraic geometry [2].

1.6. **Algebraic sets, varieties, etc.**. Here and in what follows we fix a large algebraically closed field Ω. All fields considered will be subfields of Ω. If K is a subfield of Ω, we denote by K^{alg} the algebraic closure of K, i.e., the set of elements of Ω which are algebraic over K. We first define affine algebraic sets.

Affine n-space, $\mathbb{A}^n(\Omega)$, is simply Ω^n (for $n \in \mathbb{N}$). An *algebraic subset* of Ω^n is a subset defined by polynomial equations $f_1(\bar{X}) = \cdots = f_m(\bar{X}) = 0$, where the $f_i(\bar{X})$ are polynomials in $\bar{X} = (X_1, \ldots, X_n)$, with coefficients in Ω.

These sets are also called *Zariski closed*. The Zariski closed subsets of Ω^n generate a topology on Ω^n, called the *Zariski topology*. This topology is Noetherian (the ascending chain condition on ideals of $\Omega[\bar{X}]$ implies the descending chain condition on Zariski closed sets).

1.7. Let V be an algebraic set. We define

$$I(V) = \{f(\bar{X}) \in \Omega[\bar{X}] \mid f(\bar{a}) = 0 \text{ for all } \bar{a} \in V\}.$$

The coordinate ring of V, $\Omega[V]$, is defined to be $\Omega[\bar{X}]/I(V)$.

We say that V is *defined over the subfield* K of Ω, if $I(V)$ is generated by $I(V) \cap K[\bar{X}]$. In this case we can also form the coordinate ring of V over K, $K[V] = K[\bar{X}]/I(V) \cap K[\bar{X}]$.

A closed subset V of Ω^n is *irreducible* if whenever $V = V_1 \cup V_2$ with V_1, V_2 closed subsets of Ω^n, then $V = V_1$ or $V = V_2$. An irreducible closed set is also called a *variety*.

If V is a variety, we define the field of rational functions of V to be the field of fractions of $\Omega[V]$; we denote it by $\Omega(V)$.

Because the Zariski topology is Noetherian, it follows that every algebraic set V can be written (uniquely up to permutation) as

$$V = V_1 \cup \cdots \cup V_m$$

for some m and varieties $V_1, \ldots, V_m$ such that $V_i \not\subseteq V_j$ for $i \neq j$. The V_i are called the *irreducible components* of V.

1.8. **Some classical results**.

1 - An (affine) algebraic set V is a variety if and only $I(V)$ is prime.

2 - If $V \subseteq W$ are algebraic sets, then $I(V) \supseteq I(W)$.

3 - (Nullstellensatz) Let I be an ideal of $\Omega[\bar{X}]$, and let $V(I) = \{\bar{a} \in \Omega^n \mid f(\bar{a}) = 0 \text{ for all } f(\bar{X}) \in I\}$. Then

$$V(I) \neq \emptyset \iff I \neq (1).$$

4 - If $I \subseteq J$ are ideals in $\Omega[\bar{X}]$ then $V(I) \supseteq V(J)$.

5 - If I is a radical ideal of $\Omega[\bar{X}]$ (i.e., $a^n \in I$ implies $a \in I$), then $I(V(I)) = I$.

6 - If V is an algebraic subset of Ω^n then $V(I(V)) = V$.

7 - If $V_1, \ldots, V_m$ are the irreducible components of V, then $I(V_1), \ldots, I(V_m)$ are the minimal prime ideals containing $I(V)$, and $I(V) = \bigcap_{i=1,\ldots,m} I(V_i)$.

1.9. **Remarks**. (1) If K is a subfield of Ω, one can also define the notion of K-irreducible subsets of Ω^n: an algebraic set V is K-irreducible if it is defined over K and cannot be written as the union of two proper algebraic subsets which are defined over K. This corresponds to the ideal $I(V) \cap K[\bar{X}]$ being prime.

(2) One can show that if the algebraic set V is defined over K, then V is a variety if and only if V is K^{alg}-irreducible (if and only if $I(V) \cap K[\bar{X}]$ generates a prime ideal in $K^{alg}[\bar{X}]$).

(3) It may be that an algebraic set is defined by polynomial equations with their coefficients in K, but is not defined over K. This can happen in positive characteristic. Indeed, assume that K is a field of characteristic $p > 0$, and that $a \in K$ does not have a p-th root in K. Then the set $V = \{a^{1/p}\}$ is defined by the equation $X^p - a = 0$ (with coefficients in K), but $I(V)$ is generated by $X - a^{1/p}$, and V is therefore not defined over K as $a^{1/p} \notin K$.

(4) If V is an algebraic set, there is a smallest field K over which V is defined, and this field is called the *field of definition* of V. If V is defined by polynomial equations with coefficients in K, then the field of definition of V is contained in

— K if $char(K) = 0$,

— the perfect hull of K (= closure of K under p-th roots) if $char(K) = p > 0$.

[Recall that in characteristic $p > 0$, the Frobenius map $x \mapsto x^p$ defines an injective endomorphism of the field K, as $(x + y)^p = x^p + y^p$. Hence, $K^{1/p^n} = \{a \in \Omega \mid a^{p^n} \in K\}$ is a subfield of Ω, and so is the perfect hull K^{1/p^∞} of K: $K^{1/p^\infty} = \bigcup_{n\in\mathbb{N}} K^{1/p^n}$.]

1.10. **Dimension, generics**. Let $V \subseteq \Omega^n$ be a variety defined over K. We define the *dimension of* V, $dim(V)$, to be $tr.deg(\Omega[V]/\Omega)$. Note that if $V \subseteq \Omega^n$, then $dim(V) \leq n$. The tuple $\bar{a} = (a_1, \ldots, a_n)$ is a *generic of* V *over* K if the K-morphism $K[\bar{X}] \to K[\bar{a}]$ which sends X_i to a_i for $i = 1, \ldots, n$, has kernel $I(V) \cap K[\bar{X}]$.

If V is an algebraic set, then $dim(V)$ is the maximum of the dimensions of the irreducible components of V.

Remark. If V is K-irreducible, then the irreducible components of V are conjugate under $Aut(K^{alg}/K)$, and therefore have the same dimension. Thus one can also define $dim(V)$ as $tr.deg(K[V]/K)$, and define a notion of generic over K.

1.11. **Locus of a point**. Let K be a subfield of Ω, and $\bar{a} = (a_1, \ldots, a_n)$. Define

$$I(\bar{a}/K) = \{f(\bar{X}) \in K[\bar{X}] \mid f(\bar{a}) = 0\},$$

where $X = (X_1, \ldots, X_n)$. Then $I(\bar{a}/K)$ is a prime ideal of $K[\bar{X}]$. The set V of points of Ω^n at which all elements of $I(\bar{a}/K)$ vanish, is therefore K-irreducible, and is called the *locus* of $\bar{a}$ over K. Then

— $\bar{a}$ is a generic of V over K,

— Let $\bar{b} \in \Omega^n$. Then $\bar{b} \in V \iff I(\bar{b}/K) \supseteq I(\bar{a}/K)$.

— Assume that $\bar{b} = (b_1, \ldots, b_n) \in V$. Then there is a unique K-morphism $\varphi : K[\bar{a}] \to K[\bar{b}]$ which sends a_i to b_i for $i = 1, \ldots, n$. This morphism is an isomorphism if and only if $\bar{b}$ is a generic of V.

— Let V_1 be an irreducible component of V, let $L = K(\bar{a}) \cap K^{alg}$, and let $\hat{L}$ be the normal closure of L over K (= the field generated by all conjugates of L under the action of $Aut(K^{alg}/K)$). Then the set $\{V_1^\tau \mid \tau \in Aut(\hat{L}/K)\}$ is precisely the set of irreducible components of V.

Remark - warning. If the characteristic is $p > 0$, the locus V of $\bar{a}$ over K is not necessarily *defined over* K. One has: V is defined over K if and only if $K(\bar{a})$ is a *separable extension of* K, i.e.: $K(\bar{a})$ and $K^{1/p}$ are linearly disjoint over K.

1.12. **Morphisms**.

Let $V \subseteq \Omega^n$, $W \subseteq \Omega^m$ be algebraic sets. Let us write $\Omega[V] = \Omega[\bar{x}]$, where $\bar{x} = (x_1, \dots, x_n)$, and each x_i is the image of X_i in $\Omega[V]$.

One can think of an element of $\Omega[V]$ as a function $V \to \Omega$. Indeed, clearly an element $f(\bar{X})$ of $\Omega[\bar{X}]$ defines a function : $\Omega^n \to \Omega$. This function restricts to a function $\hat{f}$ defined on V. One then has: $\hat{f} = \hat{g}$ if and only if $f - g$ vanishes on V, if and only if $f - g \in I(V)$.

A *morphism* $f : V \to W$ is given by a tuple $(f_1(\bar{x}), \dots, f_m(\bar{x}))$ of elements of $\Omega[V]$, such that for all $\bar{a} \in V$ one has $(f_1(\bar{a}), \dots, f_m(\bar{a})) \in W$. Note that it suffices to check this for generics of the irreducible components of V.

Given $f : V \to W$ as above, we obtain a dual morphism of Ω-algebras $f^* : \Omega[W] \to \Omega[V]$, given by $f^*(g) = g \circ f$, i.e., $f^*(g)(\bar{x}) = g(f_1(\bar{x}), \dots, f_m(\bar{x})) \in \Omega[V]$.

Assume that f, V and W are all defined over K, and let $\bar{a}$ be a generic of V over K. One has that f^* is injective if and only if $f(V)$ is Zariski dense in W, if and only $f(\bar{a})$ is a generic of W over K. (The proof is an exercise). In this case, one says that f is *generically onto*.

§2. The theory ACFA. Notation is as in the previous chapter.

2.1. Consider the theory, called ACFA, whose models are the $\mathcal{L}$-structures K satisfying:

(1) K is an algebraically closed field.
(2) σ is an automorphism of K.
(3) If U and V are varieties defined over K, with $V \subseteq U \times U^\sigma$, such that the projections of V to U and to U^σ are generically onto, then there is a tuple $\bar{a}$ in K such that $(\bar{a}, \sigma(\bar{a})) \in V$.

Explanation of the notation

— σ extends to an automorphism of $K[\bar{X}]$ which leaves the elements of $\bar{X}$ fixed. Then $U^\sigma = V(\sigma(I(U))$, i.e., $U^\sigma \cap K^n = \sigma(U \cap K^n)$.

— The projection maps are induced by $\pi_1 : U \times U^\sigma \to U$ and $\pi_2 : U \times U^\sigma \to U^\sigma$. Our hypothesis simply says that $\pi_1(V)$ is Zariski dense in U, and $\pi_2(V)$ is Zariski dense in U^σ. Equivalently, if whenever $(\bar{a}, \bar{b})$ is a generic of V over K, then $\bar{a}$ is a generic of U over K, and $\bar{b}$ a generic of U^σ over K.

Why (3) is first-order.

Write $I(U) = (f_1(\bar{X}), \dots, f_m(\bar{X}))$, and $I(V) = (g_1(\bar{X}, \bar{Y}), \dots, g_s(\bar{X}, \bar{Y}))$. Choose a tuple $\bar{u}$, and polynomials $F_i(\bar{U}, \bar{X}) \in \mathbb{Z}[\bar{U}, \bar{X}]$, $G_j(\bar{U}, \bar{X}, \bar{Y}) \in \mathbb{Z}[\bar{U}, \bar{X}, \bar{Y}]$, such that $f_i(\bar{X}) = F_i(\bar{u}, \bar{X})$ for $i = 1, \dots, m$ and $g_j(\bar{X}) = G_j(\bar{u}, \bar{X}, \bar{Y})$ for $j = 1, \dots, s$.

Fact: The following properties of the tuple $\bar{u}$ are expressible by a first-order formula:

— $F_1(\bar{u}, \bar{X}), \dots, F_m(\bar{u}, \bar{X})$ generate a prime ideal I in $K[\bar{X}]$,

— $G_1(\bar{u}, \bar{X}, \bar{Y}), \ldots, G_s(\bar{u}, \bar{X}, \bar{Y})$ generate a prime ideal J in $K[\bar{X}, \bar{Y}]$, which intersects $K[\bar{X}]$ in I.

The second property tells us that the dual of the projection map gives an inclusion $K[\bar{X}]/I \subseteq K[\bar{X}, \bar{Y}]/J$, which exactly says that $V(J)$ projects generically onto $V(I)$. From the fact, we deduce that each instance of axiom (3) is elementary. (Note that (3) is in fact a scheme of axioms: one for each triple (n, m, d), where n is an upper bound on the number of variables of U, m an upper bound on the number of polynomials defining the varieties U and V, and d an upper bound on the degree of these polynomials.)

Remarks. The above fact holds for an arbitrary field K, and the formulas expressing the required properties of the tuple $\bar{u}$ do not depend on the field K. For a proof, see e.g. the paper by Van den Dries and Schmidt [13]. In this paper there are other very nice (and useful) definability results for ideals in polynomial rings over fields. E.g., define uniformly the minimal prime ideals containing an ideal I, which when dualised, corresponds to finding the K-irreducible components of an algebraic set.

Recall that every formula of the field language is equivalent modulo the theory of algebraically closed fields, to a quantifier-free formula. Hence for instance the property of $\bar{u}$, that $F_1(\bar{u}, \bar{X}), \ldots, F_m(\bar{u}, \bar{X})$ generate a prime ideal in $K^{alg}[\bar{X}]$, is an elementary property of the tuple $\bar{u}$ in K.

2.2. **Theorem**. Every difference field embeds in a model of ACFA. The models of ACFA are exactly the generic difference fields.

Proof. Let (K, σ) be a difference field. Then σ lifts to an automorphism of K^{alg}, and so axioms (1) and (2) are no problem. So, let K be an algebraically closed difference field, let U and V be varieties satisfying the hypotheses of (3). We want to find a difference field L extending K, and containing a tuple $\bar{a}$ with $(\bar{a}, \sigma(\bar{a})) \in V$.

Let $(\bar{a}, \bar{b})$ be a generic of V over K (recall, we work in Ω). Then $\bar{a}$ is a generic of U over K, and $\bar{b}$ is a generic of U^σ over K. This exactly says that $I(\bar{b}/K) = \sigma(I(\bar{a}/K))$, so that σ extends uniquely to a morphism $\tau : K(\bar{a}) \to K(\bar{b})$ sending $\bar{a}$ to $\bar{b}$. Let $L = K(\bar{a}, \bar{b})^{alg}$. By properties of algebraically closed fields, τ lifts to an automorphism ρ of L. Hence (L, ρ) is a difference field extending (K, σ) and contains a solution to our equation.

A standard chain argument now shows that every difference field embeds in a model of ACFA (Exercise). We now need to show that the models of ACFA are generic. Let K be a model of ACFA, $f_1(\bar{X}), \ldots, f_m(\bar{X}) \in K[\bar{X}]_\sigma$, and assume that there is a difference field L containing K, and a tuple $\bar{a}$ in L such that $f_1(\bar{a}) = \cdots = f_m(\bar{a}) = 0$. We want to show that there is such an $\bar{a}$ in K.

Let $\ell \in \mathbb{N}$ be such that $f_1(\bar{X}), \ldots, f_m(\bar{X}) \in K[\bar{X}, \ldots, \sigma^\ell(\bar{X})]$. Consider the varieties

— U with generic over K the tuple $\bar{b} = (\bar{a}, \sigma(\bar{a}), \ldots, \sigma^{\ell-1}(\bar{a}))$,

— V with generic over K the tuple $(\bar{b}, \sigma(\bar{b}))$.

Then $\sigma(\bar{b}) = (\sigma(\bar{a}), \ldots, \sigma^\ell(\bar{a}))$ is a generic of U^σ. Thus $V \subseteq U \times U^\sigma$, and projects generically onto U and onto U^σ. By axiom (3), there is $\bar{c} \in K^{n\ell}$ such that $(\bar{c}, \sigma(\bar{c})) \in V$. Then $\bar{c}$ can be written $(\bar{d}, \sigma(\bar{d}), \ldots, \sigma^{\ell-1}(\bar{d}))$. Since

$I(\bar{c}, \sigma(\bar{c})/K)$ contains $I(\bar{b}, \sigma(\bar{b})/K)$, we get that $I(\bar{d}, \sigma(\bar{d}), \dots, \sigma^\ell(\bar{d})/K)$ contains $I(\bar{a}, \sigma(\bar{a}), \dots, \sigma^\ell(\bar{a})/K)$, and therefore that $f_1(\bar{d}) = \cdots = f_m(\bar{d}) = 0$.

2.3. **Corollaries**. (1) ACFA is *model complete*, i.e., if $K_1 \subseteq K_2$ are models of ACFA, then $K_1 \prec K_2$.

(2) Every formula is equivalent, modulo ACFA, to an existential formula.

2.4. **Exercise 2**. Show that if all models of a theory T are existentially closed (among models of T), then T is model complete. [Hint of proof: show first that if $A \subseteq B$ and A is existentially closed in B, then there is an elementary extension C of A containing B. Let now $A \subseteq B$ be models of T. Using the first step, construct elementary chains $(A_i)_{i\in\omega}$ and $(B_i)_{i\in\omega}$, with $A_0 = A$, $B_0 = B$, and $A_i \subseteq B_i \subseteq A_{i+1} \subseteq B_{i+1}$. Then $\bigcup_i A_i = \bigcup_i B_i$ is an elementary extension of both A and B.]

2.5. **Definition**. Let $E \subseteq K_1, K_2$ be subfields of Ω. One says that K_1 and K_2 are *algebraically independent over* E, or *free over* E, if for every $n \in \mathbb{N}$, whenever $a_1, \dots, a_n \in K_1$ are algebraically independent over E, then they remain algebraically independent over K_2.

This notion corresponds to independence in the theory of algebraically closed fields, and is a symmetrical notion: K_1 is free from K_2 over E if and only if K_2 is free from K_1 over E (see Lang's book [2]). It is also transitive: if $K_2 \subseteq K_3$, then K_1 and K_3 are free over E if and only if K_1 and K_2 are free over E, and K_1K_2 and K_3 are free over E.

2.6. **Definition**. Let $E \subseteq K_1, K_2$ be subfields of Ω. One says that K_1 and K_2 are *linearly disjoint over* E if for every $n \in \mathbb{N}$, whenever $a_1, \dots, a_n \in K_1$ and $b_1, \dots, b_n \in K_2$ are such that $\sum_{i=1}^n a_i b_i = 0$ and not all b_i's are 0, then there are $c_1, \dots, c_n \in E$ such that $\sum_{i=1}^n a_i c_i = 0$ and not all c_i's are 0.

Recall also that the tensor product $K_1 \otimes_E K_2$ is defined as follows: Fix a basis B_i of the E-vector space K_i, with $1 \in B_i$, $i = 1, 2$. Then, as an E-vector space, $K_1 \otimes_E K_2$ has basis

$$\{a \otimes b \mid a \in B_1,\ b \in B_2\}.$$

If $c = \sum_{a\in B_1} c_a a$ and $d = \sum_{b\in B_2} d_b b$ (with the c_a and d_b in E; all but finitely many of the c_a's and d_b's are 0), then we write $c \otimes d$ for the element $\sum_{a\in B_1, b\in B_2} c_a d_b (a \otimes b)$. Multiplication on the elements of the basis is given by

$$(a \otimes b) \cdot (c \otimes d) = (ac) \otimes (bd),$$

and extended by linearity to the whole space. Note that K_1 and K_2 embed in $K_1 \otimes_E K_2$, via $a \mapsto a \otimes 1$ and $b \mapsto 1 \otimes b$. If $e \in E$, $a \in K_1$ and $b \in K_2$, then we have $ae \otimes b = e(a \otimes b) = a \otimes eb$.

Fact. K_1 and K_2 are linearly disjoint over E if and only if $K_1 \otimes_E K_2$ is a domain, equal to $K_1[K_2]$, the subring of Ω generated by K_1 and K_2.

For details and proofs, see Lang's book [2]. The proof of the fact is not difficult. One should note that linear disjointness is a symmetrical notion, and implies algebraic independence. It is also transitive. Here are some special cases:

— If E is an algebraically closed field, then K_1 and K_2 are algebraically independent over E if and only if they are linearly disjoint over E.

— If one of K_1 or K_2 is a Galois extension of E, then K_1 and K_2 are linearly disjoint over E if and only if $K_1 \cap K_2 = E$.

2.7. If E is a subset of K, one denotes by $\mathcal{L}(E)$ the language obtained by adjoining to $\mathcal{L}$ constant symbols for the elements of E. Then K expands naturally to an $\mathcal{L}(E)$-structure, by interpreting the constant symbol corresponding to $e \in E$ by the element e itself. The set of quantifier-free $\mathcal{L}(E)$-sentences true in K is denoted by $qfdiag(E)$, and it describes the isomorphism type of the $\mathcal{L}$-substructure of K generated by E. So, a model of $qfdiag(E)$ will be an $\mathcal{L}$-structure containing an isomorphic copy of the $\mathcal{L}$-substructure of K generated by E. Elementary equivalence in the language $\mathcal{L}(E)$ is denoted by $\equiv_E$.

Theorem. Let K_1 and K_2 be models of ACFA, containing a common algebraically closed difference subfield E. Then $K_1 \equiv_E K_2$.

Proof. To avoid confusion we will denote by σ_i the automorphism of K_i that we are considering.

Step 1. Choose an E-isomorphic copy K_2' of the field K_2 (by an E-isomorphism φ), which is free from K_1 over E, and let $\sigma_2' = \varphi\sigma_2\varphi^{-1}$. Because E is algebraically closed, K_1 and K_2' are then linearly disjoint over E. Then the difference fields (K_2, σ_2) and (K_2', σ_2') are E-isomorphic via φ, and therefore elementarily equivalent over E. Hence, replacing K_2 by K_2', we may assume that K_1 and K_2 are linearly disjoint over E.

Step 2. We will now show that σ_1 and σ_2 have a common extension to K_1K_2 (the subfield of Ω generated by K_1 and K_2). We first define $\tau(a \otimes b) = \sigma_1(a) \otimes \sigma_2(b)$ for $a \in K_1$, and $b \in K_2$. Since σ_1 and σ_2 agree on E, and K_1 and K_2 are linearly disjoint over E, this is well-defined. This extends (by linearity) to $K_1 \otimes_E K_2$, which we identify with $K_1[K_2]$, and we then extend τ to the field of fractions of $K_1[K_2]$, i.e., to K_1K_2.

Step 3. The difference field (K_1K_2, τ) embeds in a model L of ACFA. Because ACFA is model complete (Corollary 2.3(1)) we then have $K_i \prec L$ for $i = 1, 2$, which implies that K_1 and K_2 satisfy the same $\mathcal{L}(E)$-sentences, and shows the result.

2.8. **Corollary**. Let E be an algebraically closed difference field. Then ACFA$\cup qfdiag(E)$ is complete.

Proof. If K_1 and K_2 are models of ACFA$\cup qfdiag(E)$, then K_1 and K_2 contain difference subfields E_1 and E_2 respectively, which are isomorphic to E. Moving K_2 by an isomorphism, we may assume that $E_1 = E_2$. The result then follows by Theorem 2.7.

2.9. **Corollary**. The completions of ACFA are obtained by adjoining to ACFA a description of the isomorphism type of the difference field consisting of elements algebraic over the prime field.

Proof. If $T = Th(K)$ is a complete theory containing ACFA, then T will specify the characteristic, and therefore the isomorphism type of the prime field k. Note that the elements of k are in fact (interpretations of) terms of the language $\mathcal{L}$. Let L be a finite Galois extension of k of degree n over k, α a generator of L over k, and $p(X) \in k[X]$ its minimal (monic) polynomial. Since L is Galois over

k, and k is fixed by σ, $\sigma(L)$ will contain all the roots of $p(X)$, and therefore will equal L. Hence, $\sigma(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i$ for some elements $a_i \in k$. The sentence

$$\exists x\ p(x) = 0 \wedge \sigma(x) = \sum_{i=0}^{n-1} a_i x^i$$

will therefore belong to T. The set of all such sentences will describe the isomorphism type of the difference subfield k^{alg} of K.

The converse follows from Theorem 2.7.

2.10. **Notation**. If A is a subset of an algebraically closed difference field K, we denote by $cl_\sigma(A)$, the difference field generated by A, and by $acl_\sigma(A)$ the smallest algebraically closed difference field containing A. Note that $cl_\sigma(A)$ is the field generated by the sets $\sigma^i(A), i \in \mathbb{Z}$, and that $acl_\sigma(A)$ is simply the algebraic (field-theoretic) closure of $cl_\sigma(A)$.

Recall that the model-theoretic definable and algebraic closure are defined as follows: let M be a model of a theory, and $A \subset M$. The *definable closure* of A in M, denoted $dcl(A)$, is the set of elements $a \in M$, such that there is some formula $\varphi(x) \in \mathcal{L}(A)$, which is satisfied by a in M and by no other element of M. We will then say that the formula $\varphi(x)$ defines a. So, $dcl(A)$ will in particular contain all elements of the substructure of M generated by A. The *algebraic closure* of A in M, denoted $acl(A)$, is the set of elements $a \in M$ which satisfy some $\mathcal{L}(A)$-formula which is satisfied by only finitely many elements of M.

Clearly $dcl(A) \subseteq acl(A)$, and $A \subseteq B$ implies $dcl(A) \subseteq dcl(B)$ and $acl(A) \subseteq acl(B)$. Moreover, one can show that $acl(acl(A)) = acl(A)$ (and of course $dcl(dcl(A)) = dcl(A)$). In the particular case of difference fields, clearly $cl(A) \supseteq cl_\sigma(A)$, and $acl(A) \supseteq acl_\sigma(A)$.

2.11. **Corollary**. Let (K_1, σ_1) and (K_2, σ_2) be models of ACFA, containing a common difference subfield (E, σ). Then

$$K_1 \equiv_E K_2 \iff (E^{alg}, \sigma_1|_{E^{alg}}) \simeq_E (E^{alg}, \sigma_2|_{E^{alg}}).$$

Proof. The left to right implication is clear, as elements of E^{alg} are algebraic over E. For the converse, let $\varphi : E^{alg} \to E^{alg}$ be an E-isomorphism such that $\varphi\sigma_1 = \sigma_2\varphi$. Extend φ to an automorphism ψ of Ω, and let $(K_1', \sigma_1') = (\psi(K_1), \psi\sigma_1\psi^{-1})$ be the difference field image of K_1 by ψ. Then $K_1 \equiv_E K_1'$, and σ_1' and σ_2 agree on E^{alg}. So we may apply 2.7

2.12. **Corollary**. Let $\varphi(\bar{x})$ be a formula. Then, modulo ACFA, $\varphi(\bar{x})$ is equivalent to a disjunction of formulas of the form $\exists y\ \psi(\bar{x}, y)$, where $\psi(\bar{x}, y)$ is quantifier-free, and for every difference field K and $(\bar{a}, b)$ in K satisfying ψ, we have that b is algebraic over $(\bar{a}, \sigma(\bar{a}), \dots)$.

2.13. **Exercise 3**. Give a proof of 2.12. [Hint: First note that if E is a separably closed difference field, then $qfdiag(E) \vdash qfdiag(E^{alg})$ modulo the theory of difference fields. Then, for every model K of ACFA, and tuple $\bar{a}$ satisfying φ, find a formula ψ_a implying φ and of the required form. Use compactness to conclude.]

2.14. **Definition of types and saturated models**. Let M be an $\mathcal{L}$-structure, A a subset of M, and $\bar{a}$ an n-tuple of elements of M. The *type of* $\bar{a}$ *over* A *in* M, denoted $tp(\bar{a}/A)$ or sometimes $tp_M(\bar{a}/A)$, is the set of $\mathcal{L}(A)$-formulas $\varphi(\bar{x})$ satisfied by $\bar{a}$ in M, where $\bar{x}$ is a fixed n-tuple of variables. A *partial* n*-type over* A is a set $\Gamma(\bar{x})$ of $\mathcal{L}(A)$-formulas in the variables $\bar{x}$, such that every finite conjunction of elements of $\Gamma(\bar{x})$ is satisfiable by some n-tuple of M. By compactness, a partial n-type over A will be realised in some elementary extension M^* of M, i.e., M^* will contain some tuple $\bar{a}$ which satisfies all formulas of $\Gamma(\bar{x})$.

If κ is an infinite cardinal, an $\mathcal{L}$-structure M is κ*-saturated* if for every $A \subseteq M$ with $|A| < \kappa$, every (partial) type over A is realised in M. The structure M is saturated iff it is $|M|$-saturated. Saturated models are quite useful, as they realise many types and have many automorphisms: if M is saturated and $f : A \to B$ is an elementary map between two subsets of M of size $< |M|$, then f extends to an automorphism of M.

2.15. **Corollary**. Let E be a difference subfield of a model K of ACFA, and let $\bar{a}$ and $\bar{b}$ be tuples in K of the same length. Then $tp(\bar{a}/E) = tp(\bar{b}/E)$ if and only if there is an E-isomorphism (of difference fields) $acl_\sigma(E\bar{a}) \to acl_\sigma(E\bar{b})$ sending $\bar{a}$ to $\bar{b}$.

Proof. Extend the E-isomorphism $acl_\sigma(E\bar{a}) \to acl_\sigma(E\bar{b})$ to an E-isomorphism $\varphi : K \to K_1$ (for some difference field K_1). Then $tp_K(\bar{a}/E) = tp_{K_1}(\bar{b}/E)$ (since $\varphi(\bar{a}) = \bar{b}$). By Theorem 2.7, $K_1 \equiv_{acl_\sigma(E\bar{b})} K$, which implies that $tp(\bar{a}/E) = tp(\bar{b}/E)$.

2.16. **Corollary**. Let K be a model of ACFA, and A a subset of K. Then $acl_\sigma(A)$ equals the model-theoretic algebraic closure of A, $acl(A)$.

Proof. Clearly $acl_\sigma(A) \subseteq acl(A)$. Choose an $acl_\sigma(A)$-isomorphic copy K_1 of K, which is linearly disjoint from K over $acl_\sigma(A)$. As in 2.7, KK_1 embeds in a model L of ACFA. By 2.15, if $a \in K \setminus acl_\sigma(A)$, then there is $b \in K_1 \setminus acl_\sigma(A)$ realising the same type over $acl_\sigma(A)$ as a. Hence no type realised in $K \setminus acl_\sigma(A)$ is algebraic.

2.17. **Saturated models of ACFA**. Let K be a saturated model of ACFA. Then K has the following property: if E is an algebraically closed difference subfield of K, and F is a difference field extending E, and with $|F| < |K|$, then there is an E-embedding of F into E.

Thus saturated models of ACFA, of large enough cardinality, play the role of universal models of algebraic geometry.

§3. σ-closed sets, independence and SU-rank. We keep the notation and conventions introduced before. We work in a (sufficiently saturated) model K of ACFA.

3.1. **σ-closed sets, and the topology it generates**. We work in a (sufficiently saturated) model K of ACFA. In analogy with the Zariski topology, we define the σ-topology on K^n. Given $B \subset K[\bar{X}]_\sigma$, $\bar{X} = (X_1, \ldots, X_n)$, we set

$$V(B) = \{\bar{a} \in K^n \mid f(\bar{a}) = 0 \text{ for all } f(\bar{X}) \in B\}.$$

Dually, if $S \subseteq K^n$, we define

$$I_\sigma(S) = \{f(\bar{X}) \in K[\bar{X}]_\sigma \mid f(\bar{a}) = 0 \text{ for all } \bar{a} \in S\}.$$

If E is a difference subfield of K and $\bar{a} \in K^n$, we define

$$I_\sigma(\bar{a}/E) = \{f(\bar{X}) \in E[\bar{X}]_\sigma \mid f(\bar{a}) = 0\}.$$

We call the sets of the form $V(B)$ the σ-closed subsets of K^n. One checks easily that $V(I_\sigma(B)) = B$. Some of the following results are theorems (see Cohn's book):

Facts and remarks. Note that $I_\sigma(S)$ is an ideal I of $K[\bar{X}]$ with the following properties:

(i) $f \in I \iff \sigma(f) \in I$.
(ii) If $f^m\sigma(f)^n \in I$, then $f \in I$.

Ideals satisfying (i) are called *reflexive σ-ideals* (and σ will then induce an injective endomorphism on the quotient of $K[\bar{X}]$ by such an ideal). Ideals satisfying in addition condition (ii) are called *perfect* σ-ideals. Prime ideals satisfying (i) and (ii) are called *prime σ-ideals*. Perfect σ-ideals are the analogues of radical ideals, and are intersections of prime σ-ideals.

3.2. **Fact**. Even though $K[\bar{X}]_\sigma$ does not satisfy the a.c.c. on σ-ideals, it satisfies it on perfect σ-ideals, and this implies that the σ-topology on K^n is Noetherian.

3.3. **Exercise 4**. Show that if I is a prime σ-ideal then $I_\sigma(V(I)) = I$. [Warning: your proof should use the fact that K is a model of ACFA. You may use the fact that a field with a distinguished endomorphism embeds in an inversive difference field].

3.4. **Definition**. Let E be a difference subfield of K, and $a \in K$. We say that a is *transformally transcendental* over E if $I_\sigma(a/E) = 0$. Otherwise, we say that a is *transformally algebraic over E*. A tuple is *transformally algebraic* over E if all its elements are.

If a is transformally transcendental over E, then the elements $\sigma(a), i \in \mathbb{N}$, are algebraically independent over E. Hence, applying σ^{-1}, so are the elements $\sigma(a), i \in \mathbb{Z}$. Thus, the difference field generated by a over E is isomorphic to $E(X^{\sigma^i} \mid i \in \mathbb{Z})$ (with the obvious action of σ).

Similarly, one says that n-tuple $\bar{a}$ is it *transformally independent* over E, if $I_\sigma(\bar{a}/E) = (0)$. There are notions of *transformal transcendental bases*, *transformal transcendental degree* of an extension, etc.

Assume now that a is transformally algebraic over E, and let m be least such that some $f(X) = F(X, X^\sigma, \ldots, X^{\sigma^m}) \in I_\sigma(a/E)$. Choose such an $f(X)$ of lowest degree when viewed as a polynomial in X^{σ^m}. Then $F(a, \ldots, \sigma^{m-1}(a), Y)$ is irreducible over $E(a, \ldots, \sigma^{m-1}(a))$ because $I_\sigma(a/E) \cap E[X, \ldots, X^{\sigma^m}]$ is prime, and is the minimal polynomial of $\sigma^m(a)$ over $E(a, \ldots, \sigma^{m-1}(a))$.

From $F(a, \ldots, \sigma^m(a)) = 0$, we deduce that $\sigma(F)(\sigma(a), \ldots, \sigma^{m+1}(a)) = 0$, so that the minimal polynomial of $\sigma^{m+1}(a)$ over $E(a, \ldots, \sigma^m(a))$ divides $\sigma(F)(\sigma(a), \ldots, \sigma^m(a), Y)$, and therefore has degree bounded above by the degree of $F(a, \ldots, \sigma^{m-1}(a), Y)$. It follows that $I_\sigma(a/E)$, as a σ-ideal, is finitely

generated, since from some point on, the degree of the minimal polynomial of $\sigma^n(a)$ over $E(a, \dots, \sigma^{n-1}(a))$ must stabilize.

Note that we also have that

$$acl_\sigma(Ea) = E(a, \dots, \sigma^{m-1}(a))^{alg}.$$

Similarly, if $\bar{a}$ is transformally algebraic over E, then there is an n such that $acl_\sigma(E\bar{a}) = E(\bar{a}, \dots, \sigma^n(\bar{a}))^{alg}$.

3.5. **Exercise 5**.

(1) Use the preceding remarks to show that every prime σ-ideal of $E[\bar{X}]_\sigma$, is finitely generated (as a σ-ideal).
(2) (harder) Let I be a perfect σ-ideal of $K[\bar{X}]$, $\bar{X} = (X_1, \dots, X_n)$, and assume that $I \cap K[X_i]_\sigma \neq 0$ for all $i = 1, \dots, n$. Show that any descending sequence of σ-closed subsets F_j of $V(I)$ is finite [Hint: Look at the Zariski closures of $\{(\bar{a}, \sigma(\bar{a}), \dots, \sigma^m(\bar{a})) \mid \bar{a} \in F_j\}$ for m large enough, use induction on the dimension of the algebraic sets considered.]
(3) Using (2), show that the σ-topology is Noetherian.

3.6. **Definition**. Let A, B, C be subsets of a model K of ACFA. We say that A and B are *independent over* C if the fields $acl_\sigma(CA)$ and $acl_\sigma(CB)$ are free (or equivalently, linearly disjoint) over $acl_\sigma(C)$. We denote it by $A \downarrow_C B$.

Remarks. Independence is clearly a symmetrical notion, and is transitive, i.e.: let $B' \subset B$. Then

$$A \downarrow_C B \iff A \downarrow_C B' \text{ and } A \downarrow_{C \cup B'} B.$$

Note also that by definition

$$A \downarrow_C B \iff acl_\sigma(C, A) \downarrow_{acl_\sigma(C)} acl_\sigma(C, B)$$

and that

$$acl_\sigma(C, A) = (acl_\sigma(C) acl_\sigma(A))^{alg}.$$

Assume for simplicity, that $C \subseteq B$ are algebraically closed difference fields. Then A and B are independent over C if and only if, for every tuple $\bar{a} \in A$, the ideal $I_\sigma(\bar{a}/B)$ is generated by its intersection with $C[\bar{X}]_\sigma$.

Moreover, independence satisfies the extension property: given A, B and C, there is A' realising $tp(A/C)$ in some elementary extension of K such that A' and B are independent over C. Indeed, without loss of generality, we may assume that C, A and B are algebraically closed difference fields, with $C \subset A \cap B$. Let A' be a C-isomorphic copy of A which is free from B over C. Then A' is linearly disjoint from B over C, reasoning as in Step 2 of Theorem 2.7, we get that there is an elementary extension L of K which contains the difference fields A' and B. Then A' and B are independent over C, and $tp_L(A'/C) = tp_L(A/C)$.

3.7. **Exercise 6**. Let K be a model of ACFA, and A, B, C, D algebraically closed difference subfields of K. Give a proof, or convince yourself, of the following facts:

(1) (Symmetry) If $A \downarrow_C B$ then $B \downarrow_C A$.

(2) (Transitivity). If $C \subseteq A \cap B$ and $B \subseteq D$,
$$A \downarrow_C D \iff A \downarrow_C B \quad \text{and} \quad A \downarrow_B D.$$
(3) $A \downarrow_C B$ if and only if for every finite tuple $\bar{b}$ from B, $A \downarrow_C \bar{b}$.
(4) (Extension) In some elementary extension of K there is A' realising $tp(A/C)$ with $A' \downarrow_C B$. (This was already explained above)
(5) There is a finite subset E of C such that $A \downarrow_E C$.

3.8. **The independence theorem**. Let K be a model of ACFA (sufficiently saturated), let $E = acl_\sigma(E) \subseteq K$, and $\bar{a}$, $\bar{b}$, $\bar{c}_1$ and $\bar{c}_2$ tuples in K, such that

(i) $tp(\bar{c}_1/E) = tp(\bar{c}_2/E)$,
(ii) $\bar{a}$ and $\bar{c}_1$ are independent over E, $\bar{a}$ and $\bar{b}$ are independent over E and $\bar{b}$ and $\bar{c}_2$ are independent over E.

Then there is $\bar{c}$ realising $tp(\bar{c}_1/E \cup \bar{a}) \cup tp(\bar{c}_2/E \cup \bar{b})$, independent from $(\bar{a}, \bar{b})$ over E.

Proof. Let $\bar{c}$ realise $tp(\bar{c}_1/E)$, independent from $(\bar{a}, \bar{b})$ over E. Let $A = acl_\sigma(E\bar{a})$, $B = acl_\sigma(E\bar{b})$, $C = acl_\sigma(E\bar{c})$, and fix E-isomorphisms (of difference fields) $\varphi_1 : acl_\sigma(E\bar{c}_1) \to C$ and $\varphi_2 : acl_\sigma(E\bar{c}_2) \to C$, with $\varphi_i(\bar{c}_i) = \bar{c}$.

Let σ_0 be the restriction of σ to $(AB)^{alg}C$. Since A is linearly disjoint from $acl_\sigma(E, \bar{c}_1)$ and from C over E, we may extend φ_1 to a **field**-isomorphism $\psi_1 : acl_\sigma(A\bar{c}_1) \to (AC)^{alg}$, which is the identity on A. Then $\sigma_1 = \psi_1 \sigma \psi_1^{-1}$ is an automorphism of $(AC)^{alg}$ which agrees with σ on A and on C. Indeed, σ_1 agrees with σ on A because ψ_1 is the identity on A, and on C because ψ_1 extends the difference field isomorphism $\varphi_1 : acl_\sigma(E\bar{c}_1) \to C$. Note also that by definition of σ_1, the isomorphism ψ_1 is an isomorphism between the difference field $(acl_\sigma(A\bar{c}_1), \sigma)$ and the difference field $((AC)^{alg}, \sigma_1)$

Similarly, we may extend φ_2 to a field-isomorphism $\psi_2 : acl_\sigma(B, \bar{c}_2) \to (BC)^{alg}$ which is the identity on B. The automorphism $\sigma_2 = \psi_2 \sigma \psi_2^{-1}$ agrees with σ on B and C.

Assume that there is an automorphism τ of $L = (AB)^{alg}(AC)^{alg}(BC)^{alg}$ which extends σ_0, σ_1 and σ_2. Then we can find some model M of ACFA containing (L, τ). As τ extends σ_0, we then have that $tp_M(AB/E) = tp_K(AB/E)$ (by 2.7). By 2.15, we also have
$$tp_M(\bar{c}/A) = tp_K(\bar{c}_1/A), \quad \text{and} \quad tp_M(\bar{c}/B) = tp_K(\bar{c}_2/B)$$
because τ extends σ_1 and σ_2, and the ψ_i are difference fields isomorphisms fixing A and B respectively. Clearly, $\bar{c}$ is independent from (A, B) over E, and this will have finished the proof.

It remains to show that there is such an automorphism τ of L. To do that, it suffices to show that σ_0 and σ_1 have a common (and necessarily unique) extension τ_1 to $(AB)^{alg}(AC)^{alg}$, and that τ_1 and σ_2 have a common extension to L.

To show that σ_0 and σ_1 have a common extension τ_1 to $(AB)^{alg}(AC)^{alg}$, it is enough to show that their domains are linearly disjoint over their intersection, and that σ_0 and σ_1 agree on this intersection. Similarly for τ_1 and σ_2.

The domain of σ_0 is $(AB)^{alg}C$, the domain of σ_1 is $(AC)^{alg}$, which is a Galois extension of AC. By definition, σ_0 is the restriction of σ ($\in Aut(K)$), and we know that σ_1 and σ agree on AC. It follows that it suffices to show that

$$(AB)^{alg}C \cap (AC)^{alg} = AC. \tag{1}$$

(Here we are using the fact that $(AC)^{alg}$ is a Galois extension of AC to reduce the linear disjointness over AC to intersecting in AC). Similarly, to show that τ_1 and σ_2 have a common extension to L, it will be enough to show that

$$(AB)^{alg}(AC)^{alg} \cap (BC)^{alg} = BC. \tag{2}$$

Unfortunately the proof of either of these equations uses tools slightly beyond the scope of this course, since I had chosen not to assume anything known in stability theory. For sake of completeness I will give the proof using stability results. The reader unfamiliar with stable theories may just skip this part and admit the equations (1) and (2), and therefore the result. Let us prove (2) first. Algebraists would prove it via specialisations, the ideas are essentially the same (but not the way it is said).

Let $\alpha \in (BC)^{alg} \cap (AB)^{alg}(AC)^{alg}$, and write $\alpha = \sum_{i=1}^{n} \beta_i\gamma_i$, where $\beta_i \in (AB)^{alg}$, $\gamma_i \in (AC)^{alg}$. Let $\bar{a}'$, $\bar{b}'$ and $\bar{c}'$ be tuple of elements from A, B and C respectively, and $f_i(\bar{X}, \bar{Y}, U), g_i(\bar{X}, \bar{Z}, V)$ be polynomials over E, such that $f_i(\bar{a}', \bar{b}, U)$ is the minimal polynomial of β_i over AB, and $g_i(\bar{a}', \bar{c}', V)$ is the minimal polynomial of γ_i over AC for $i = 1, \dots, n$. Then

$$K \models \exists u_1, \dots, u_n, v_1, \dots, v_n \bigwedge_i \big(f_i(\bar{a}', \bar{b}', u_i) = 0 \wedge g_i(\bar{a}', \bar{c}', v_i) = 0\big) \wedge \alpha = \sum_i u_i v_i.$$

Note that this is a formula of the field language, satisfied by $(\bar{a}', \bar{b}', \bar{c}', \alpha)$. By assumption, $\bar{a}'$ is independent from $(BC)^{alg}$ over E, in the sense of the theory of algebraically closed fields. Hence every formula represented in $tp_{ACF}(\bar{b}', \bar{c}', \alpha/A)$ is already represented in $tp_{ACF}(\bar{b}', \bar{c}', \alpha/E)$ (here tp_{ACF} denotes the type in the theory of algebraically closed fields). This precisely means that there is a tuple $\bar{e}$ in E such that

$$K \models \exists u_1, \dots, u_n, v_1, \dots, v_n \bigwedge_i \big(f_i(\bar{e}, \bar{b}', u_i) = 0 \wedge g_i(\bar{e}, \bar{c}', v_i) = 0\big) \wedge \alpha = \sum_i u_i v_i.$$

If $\beta_1', \dots, \beta_n', \gamma_1', \dots, \gamma_n'$ satisfy $\bigwedge_i \big(f_i(\bar{e}, \bar{b}', \beta_i') = 0 \wedge g_i(\bar{e}, \bar{c}', \gamma_i') = 0\big) \wedge \alpha = \sum_i \beta_i'\gamma_i'$, then $\beta_i' \in B$ and $\gamma_i' \in C$, which shows that $\alpha \in BC$, and proves (2). Permuting A, B, C, we obtain that $(AC)^{alg} \cap (AB)^{alg}(BC)^{alg} = AC$, from which we get (1).

3.9. □□□ **Corollary**. All completions of ACFA are supersimple, and independence corresponds to non-forking.

Proof. See the paper by Kim and Pillay [15]. They show that if you have an independence notion, which is

(i) symmetric,
(ii) transitive,
(iii) has the extension property,
(iv) is such that, given a finite tuple $\bar{a}$ and a set A, there is $A_0 \subseteq acl^{eq}(A)$ such that $\bar{a}$ and A are independent over A_0, and $|A_0| \leq |\mathcal{L}| + \aleph_0$,
(v) satisfies the independence theorem.

Then this notion of independence coincides with non-forking, and the theory is simple. If in (iv), the set A_0 can always be taken finite, then the theory is supersimple.

In our case, given the complete theory of a model K of ACFA, items (i) – (iii) are immediate because similar statements hold for non-forking in algebraically closed fields, (v) is 3.8. From our definition of independence and the descending chain condition on σ-closed sets (3.2), it follows that in (iv) we can always take A_0 to be finite. □□□

3.10. **Definitions of forking and of the SU-rank**. The SU-rank is a rank on types, based on non-independence in the same way the U-rank is.

Let K be a model of ACFA, sufficiently saturated, $E \subseteq F$ algebraically closed subsets of K, and $\bar{a}$ a tuple of elements, $p = tp(\bar{a}/E)$, $q = tp(\bar{a}/F)$. We say that q *forks* over E, or that q *is a forking extension of* p, iff $\bar{a} \not\downarrow_E F$. Otherwise, we say that q *does not fork over* E, or that q *is a non-forking extension of* p *to* F.

We define $\mathrm{SU}(p) = \mathrm{SU}(\bar{a}/E) \geq \alpha$ by induction on the ordinal α:

— $\mathrm{SU}(p) \geq 0$

— $\mathrm{SU}(p) \geq \alpha + 1$ iff p has a forking extension q such that $\mathrm{SU}(q) \geq \alpha$, iff there is $B = acl_\sigma(B)$ containing E such that $acl_\sigma(E\bar{a})$ and B are not linearly disjoint over $acl_\sigma(E)$, and $SU(\bar{a}/B) \geq \alpha$.

— If α is a limit ordinal, then $\mathrm{SU}(p) \geq \alpha$ iff $\mathrm{SU}(p) \geq \beta$ for all $\beta < \alpha$.

We then define $\mathrm{SU}(p)$ to be the least α such that $\mathrm{SU}(p) \not\geq \alpha + 1$ if it exists, and ∞ otherwise.

3.11. **Exercise 7**. Let $\bar{a}, E \subseteq F, K$ be as above. Give a proof, or convince yourself of the following facts:

(1) $\mathrm{SU}(\bar{a}/F) \leq \mathrm{SU}(\bar{a}/E)$. [Hint: show by induction on α that $\mathrm{SU}(\bar{a}/F) \geq \alpha$ implies $\mathrm{SU}(\bar{a}/E) \geq \alpha$.]
(2) If $\bar{a} \downarrow_E F$, then $\mathrm{SU}(\bar{a}/E) = \mathrm{SU}(\bar{a}/F)$. [Again, use induction on α. The independence theorem intervenes in the proof.]
(3) Deduce from Remark 3.6 and the noetherianity of the σ-topology that $\mathrm{SU}(\bar{a}/E) < \infty$.

3.12. **Remark**. As explained in the exercise, Fact 3.2 yields that the SU-rank of a type (of a finite tuple) exists. It is however much stronger: You could imagine that there could exist an infinite descending sequence of σ-closed sets all defined over $acl_\sigma(\emptyset)$.

3.13. **Natural sum on ordinals**. Every ordinal can be written uniquely as

$$\alpha = \omega^{\alpha_1} a_1 + \cdots + \omega^{\alpha_n} a_n,$$

where $\alpha_1 > \cdots > \alpha_n \geq 0$ are ordinals, and $a_1, \ldots, a_n$ are positive integers. If $\beta = \omega^{\beta_1} b_1 + \cdots + \omega^{\beta_m} b_m$, then we define $\alpha \oplus \beta$ as follows. First, relaxing the condition on $a_1, \ldots, a_n, b_1, \ldots, b_m$ to be positive and allowing them to be 0, we may assume that $m = n$ and $\alpha_i = \beta_i$ for $i = 1, \ldots, n$. Then one sets

$$\alpha \oplus \beta = \omega^{\alpha_1}(a_1 + b_1) + \cdots + \omega^{\alpha_n}(a_n + b_n).$$

One verifies that $\oplus$ is commutative and transitive.

While $\oplus$ coincides with the usual ordinal addition on finite ordinals, it definitely does not on infinite ones. For instance $1 \oplus \omega = \omega \oplus 1 = \omega + 1$, but $1 + \omega = \omega$.

3.14. **Properties of the SU-rank**. One can show that the SU-rank satisfies the so-called Lascar inequality: given another tuple $\bar{b}$,

$$\mathrm{SU}(\bar{a}/E\bar{b}) + \mathrm{SU}(\bar{b}/E) \leq \mathrm{SU}(\bar{a}, \bar{b}/E) \leq \mathrm{SU}(\bar{a}/A\bar{b}) \oplus \mathrm{SU}(\bar{b}/A).$$

This is shown by induction. For the first inequality, one shows that $\mathrm{SU}(\bar{b}/E) \geq \alpha$ implies $\mathrm{SU}(\bar{a}/E\bar{b}) + \alpha \geq \mathrm{SU}(\bar{a}, \bar{b}/E)$. For the second, that $\mathrm{SU}(\bar{a}, \bar{b}/E) \geq \alpha$ implies $\mathrm{SU}(\bar{a}/E\bar{b}) \oplus \mathrm{SU}(\bar{a}/E) \geq \alpha$. The proof is not difficult, but one can also consult e.g. Wagner's book on simple theories [19].

3.15. **SU-rank of definable sets, or of formulas**. Let $S \subseteq K^n$ be a definable set, defined by a formula $\varphi(\bar{x})$ over some E, and assume that K is sufficiently saturated (otherwise our definition will not make sense). We define $\mathrm{SU}(\varphi) = \mathrm{SU}(S) = \sup\{\mathrm{SU}(\bar{a}/A) \mid \bar{a} \in S\}$. One can show that this sup is attained, i.e., that there is some $\bar{a}$ satisfying φ and such that $\mathrm{SU}(\bar{a}/A) = \mathrm{SU}(\varphi)$.

3.16. **Remarks**. Note the following special cases:

$$\mathrm{SU}(\bar{a}/E) = 0 \iff \bar{a} \in acl_\sigma(E)$$
$$\mathrm{SU}(\bar{a}/E) = 1 \iff \bar{a} \notin acl_\sigma(E) \quad \text{and for all } F \supset E,$$
$$\text{either } \bar{a} \text{ is independent from } F \text{ over } E, \text{ or } \bar{a} \in acl_\sigma(F).$$

To simplify, let us assume that E is an algebraically closed difference field (since $\mathrm{SU}(\bar{a}/acl_\sigma(E)) = \mathrm{SU}(\bar{a}/E)$.) Let us also assume for the moment, that the tuple $\bar{a}$ is transformally algebraic over E, that is, that $tr.deg(cl_\sigma(E\bar{a})/E) = n$ is **finite**. Then, $tp(\bar{a}/F)$ forks over E if and only if

$$tr.deg(cl_\sigma(F\bar{a})/F) < tr.deg(cl_\sigma(E\bar{a})/E).$$

This implies that $\mathrm{SU}(\bar{a}/E) \leq n$. Equality however does not always hold. For instance, one can show that any non-realised type containing the formula $\sigma^2(x) = x^2$, or the formula $\sigma^2(x) = x^2 + 1$, has SU-rank 1.

3.17. **The type of SU-rank** ω. Let $E = acl_\sigma(E)$, and consider an element $a \in K$ which is transformally transcendental over E, that is, the elements $\sigma^i(a), i \in \mathbb{Z}$, are algebraically independent over E. Let $b_0 = a$, and $b_n = \sigma(b_{n-1}) - b_{n-1}$ for $n \geq 1$. Then, letting $L_n = cl_\sigma(Eb_n)$, we get that each L_n contains L_{n+1}, and has transcendence degree 1 over L_{n+1}. Hence, $\mathrm{SU}(b_n/Eb_{n+1}) = 1$ (since it is not 0, and is at most 1). Hence, $\mathrm{SU}(a/Eb_n) = n$, which implies that $\mathrm{SU}(a/E) \geq \omega$. On the other hand, any forking extension of $tp(a/E)$ has finite SU-rank (since if a is not independent from F over E, then a satisfies some σ-equation, i.e., $tr.deg(cl_\sigma(Fa)/F) < \infty$). Hence, $\mathrm{SU}(a/E) = \omega$.

Note that

$$\omega = \mathrm{SU}(a, b_1/E) = \mathrm{SU}(a/Eb_1) + \mathrm{SU}(b_1/E) < \mathrm{SU}(a/Eb_1) \oplus \mathrm{SU}(b_1/E) = \omega + 1.$$

3.18. **Other examples**. Let V be a variety of dimension d defined over some $E = acl_\sigma(E) \subseteq K$. Assume that if $\bar{a} = (a_1, \ldots, a_n)$ is a tuple of $V(K)$ which is generic over E, then the elements $a_1, \ldots, a_d$ are algebraically independent over

E. Consider the type $p_V(\bar{x})$ over E which says that $x_1, \ldots, x_d$ are transformally independent over E (i.e., satisfy non non-trivial difference equation over E), and that $(x_1, \ldots, x_n) \in V$. According to the additivity rule (one can also see it directly), if $\bar{a}$ realises p_V, then $\mathrm{SU}(\bar{a}/E) = \omega_d$. The type $p_V(\bar{x})$ is in a sense a *generic type of the variety* V. One can show that this type is complete.

Finally, one shows easily that if $\bar{a}$ is any tuple of K, then $\mathrm{SU}(\bar{a}/E)$ is of the form $\omega n + m$ for some non-negative integers n, m.

3.19. **Definition of imaginaries, etc.** Let M be a model of a complete theory T in a language $\mathcal{L}$. We assume M to be sufficiently saturated. Let $S \subseteq M^n$ be a 0-definable set, and let $E \subseteq S^2$ be a 0-definable equivalence relation. Then each E-equivalence class $\bar{a}/E$, with $\bar{a} \in S$, is called an *imaginary* element.

Given S and E as above, the set S/E is interpretable in M. To each such pair, we associate a new sort, and let M^{eq} be the many-sorted structure with sorts indexed by the pairs (S, E) as above, the "real sort" being the $\mathcal{L}$-structure M, and the sort indexed by (S, E) being the set S/E; there is also a projection map $S \to S/E$ for each (S, E). The structure M^{eq} is then interpretable in M. The difference between many-sorted logic and 1-sorted logic, is that all quantifiers, variables and constants have a sort attached to them, so that you will have things like $\forall x \in M$, $\forall y \in S/E$. Note also that M^n becomes a sort, so that an n-tuple of M can be thought of as an element of M^{eq}.

An important example of imaginary is the following. Let $D \subseteq M^k$ be a definable set, defined by some formula $\varphi(\bar{x}, \bar{b})$, where $\varphi(\bar{x}, \bar{y}) \in \mathcal{L}$ and $\bar{b}$ is an n-tuple from M. Define an equivalence relation E on M^n by:

$$E(\bar{y}, \bar{z}) : \forall \bar{x}\, (\varphi(\bar{x}, \bar{y}) \leftrightarrow \varphi(\bar{x}, \bar{z})).$$

Then the equivalence class $\bar{b}/E$ has the following property: for all $\rho \in Aut(M)$, $\rho(D) = D$ if and only if ρ fixes $\bar{b}/E$.

The imaginary element $\bar{b}/E$ will be called a *code for* D.
We say that T *eliminates imaginaries* if whenever $D \subseteq M^k$ is definable (with parameters), then there is tuple $\bar{d}$ in M, such that for any $\rho \in Aut(M)$,

$$\rho(D) = D \iff \rho \text{ fixes the elements of the tuple } \bar{d}.$$

If the language $\mathcal{L}$ has at least two terms t_0, t_1 and $T \models t_0 \neq t_1$, then T eliminates imaginaries if and only if whenever $S \subseteq M^n$ is 0-definable, and $E \subseteq S^2$ is a 0-definable equivalence relation, then there is a 0-definable function $f : S \to M^k$ for some k, such that for every $\bar{y}, \bar{z} \in S$, we have

$$M \models f(\bar{y}) = f(\bar{z}) \iff E(\bar{y}, \bar{z}).$$

3.20. **Some facts**. (1) If T eliminates imaginaries, and $A \subset M$, then $T(A)$ eliminates imaginaries as well ($T(A)$ is the set of sentences in the language $\mathcal{L}(A)$ obtained by adjoining to $\mathcal{L}$ a constant symbol for each element of A, which hold in the $\mathcal{L}(A)$-structure $(M, a)_{a \in A}$.)

(2) □□□ Assume that M is stable. Working in M^{eq} instead of M, one has the following: if a is independent from b over cd and from c over bd, then a is independent from (bc) over $acl^{eq}(bd) \cap acl^{eq}(cd)$. Note that a tuple of elements

of M can be thought of as an imaginary element. The proof uses the following ingredients. By elimination of imaginaries and stability, we know that every type p over an algebraically closed set E is *stationary* (i.e., has a unique non-forking extension to any superset of E), and is *definable over* E, i.e., given a formula $\varphi(\bar{x}, \bar{y}) \in \mathcal{L}$, there is a formula $d_\varphi(\bar{y}) \in \mathcal{L}(E)$ such that for every tuple $\bar{b}$ in E, we have that

$$\varphi(\bar{x}, \bar{b}) \in p \iff M \models f_\varphi(\bar{b}).$$

The non-forking extension p' of p to a set F containing E will then be defined analogously: for every $\bar{b} \in F$, $\varphi(\bar{x}, \bar{b}) \in p' \iff M \models d_\varphi(\bar{b})$. One defines the *canonical base of* p, denoted by $Cb(p)$, to be the set of codes of the formulas $d_\varphi(\bar{y})$ (and by elimination of imaginaries, this is a subset of E). By definition we have that p does not fork over $Cb(p)$, and that the restriction of p to $Cb(p)$ is stationary. Moreover, if $E_0 \subset E$ is such that p does not fork over E_0, then $acl(E_0)$ contains $Cb(p)$.

Hence, we look at the canonical base of $tp(a/acl(bcd))$ and from the independence relations, deduce that it is contained in $acl(bd) \cap acl(cd)$.

We will use the fact that every completion of the theory ACF of algebraically closed fields eliminates imaginaries and is stable. Note that the above proof extends to the case of M simple with stable forking (for those of you who know what this means). □□□

(2') Let us rephrase (2) in a more algebraic language. We work within a sufficiently large algebraically closed field Ω. It is known that any algebraic set V defined over Ω has a *smallest field of definition*. If one looks at what it means in terms of independence, it translates as follows: let E and F be algebraically closed subfields of Ω, let $\bar{a}$ be a tuple of elements of Ω, and assume that

$$\bar{a} \downarrow_E F \quad \text{and} \quad \bar{a} \downarrow_F E.$$

This means that if V is the locus of $\bar{a}$ over $(EF)^{alg}$, then V is defined over E and V is defined over F. Indeed, let V_1 be the locus of $\bar{a}$ over E. As $E \subset EF$, we certainly have $V_1 \supseteq V$. From the fact that $\bar{a}$ is free from F over E, we know that the dimensions of V_1 and V (which equal respectively $tr.deg(\bar{a}/E)$ and $tr.deg(\bar{a}/EF)$) are equal. As V_1 is irreducible, this implies that $V = V_1$, so that V is defined over E. Reasoning similarly with the locus of $\bar{a}$ over F, one obtains that V is defined over F.

The uniqueness of the smallest field of definition of V then implies that V is defined over $E \cap F$. Hence, all equations over EF satisfied by $\bar{a}$ are implied by equations over $E \cap F$. This implies that $tr.deg(\bar{a}/E \cap F) = dim(V)$, so that

$$\bar{a} \downarrow_{E \cap F} EF.$$

(3) In the case of fields, any finite set has a code. Let us show how it works for elements of M: we want to code the definable set $\{a_1, \ldots, a_n\}$. Consider the polynomial $f(X) = \prod_{i=1}^{n}(X - a_i)$, and let $b_1, \ldots, b_n$ be its coefficients. Then any permutation of $\{a_1, \ldots, a_n\}$ fixes $b_1, \ldots, b_n$, and conversely. Hence the tuple $(b_1, \ldots, b_n)$ is a code for the set $\{a_1, \ldots, a_n\}$. There is a similar trick for finite sets of tuples.

(4) The uniqueness of the field of definition of algebraic sets also gives easily that any completion of the theory of algebraically closed fields eliminates

imaginaries. Indeed, let K be an algebraically closed field. By elimination of quantifiers, we know that any definable subset D of K^n is a Boolean combination of algebraic sets. Then D can be written $V \setminus W$, where V is the Zariski closure of D, and W is some definable subset of V, with the property that every irreducible component of its Zariski closure $\bar{W}$ is strictly contained in some irreducible component of V. In particular, $dim(\bar{W}) < dim(V)$. Clearly any automorphism ρ of K which leaves D invariant will also leave V and W invariant. The automorphism ρ leaves V invariant if and only if it fixes the field of definition of V. The result follows by induction on the dimension.

This type of proof generalises to other theories of fields which eliminate quantifiers: the theory of differentially closed fields of characteristic 0, and also the theory of separably closed fields of finite degree of imperfection (in that case, one needs however to add some constant symbols to the language).

3.21. **Theorem** Any completion of ACFA eliminates imaginaries.

Sketch of the proof. □□□ We work in a saturated model K of ACFA. We are given a 0-definable function f, and a tuple $\bar{a}$, and we look at the equivalence class e of $\bar{a}$ for the equivalence relation $E(\bar{x}, \bar{y}) \iff f(\bar{x}) = f(\bar{y})$. We want to show that there is a real tuple which is equi-definable with e.

Let $E = acl^{eq}(e) \cap K$. If e is definable over E, then we are done: choose a tuple $\bar{b} \in E$ over which e is definable. Then $\bar{b} \in acl^{eq}(e)$. Since we are in a field, there is a tuple $\bar{c}$ which codes the finite set of conjugates of $\bar{b}$ over e. Then $\bar{c}$ and e are equi-definable. Hence, we may assume that e is not definable over E, and in particular that $\bar{a} \notin E$. Our aim is to show that there is a tuple $\bar{b}$ realising $tp(\bar{a}/e)$ which is independent from $\bar{a}$ over E.

Let $p = tp(\bar{a}/e)$. Since p is non-algebraic, there is $\bar{b}$ realising p and such that $acl^{eq}(e\bar{a}) \cap acl^{eq}(e\bar{b}) = acl^{eq}(e)$, and therefore

$$acl_\sigma(E\bar{a}) \cap acl_\sigma(E\bar{b}) = E. \qquad (*)$$

Choose $\bar{b}$ realising p, satisfying $(*)$ and of maximal SU-rank over $E\bar{a}$ (note that $f(\bar{b}) = e$). Let $\bar{c}$ realise $tp(\bar{b}/E\bar{a})$, independent from $\bar{b}$ over $E\bar{a}$. Then c realises p, as $e \in dcl^{eq}(\bar{a})$. Moreover, $acl_\sigma(E\bar{c}) \cap acl_\sigma(E\bar{b}) \subseteq acl_\sigma(E\bar{b}) \cap acl_\sigma(E\bar{a})$ (because $acl_\sigma(E\bar{a}\bar{b}) \cap acl_\sigma(E\bar{a}\bar{c}) = acl_\sigma(E\bar{a})$), and therefore the tuple $(\bar{b}, \bar{c})$ also satisfies $(*)$. By maximality of the SU-rank of $\bar{b}$ over $E\bar{a}$ and because $tp(a/e) = tp(b/e)$, we get that

$$\mathrm{SU}(\bar{c}/E\bar{b}) \leq \mathrm{SU}(\bar{b}/E\bar{a}).$$

We also know that

$$\mathrm{SU}(\bar{c}/E\bar{a}\bar{b}) = \mathrm{SU}(\bar{c}/E\bar{a}) = \mathrm{SU}(\bar{b}/E\bar{a}).$$

As $\mathrm{SU}(\bar{c}/E\bar{a}\bar{b}) \leq \mathrm{SU}(\bar{c}/E\bar{b})$, we obtain that

$$\mathrm{SU}(c/E\bar{a}\bar{b}) = \mathrm{SU}(\bar{b}/E\bar{a}) = \mathrm{SU}(\bar{c}/E\bar{b}),$$

so that $cl_\sigma(\bar{c})$ is independent from $acl_\sigma(E\bar{a}\bar{b})$ over $acl_\sigma(E\bar{a})$ and over $acl_\sigma(E\bar{b})$ (in the sense of the theory of algebraically closed fields). By elimination of imaginaries of the theory of algebraically closed fields, this implies that $cl_\sigma(\bar{c})$ is (ACF-)independent from $cl_\sigma(\bar{a}, \bar{b})$ over $acl_\sigma(E\bar{a}) \cap acl_\sigma(E\bar{b}) = E$, i.e., that $\bar{c}$

is (ACFA-) independent from $(\bar{a}, \bar{b})$ over E. Hence $\mathrm{SU}(\bar{b}/E\bar{a}) = \mathrm{SU}(\bar{c}/E\bar{a}) = \mathrm{SU}(\bar{c}/E)$, so that $\bar{a}$ and $\bar{b}$ were independent over E.

Hence, we have shown that there is a realisation $\bar{b}$ of p, which is independent from $\bar{a}$ over E. Since e is not definable over E, there is $\bar{a}'$ realising $tp(\bar{a}/E)$ and with $f(\bar{a}') \neq f(\bar{a})$. Since $tp(\bar{a}'/E) = tp(\bar{a}/E)$, there is $\bar{c}'$ realising $tp(\bar{a}'/E)$, with $f(\bar{a}') = f(\bar{c}')$, and independent from $\bar{a}'$ over E and we may assume that this $\bar{c}'$ is also independent from $\bar{b}$ over E. Apply the independence theorem to $tp(\bar{a}/E\bar{b}) \cup tp(\bar{a}'/E\bar{c}')$ to derive a contradiction. □□□

3.22. **Corollary**. Let $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ be tuples in K, and assume that $\bar{a}$ is independent from $\bar{b}$ over $(\bar{c}\bar{d})$ and from $\bar{c}$ over $(\bar{b}\bar{d})$. Then $\bar{a}$ is independent from $(\bar{b}\bar{c})$ over $acl_\sigma(\bar{b}\bar{c}) \cap acl_\sigma(\bar{b}\bar{d})$.

Proof. Either use the remark about simple theories with stable forking given in 3.20(2), or equivalently, the fact that independence in models of ACFA corresponds to independence of algebraically closed sets for the theory of algebraically closed fields. One uses also the fact that $acl_\sigma(AB) = (acl_\sigma(A)acl_\sigma(B))^{alg}$.

3.23. **A useful remark**. Let K be a model of ACFA, E an algebraically closed subset of K and $\bar{a}$ a tuple of elements of K. As in the case of algebraically closed fields, one can show that $I_\sigma(\bar{a}/E)$ has a smallest field of definition (as a σ-ideal). Or more simply, this follows from the elimination of imaginaries. So, let us suppose that E is the algebraic closure of this smallest field of definition, so that in particular it is the algebraic closure of a **finite tuple**, and therefore is ranked by the SU-rank.

Claim. For n sufficiently large, if $\bar{a}_0, \ldots, \bar{a}_n$ are independent realisations of $tp(\bar{a}/E)$, then $E \subseteq acl_\sigma(\bar{a}_0, \ldots, \bar{a}_n)$.

Proof. We assume K sufficiently saturated. Construct by induction on $n \in \mathbb{N}$ a sequence $\bar{a}_n$, $n \in \mathbb{N}$, of realisations of $tp(\bar{a}/E)$, with $\bar{a}_n \downarrow_E \bar{a}_0, \ldots, \bar{a}_{n-1}$ for every n. Then

$$\mathrm{SU}(E/\bar{a}_0, \ldots, \bar{a}_n) \leq \mathrm{SU}(E/\bar{a}_0, \ldots, \bar{a}_{n-1})$$

for every n, so that there is some index m such that $\mathrm{SU}(E/\bar{a}_0, \ldots, \bar{a}_{m+1}) = \mathrm{SU}(E/\bar{a}_0, \ldots, \bar{a}_m)$. Take the smallest such m. Then

$$E \downarrow_{\bar{a}_0, \ldots, \bar{a}_m} \bar{a}_{m+1},$$

and by assumption

$$\bar{a}_{m+1} \downarrow_E \bar{a}_0, \ldots, \bar{a}_m.$$

Corollary 3.22 then gives

$$\bar{a}_{m+1} \downarrow_{E \cap acl_\sigma(\bar{a}_0, \ldots, \bar{a}_m)} E, \bar{a}_0, \ldots, \bar{a}_m,$$

and therefore $E \subseteq acl_\sigma(\bar{a}_0, \ldots, \bar{a}_m)$.

3.24. **Exercise 8**. Show that the formula $\sigma^2(x) = x^2$ has SU-rank 1. I.e., you need to show that given any algebraically closed difference field E and element a satisfying $\sigma^2(x) = x^2$, one **cannot have** $tr.deg(cl_\sigma(Ea)/E) = 1$.

§4. Study of the fixed field. A particularly important definable subset of a model K of ACFA is the fixed field, $Fix(\sigma) = \{x \in K \mid \sigma(x) = x\}$. It turns out that this subfield is responsible for much of the bad behaviour of models of ACFA. We will show that $Fix(\sigma)$ is a pseudo-finite field, i.e., is elementary equivalent to an ultraproduct of finite fields (or equivalently, is an infinite model of the theory of finite fields). Pseudo-finite fields were first studied by Ax, see [9]. Some very nice results on pseudo-finite fields were also obtained in two papers by E. Hrushovski and A. Pillay ([11] and [12])

4.1. **Theorem**. Let K be a model of ACFA, and $F = Fix(\sigma)$. Then F is a pseudo-finite field.

Proof. We need to show that

(i) F is perfect (i.e., if $char(F) = p > 0$, then every element is a p-th power).
(ii) $\mathcal{G}al(F^{alg}/F) \simeq \hat{\mathbb{Z}} \simeq \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} \simeq \prod_{p \text{ prime}} \mathbb{Z}_p$.
(iii) F is pseudo-algebraically closed (PAC), i.e., every variety defined over F has a point with coordinates in F.

Item (i) is no problem: if the characteristic is $p > 0$, then every element a has a unique p-th root, denoted by $a^{1/p}$. Hence $\sigma(a) = a$ implies $\sigma(a^{1/p}) = a^{1/p}$, and F is perfect. Item (iii) is no problem either: let U be a variety defined over F, and consider the diagonal subvariety $V \subseteq U \times U$, i.e., V is defined by $\bar{x} \in U$, $\bar{y} \in U$, and $\bar{x} = \bar{y}$. Then $U = U^\sigma$, and U, V satisfy the hypotheses of axiom (3) of ACFA, so that there is $\bar{a} \in K$ with $(\bar{a}, \sigma(\bar{a})) \in V$, i.e., $\bar{a} \in U$ and $\sigma(\bar{a}) = \bar{a}$.

Let us now look at item (ii). First of all, if L is a finite Galois extension of F, then $\sigma(L) = L$: if α generates L over F, then σ fixes the coefficients of the minimal monic polynomial of α over F, so that $\sigma(\alpha) \in L$. Hence σ restricts to an element of $\mathcal{G}al(L/F)$. By Galois theory, $F = Fix(\sigma)$ is the subfield of L fixed by the group generated by $\sigma_{|L}$, and this shows that $\mathcal{G}al(L/F)$ is cyclic, generated by $\sigma_{|L}$.

We will now show that for every n, F has **at most one** Galois extension of degree n. Given a finite Galois extension L of F, there is a 1-1 correspondence between algebraic extensions of F contained in L, and subgroups of $\mathcal{G}al(L/F)$, under which the extensions which are Galois over F correspond to the normal subgroups of $\mathcal{G}al(L/F)$. Every finite algebraic extension of F is contained in a finite Galois extension of F, and all subgroups of a cyclic group are normal. Hence every algebraic extension of F is Galois.

Assume now by way of contradiction that F has two Galois extensions, L and M, of the same degree n over F. Consider $\mathcal{G}al(LM/F)$. Then $\mathcal{G}al(LM/L)$ and $\mathcal{G}al(LM/M)$ are subgroups of $\mathcal{G}al(LM/F)$ of order $d = [LM : F]/n$. But $\mathcal{G}al(LM/F)$ is cyclic, and therefore has only one subgroup of order d: this implies that $L = M$.

To show (ii), it will be enough to show that for every n, F has **at least** one Galois extension of degree n. But this is easy: consider the difference field extension $L = K(X_1, \ldots, X_n)$ of K ($X_1, \ldots, X_n$ indeterminates), with $\sigma(X_i) = X_{i+1}$ for $i = 1, \ldots, n-1$, and $\sigma(X_n) = X_1$. Then

$$L \models \exists x \ \sigma^n(x) = x \wedge \bigwedge_{1 \leq i < n} \sigma^i(x) \neq x,$$

so that K satisfies the same sentence. Let $a \in K$ be such that $\sigma^n(a) = a$, $\sigma^i(a) \neq a$ for $1 \leq i < n$. By Galois theory, a generates a Galois extension of degree n of F.

4.2. **An example** We saw earlier that if A is an algebraically closed difference field, then ACFA $\cup\, qftp(A)$ is complete. Hence, in a sense, ACFA is close to having quantifier-elimination. However, it does not. Here is an example:

Let $a, b \in Fix(\sigma)$ be transcendental elements, and assume that a does not have a square root in $Fix(\sigma)$ (so, we assume that $char(Fix(\sigma)) \neq 2$). Then we have:

$$K \models \forall y\, y^2 = a \rightarrow \sigma(y) \neq y$$
$$K \models \exists y\ y^2 = b^2 \wedge \sigma(y) = y.$$

However, a and b^2 have the same quantifier-free type, as the quantifier-free type of a transcendental element of the fixed field is unique: it simply says that the element satisfies no non-trivial equation (over $\mathbb{Q}$ or over $\mathbb{F}_p$).

4.3. **Proposition**. Let $K \models$ ACFA, and consider $F = Fix(\sigma) = \{x \in K \mid \sigma(x) = x\}$. Every definable subset of F^n is definable in the pure field F. In other words, the structure on F induced by K is the one of the pure field F.

Proof. We assume K sufficiently saturated. Let $S \subset F^n$ be definable (in K). Then $\sigma(S) = S$. By elimination of imaginaries, this implies that there is a tuple $\bar{c}$ of elements of F, and a formula $\varphi(\bar{x}, \bar{y})$ such that $\varphi(\bar{x}, \bar{c})$ defines S. Hence, we have shown that S is definable over F. To finish the proof, it suffices to show that there is a "small" subset C of F such that every field-automorphism of F which fixes C is an elementary map within the structure K (exercise).

Let C be a countable elementary substructure of the field F. Then C^{alg} and F are linearly disjoint over C because $C \prec F$. If C_n is the unique algebraic extension of C of degree n, then FC_n is an algebraic extension of F of degree n also, and therefore is the unique algebraic extension of F of degree n. Hence $F^{alg} = FC^{alg}$.

Let ρ be a field-automorphism of F which is the identity on C. Because C^{alg} and F are linearly disjoint over C, we can extend ρ to a field-automorphism $\tilde{\rho}$ of FC^{alg} which is the identity on C^{alg}. Since $F^{alg} = FC^{alg}$, we get that $\tilde{\rho}$ is defined on $F^{alg} = acl_\sigma(F)$. We have

$$\sigma\tilde{\rho}|_F = \tilde{\rho}\sigma|_F$$

because $\sigma|_F = id_F$, and

$$\sigma\tilde{\rho}|_{C^{alg}} = \tilde{\rho}\sigma|_{C^{alg}}$$

because $\rho|_{C^{alg}} = id_{C^{alg}}$. Hence, $\tilde{\rho}$ commutes with σ on C^{alg} and on F, so that $\tilde{\rho}$ is an automorphism of the difference field $acl_\sigma(F)$. By 2.15, $\tilde{\rho}$ is an elementary map.

4.4. **Exercise 9**. Let K be a model of ACFA, F its fixed field.

(1) Let E be a subfield of F such that $E^{alg}F = F^{alg}$, and $\bar{a}$ a tuple of elements of F. Show that $\mathrm{SU}(\bar{a}/E) = tr.deg(E(\bar{a})/E)$.

(2) Let S be a definable subset of F^n. Show that $\mathrm{SU}(S)$ equals the algebraic dimension of the Zariski closure (in K) of S.

§5. Orthogonality and modularity. In this section we will show that we can reduce the study of types of finite SU-rank to the study of types of SU-rank 1. We will always be working in a model K of ACFA, which we will assume to be sufficiently saturated.

5.1. **Definitions**. Let A and B subsets of K, and p, q types over A and B respectively.

(1) If $A = B$, then we say that p and q are *almost orthogonal* (denoted by $p \perp^a q$) if whenever $\bar{a}$ realises p and $\bar{b}$ realises q, then $\bar{a}$ and $\bar{b}$ are independent over A.
(2) We say that p and q are *orthogonal* (denoted by $p \perp q$) if whenever C contains $A \cup B$, and $\bar{a}$ is a realisation of p which is independent from C over A, $\bar{b}$ is a realisation of q which is independent from C over B, then $\bar{a}$ and $\bar{b}$ are independent over C.
(3) Recall that $S \subseteq K^n$ is *∞-definable over E*, or *type-definable over E*, if there is a partial n-type Φ over E (i.e., a consistent set of $\mathcal{L}(E)$-formulas in the variables $(x_1, \ldots, x_n)$) such that S is the set of n-tuples from K satisfying Φ.
(4) Let S be a set which is (∞-) definable over B. We say that p is *orthogonal to S* (denoted by $p \perp S$, or by $p \perp \varphi$ if S is defined by φ) if p is orthogonal to all types over supersets of B which are realised in S, i.e.: for all C containing $A \cup B$, and $\bar{a}$ realising p and independent from C over A, and $\bar{b} \in S$, we have that $\bar{a}$ and $\bar{b}$ are independent over C. One also says that p is *foreign* to S or to φ.

5.2. **Remark and example**. Note that in (4) above, we do not require that $\bar{b}$ be independent from C over B. Here is an example which shows that orthogonality to a set and to a type are different.

Let $E = acl_\sigma(E) \subseteq K$, and let p be the type of a transformally transcendental element a over E, let P be the set of realisations of p over E.

Then p is orthogonal to all types of finite SU-rank over E: indeed, assume that a is transformally transcendental over $F = acl_\sigma(F) \supset E$, and that $\mathrm{SU}(b/F) < \omega$, but a and b are not independent over F. This means that $I_\sigma(a/acl_\sigma(Fb))$ is non-zero, and therefore that a is transformally algebraic over $acl_\sigma(Fb)$, i.e., $\mathrm{SU}(a/Fb) < \omega$. But this contradicts Lascar's inequality: on the one hand, we have $\mathrm{SU}(a, b/F) \geq \mathrm{SU}(a/F) = \omega$, and on the other, we have $\mathrm{SU}(a, b/F) \leq \mathrm{SU}(a/Fb) \oplus \mathrm{SU}(b/F) < \omega$.

However, let $c = \sigma(a) - a$, let a' be a realisation of $tp(a/acl_\sigma(Ec))$, independent from a over Ec, and let $b = a - a'$. Then $\sigma(b) = \sigma(a) - \sigma(a') = (a + c) - (a' + c) = a - a' = b$, so that $\mathrm{SU}(b/E) = 1 = \mathrm{SU}(b/Ea')$. So we have that $tp(b/E) \not\perp tp(a/Ea')$, and therefore $tp(b/E) \not\perp P$.

5.3. **Another comment about orthogonality**. Orthogonality or non-orthogonality tell us about interactions between sets. For instance, let D_1 and D_2 be two infinite definable sets, defined over some $E = acl_\sigma(E)$.

If all types realised in D_1 are orthogonal to all types realised in D_2, then this means that whenever you take a tuple $\bar{a}$ of elements in D_1 and a tuple $\bar{b}$ of elements of D_2, then they are independent over any set containing E. In particular, any definable map $f : S \to D_2^m$, where $S \subseteq D_1^n$, for some integers m, n, will take only finitely many values.

Assume in addition that all types realised in D_1 and in D_2 are stationary (Recall that a type over a set A is *stationary* if it has a unique non-forking extension to any set containing A). It will then follow that any definable subset of $D_1 \times D_2$ is a finite union of rectangles, i.e., is of the form $\bigcup_{i=1}^n S_i \times T_i$, where S_i is a definable subset of D_1 and T_i is a definable subset of D_2.

5.4. **Exercise 10**. Let $E = acl_\sigma(E) \subset K$, $\bar{a}$, $\bar{b}$ tuples from K, and assume that $\mathrm{SU}(\bar{a}/E) = \mathrm{SU}(\bar{b}/E) = 1$. Show that $tp(\bar{a}/E) \not\perp tp(\bar{b}/E)$ implies that $tr.deg(cl_\sigma(E\bar{a})/E) = tr.deg(cl_\sigma(E\bar{b})/E)$.

5.5. **Exercise 11**. Let p, q, r be types over algebraic closed sets A, B, and C respectively. Assume that p, q and r have SU-rank 1, and that $A \mathop{\smile\!\!\!\!\!\!|}_B C$. Show that if $p \not\perp q$ and $q \not\perp r$, then $p \not\perp r$. [Warning: your proof should use all the assumptions on A, B, C: their being algebraically closed, and the independence hypothesis. Non-orthogonality **is not** an equivalence relation on types of SU-rank 1. One can however show that the relation E defined by $E(p, q)$ if and only if there is r of SU-rank 1 such that $p \not\perp r$ and $q \not\perp r$ defines an equivalence relation on types of SU-rank 1.]

5.6. **Exercise 12**. Let $E = acl_\sigma(E) \subset K$, and $a \in K$ with $\mathrm{SU}(a/E) = 1$. Assume that $tp(a/E) \not\perp (\sigma(x) = x)$. We know that $tr.deg(cl_\sigma(Ea)/E) = 1$, so that $E(a)^{alg} = acl_\sigma(Ea)$. Show that there exists an integer N such that $[E(a, \sigma^k(a)) : E(a)] \leq N$ for every $k \in \mathbb{Z}$. [Hint: take $E' = acl_\sigma(E')$ independent from a over E such that there is some $b \in acl_\sigma(E'a) \setminus E'$, with $\sigma(b) = b$. Then for every k one has $[E(a, \sigma^k(a)) : E(a)] = [E'(a, \sigma^k(a)) : E'(a)]$, so we may assume that $E = E'$. Let $m = [E(a, b) : E(a)]$, $n = [E(a, b) : E(b)]$. Show that $[E(a, b, \sigma^k(a)) : E(a)] \leq mn$.]

5.7. **Remark**. One can show that the converse is true, but the proof is much harder.

5.8. **Exercise 13/Example**. Let $E = acl_\sigma(E) \subset K$, let $a \in E$, and let $b \in K \setminus E$ satisfy $\sigma(x) - x = a$.

(a) Show that $tp(b/E) \not\perp (\sigma(x) = x)$.
(b) Show that $tp(b/E)$ is not almost orthogonal to some type containing $\sigma(x) = x$, if and only if there is an integer $m > 0$ and $\alpha \in E$ satisfying $\sigma^m(x) = x + a + \cdots + \sigma^{m-1}(a)$. [Hint: assume that $c \in (acl_\sigma(Eb) \setminus E) \cap Fix(\sigma)$; looking at the coefficients of the minimal polynomial of c over $cl_\sigma(Eb)$, we may in fact assume that $c \in cl_\sigma(Eb)$, so that $c = g(b)$ for some $g(X) \in E(X)$. Look at the sets S_0 of poles and S_1 of zeroes of g, and use the equation $g(b) = g^\sigma(b + a)$.]

5.9. **Proposition**. Every finite SU-rank type is non-orthogonal to a type of SU-rank 1.

Proof. Let $E = acl_\sigma(E) \subset K$, and let $\bar{a}$ be a tuple in K with $\mathrm{SU}(\bar{a}/E) = n < \omega$. We want to find $F = acl_\sigma(F)$ independent from $\bar{a}$ over E, and $b \in acl_\sigma(F\bar{a}) \setminus F$ such that $\mathrm{SU}(b/F) = 1$.

By definition of the SU-rank, there is some tuple $\bar{d}$ such that $\mathrm{SU}(\bar{a}/E\bar{d}) = n-1$. Given such a tuple, we may always write it as $(\bar{b}, \bar{c})$, with $\bar{c}$ independent from $\bar{a}$ over E. Find $(\bar{b}, \bar{c})$ such that $\bar{c}$ and $\bar{a}$ are independent over E, $\mathrm{SU}(\bar{a}/E\bar{b}\bar{c}) = n-1$, and $\mathrm{SU}(\bar{b}/E\bar{c})$ is least possible.

Let $\bar{a}'$ realise $tp(\bar{a}/E\bar{b}\bar{c})$ and independent from $\bar{a}$ over $E\bar{b}\bar{c}$. Then $\mathrm{SU}(\bar{a}/E\bar{b}\bar{c}\bar{a}') = \mathrm{SU}(\bar{a}/E\bar{b}\bar{c}) = n - 1$.

Claim. $\bar{a}$ and $\bar{a}'$ are not independent over $E\bar{c}$.

Otherwise, assume that $\bar{a}$ and $\bar{a}'$ are independent over $E\bar{c}$, and let $\bar{c}' = (\bar{c}, \bar{a}')$. Since $\bar{a}'$ realises $tp(\bar{a}/E\bar{b}\bar{c})$, we have $\mathrm{SU}(\bar{a}'/E\bar{b}\bar{c}) < \mathrm{SU}(\bar{a}'/E\bar{c})$; hence, by symmetry we get $\mathrm{SU}(\bar{b}/E\bar{c}\bar{a}') < \mathrm{SU}(\bar{b}/E\bar{c})$, so that the pair $(\bar{b}, \bar{c}')$ contradicts the minimality of $\mathrm{SU}(\bar{b}/E\bar{c})$.

Hence $\bar{a}'$ and $\bar{a}$ are not independent over $E\bar{c}$, so that $\mathrm{SU}(\bar{a}/E\bar{c}\bar{a}') = \mathrm{SU}(\bar{a}'/E\bar{c}\bar{a}) = n - 1$. It follows that $\bar{a}'$ is independent from $\bar{b}$ over $E\bar{c}\bar{a}$. As it was independent from $\bar{a}$ over $E\bar{c}\bar{b}$ by definition, we get that $\bar{a}'$ is independent from $(\bar{a}\bar{b})$ over $acl_\sigma(E\bar{c}\bar{a}) \cap acl_\sigma(E\bar{c}\bar{b})$ (by 3.22). Let $\bar{d} \in acl_\sigma(E\bar{c}\bar{a}) \cap acl_\sigma(E\bar{c}\bar{b})$ be such that $\bar{a}'$ and $\bar{a}\bar{b}$ are independent over $E\bar{c}\bar{d}$. By the claim, we know that $\bar{d} \notin acl_\sigma(E\bar{c})$, and this implies that

$$\mathrm{SU}(\bar{a}/E\bar{c}\bar{d}) < n,$$

as $\bar{d} \in acl_\sigma(E\bar{c}\bar{a})$. We now obtain

$$n - 1 = \mathrm{SU}(\bar{a}/E\bar{c}\bar{b}) \leq \mathrm{SU}(\bar{a}/E\bar{c}\bar{d}) < \mathrm{SU}(\bar{a}/E\bar{c}) = n,$$

so that $\mathrm{SU}(\bar{a}/E\bar{c}\bar{d}) = n - 1$, which implies that $\mathrm{SU}(\bar{d}/E\bar{c}) = 1$.

5.10. **Definitions**. Let S be an (∞-) definable set, defined over some $E = acl_\sigma(E)$. We say that S is *modular* if, for every m and n, and $\bar{a} \in S^m$, $\bar{b} \in S^n$, we have that $\bar{a}$ and $\bar{b}$ are independent over $acl_\sigma(E\bar{a}) \cap acl_\sigma(E\bar{b})$.

A type (over some set E) is *modular* if the set of its realisations is modular.

Remarks. (1) In general, one requires that $\bar{a}$ and $\bar{b}$ are independent over $acl^{eq}(E\bar{a}) \cap acl^{eq}(E\bar{b})$. We use the fact that $Th(K)$ eliminates imaginaries.

(2) This notion is also sometimes referred to as "1-basedness" in the case of stable theories.

(3) There is no harm in extending the notion to sets which are invariant under E-automorphism of K, i.e., sets of realisations of a set of types over E.

5.11. **Canonical bases**. Let $E = cl_\sigma(E)$, $\bar{a}$ a tuple. Since $I_\sigma(\bar{a}/E)$ is finitely generated as a σ-ideal, there is an integer m such that the (algebraic) locus V of $(\bar{a}, \ldots, \sigma^m(\bar{a}))$ over E completely describes $qftp(\bar{a}/E)$, i.e.,

If $\bar{b}$ is such that $(\bar{b}, \ldots, \sigma^m(\bar{b}))$ has locus V over E, then $qftp(\bar{b}/E) = qftp(\bar{a}/E)$.

Let k_0 be the field of definition of V, and let k be the difference field generated by k_0. Then $tp(\bar{a}/E)$ does not fork over k, and k is in a sense smallest with that property (not quite true in positive characteristic). We call k the *canonical base* of $tp(\bar{a}/E)$, and denote it by $Cb(\bar{a}/E)$.

5.12. **Comments**. (1) It is well-known that if $\bar{c}_i$, $i \in \omega$, is an independent sequence of generics of V over E, then k_0 is contained in the field generated

by $\bar{c}_0, \ldots, \bar{c}_N$ for some N. Hence, the same is true in our case **provided E is algebraically closed**: if $\bar{a}_i$, $i \in \omega$, is a sequence of independent realisations of $tp(\bar{a}/E)$, then k is contained in $cl_\sigma(\bar{a}_0, \ldots, \bar{a}_N)$ for some N.

(2) Our definition does not quite agree with the usual definition of canonical bases for types in simple theories.

(3) What we are really interested in, is that k^{alg} is the smallest algebraically closed difference field over which $tp(\bar{a}/E)$ does not fork. We could also have defined $Cb(\bar{a}/E)$ as k^{alg}. What really matters, is that by 1), there is an integer N such that if $\bar{a}_1, \ldots, \bar{a}_N$ are independent realisations of $tp(\bar{a}/E)$ then $Cb(\bar{a}/E) \subset acl_\sigma(\bar{a}_1, \ldots, \bar{a}_N)$. See Remark 3.23 for a proof.

5.13. **Corollary**. Let S be modular. Then for every n, m, and $\bar{a} \in S^n$, $\bar{b} \in K^m$, we have that $\bar{a}$ and $\bar{b}$ are independent over $C = acl_\sigma(E\bar{a}) \cap acl_\sigma(E\bar{b})$.

Proof. Let $\bar{a}_i$, $i \in \omega$, be a sequence of realisations of $tp(\bar{a}/acl_\sigma(E\bar{b}))$, independent over $E\bar{b}$, and with $\bar{a}_0 = \bar{a}$. Then $C = acl_\sigma(E\bar{a}_i) \cap acl_\sigma(E\bar{b})$ for $i \in \omega$ because $tp(\bar{a}_i/E\bar{b}) = tp(\bar{a}/E\bar{b})$. Since $\bar{a}$ is independent from $\{\bar{a}_i \mid i > 0\}$ over $E\bar{b}$, we have

$$C = acl_\sigma(E\bar{a}) \cap acl_\sigma(E\bar{a}_i \mid i > 0).$$

By the above, $acl_\sigma(E\bar{a}_i \mid i > 0)$ contains the canonical base of $tp(\bar{a}/acl_\sigma(E\bar{b}))$. By modularity, we get that this canonical base is contained in C, and therefore that $\bar{a}$ and $\bar{b}$ are independent over C.

5.14. **Remark**. This is a particularly nice way of phrasing modularity: a set S is modular if and only if, for every tuple $\bar{a}$ of elements of S and set B, we have that $acl_\sigma(E\bar{a}) \cap acl_\sigma(EB)$ contains the canonical base of $tp(\bar{a}/acl_\sigma(EB))$. It coincides with the definition of 1-basedness.

5.15. **What is modularity**? Or rather, what is it not? Modularity forbids the existence of complicated sets. For instance, in the theory of algebraically closed fields, no infinite set is modular. This comes from the typical counterexample to modularity: let a, b, c be algebraically independent over $\mathbb{Q}$, say, and let $d = ac + b$. Then

$$\mathbb{Q}(a, b)^{alg} \cap \mathbb{Q}(c, d)^{alg} = \mathbb{Q}^{alg},$$

but (a, b) and (c, d) are not independent.

In case the elements of S have SU-rank 1, modularity is equivalent to the non-existence of a SU-rank-2 family of "curves", that is, a set $C(e)$, $e \in D$, of definable subsets of S^2 of SU-rank 1, where D is definable, has SU-rank 2, and is such that if $d \neq d' \in D$, then $C(d) \cap C(d')$ is finite.

When we are in a stable situation and there is a group around, there is a remarkable theorem of Hrushovski-Pillay ([14]) which says:

Theorem. Let G be a stable group (maybe with additional structure), and assume that G is modular. Then for every n, any definable subset of G^n is a Boolean combination of cosets of definable subgroups of G^n, and these subgroups are defined over $acl(\emptyset)$.

Thus in particular, a stable modular group has essentially only one group law. Moreover, one can show that it is necessarily abelian by finite.

The completions of ACFA are unstable, and we will not be able to apply directly the result of Hrushovski-Pillay. In fact, in positive characteristic this

result will be **false**. However, all the quantifier-free formulas are "stable" and they control independence (I will not define what a stable formula is, let me just say that if T is a stable theory then all formulas are stable). It will follow that some restricted version of H-P's theorem holds in positive characteristic, while the full result holds in characteristic 0.

5.16. **Lemma**. Let T be a complete theory satisfying the conclusion of 3.20(2), that if $A \downarrow_C B$ and $A \downarrow_B C$ then $A \downarrow_{acl(B)\cap acl(C)} BC$ (e.g., eliminating imaginaries, and stable or with stable forking), let A, B, C be algebraically closed sets containing $E = acl(E)$, and assume that C is independent from (A, B) over E. Then $acl(AC) \cap acl(BC) = acl((A \cap B)C)$.

Proof. Let $\alpha \in acl(AC) \cap acl(BC)$. By hypothesis, $C \downarrow_E AB$, so that $C \downarrow_A B$. Since $\alpha \in acl(AC)$, we get $(C, \alpha) \downarrow_A B$. Similarly, $(C, \alpha) \downarrow_B A$. By 3.20, we obtain $(C, \alpha) \downarrow_{A\cap B} (A, B)$, which gives $\alpha \in acl((A \cap B)C)$.

5.17. **Proposition**. Let $E = acl_\sigma(E) \subset F = acl_\sigma(F) \subset K$, let $\bar{a}$ be a tuple in K which is independent from F over E, and let S be a set of realisations of a set of types of SU-rank 1 over E.

(1) If $tp(\bar{a}/E)$ is modular, then so is $tp(\bar{a}/F)$.
(2) S is modular if and only if all types realised in S are modular.
(3) If $\mathrm{SU}(\bar{a}/E) = 1$ and $tp(\bar{a}/F)$ is modular, then $tp(\bar{a}/E)$ is modular.

Proof. (1) Let $\bar{b}$ be a finite set of realisations of $tp(\bar{a}/F)$, and let $\bar{c}$ be a finite tuple of elements of K. By modularity, $\bar{b}$ is independent from $acl_\sigma(F\bar{c})$ over $D = acl_\sigma(E\bar{a}) \cap acl_\sigma(F\bar{c})$. This implies that $\bar{b}$ is independent from $acl_\sigma(F\bar{c})$ over $acl_\sigma(FD) \subseteq acl_\sigma(F\bar{b}) \cap acl_\sigma(F\bar{c})$, and shows that $tp(\bar{a}/F)$ is modular.

(2) One direction is clear: if S is modular and $P \subset S$, then P is modular. For the other direction, assume that this is not true, and let n be minimal such that there are $\bar{a}_1, \ldots, \bar{a}_n \in S$, a tuple $\bar{b}$ in K and $C = acl_\sigma(E, \bar{a}_1, \ldots, \bar{a}_n) \cap acl_\sigma(E\bar{b})$, with $(\bar{a}_1, \ldots, a_n)$ and $\bar{b}$ not independent over C.

Note that, by minimality of n and because all tuples have SU-rank 1, we have that the elements $\bar{a}_1, \ldots, \bar{a}_n$ are independent over E. Moreover, the types $tp(\bar{a}_i/E)$ are pairwise non-orthogonal: indeed, assume by way of contradiction that $tp(\bar{a}_n/E)$ is orthogonal to $tp(\bar{a}_1/E)$. By minimality of n and transitivity of forking, we have that $(\bar{a}_1, \ldots, \bar{a}_{n-1})$ and $\bar{b}$ are independent over $C' = acl_\sigma(E, \bar{a}_1, \ldots, \bar{a}_{n-1}) \cap acl_\sigma(E\bar{b})$, and that $\bar{a}_n$ and $\bar{b}$ are not independent over $(C', \bar{a}_1, \ldots, \bar{a}_{n-1}) = (E, \bar{a}_1, \ldots, \bar{a}_{n-1})$. Hence $C = C'$, and $\bar{a}_n \in acl_\sigma(E, \bar{a}_1, \ldots, \bar{a}_{n-1}, \bar{b}) \setminus acl_\sigma(E, \bar{a}_1, \ldots, \bar{a}_{n-1})$. Since $tp(\bar{a}_n/E)$ is orthogonal to $tp(\bar{a}_1/E)$, we get that $\bar{a}_n \in acl_\sigma(E, \bar{a}_2, \ldots, \bar{a}_{n-1}, \bar{b})$, which contradicts the minimality of n.

By definition and because $\mathrm{SU}(\bar{a}_i/E) = 1$, this means that for each $i \geq 2$ there is F_i containing E and independent from $\bar{a}_i$ over E, such that $acl_\sigma(F_i\bar{a}_i) \setminus F_i$ contains a realisation $\bar{a}'_i$ of $tp(\bar{a}_1/E)$. Moving the F_i's by an E-automorphism, we may choose them such that $(F_2, \ldots, F_m)$ is independent from $(\bar{a}_1, \ldots, \bar{a}_n, \bar{b})$ over E. Setting $F = acl_\sigma(F_2, \ldots, F_m)$ and using 5.16, we then have $acl_\sigma(F, \bar{a}_1, \ldots, \bar{a}_n) \cap acl_\sigma(F\bar{b}) = acl_\sigma(FC)$, but $(\bar{a}_1, \ldots, \bar{a}_n)$ is not independent from $\bar{b}$ over $acl_\sigma(FC)$.

As each $\bar{a}_i$ is equi-algebraic over F with the realisation $\bar{a}'_i$ of $tp(\bar{a}_1/E)$, we get that:

— $acl_\sigma(F, \bar{a}_1, \bar{a}'_2, \dots, \bar{a}'_n) = acl_\sigma(F, \bar{a}_1, \dots, \bar{a}_n)$,
— $\mathrm{SU}(\bar{a}_1, \dots, \bar{a}_n/F) = n = \mathrm{SU}(\bar{a}_1, \bar{a}'_2, \dots, \bar{a}'_n/F) = \mathrm{SU}(\bar{a}_1, \bar{a}'_2, \dots, \bar{a}'_n/E)$.

Therefore (by transitivity of independence), we get that

($*$): F and $(\bar{a}_1, \bar{a}'_2, \dots, \bar{a}'_n, \bar{b})$ are independent over E.

Hence, letting $D = acl_\sigma(E, \bar{a}_1, \bar{a}'_2, \dots, \bar{a}'_n) \cap acl_\sigma(E\bar{b})$, we have (by 5.16)

$$acl_\sigma(F, a'_2, \dots, \bar{a}'_n) \cap acl_\sigma(F\bar{b}) = acl_\sigma(FD) = acl_\sigma(FC).$$

By modularity of $tp(\bar{a}_1/E)$, we also have that $(\bar{a}_1, \bar{a}'_2, \dots, \bar{a}'_n)$ and $\bar{b}$ are independent over D, and by ($*$), this gives that they are independent over $acl_\sigma(FD)$. But, since each $\bar{a}'_i$ is equi-algebraic with $\bar{a}_i$ over F, we have that $\bar{a}_1, \bar{a}'_2, \dots, \bar{a}'_n$ and $\bar{b}$ are not independent over $acl_\sigma(FC) = acl_\sigma(FD)$: this gives us the desired contradiction.

(3) Assume that $tp(\bar{a}/F)$ is modular. Note that if φ is an E-automorphism of K, then $\varphi(tp(\bar{a}/F))$ is also modular. Let $\bar{a}_1, \dots, \bar{a}_n$ be realisations of $tp(\bar{a}/E)$, $\bar{b}$ a tuple of elements of K, and $C = acl_\sigma(E\bar{a}_1, \dots, \bar{a}_n) \cap acl_\sigma(E\bar{b})$. For each i, let F_i be such that $tp(\bar{a}_i, F_i/E) = tp(\bar{a}, F/E)$; then each $tp(\bar{a}_i/F_i)$ is modular. Using (1), and moving the F_i by some E-automorphism of K, there is F' independent from $(\bar{a}_1, \dots, \bar{a}_n, \bar{b})$ over E, such that $tp(\bar{a}_i/F')$ is modular for $i = 1, \dots, n$. By 5.16, we have $acl_\sigma(F'\bar{a}_1, \dots, \bar{a}_n) \cap acl_\sigma(F'\bar{b}) = acl_\sigma(F'C)$. By (2), we get that $(\bar{a}_1, \dots, \bar{a}_n)$ and $\bar{b}$ are independent over $acl_\sigma(F'C)$. Since F' is independent from $(\bar{a}_1, \dots, \bar{a}_n, \bar{b})$ over E, this implies that $(\bar{a}_1, \dots, \bar{a}_n)$ is independent from $\bar{b}$ over C and therefore that $tp(\bar{a}/E)$ is modular.

5.18. **Corollary**. Let p and q be types over algebraically closed sets, which are of SU-rank 1, and are non-orthogonal. Then p is modular if and only if q is modular.

Proof. Let p' and q' be non-forking extensions of p and q to some set $A = acl_\sigma(A)$ containing the sets over which p and q are defined, and such that p' is non-almost-orthogonal to q'. Use 5.17.

5.19. **Non-example**. Let $E = acl_\sigma(E) \subset K$, let $\bar{a}$ be a tuple, and assume that $\mathrm{SU}(\bar{a}/E) \geq \omega$. We claim that $tp(\bar{a}/E)$ is not modular.

Indeed, we know that some element of the tuple $\bar{a}$, say a_1, is transformally transcendental over E. Take $\bar{b}$ realising $tp(\bar{a}/E)$ and independent from $\bar{a}$ over E, and let c be transformally transcendental over $acl_\sigma(E\bar{a}\bar{b})$, let $d = a_1c + b_1$. Then certainly $(\bar{a}, \bar{b})$ and (c, d) are not independent over E. Since $d = a_1b + b_1$, we have that (c, d) is independent from $(\bar{a}, \bar{b})$ over $acl_\sigma(Ea_1b_1)$, and so it is enough to show that (a_1, b_1) and (c, d) are not independent over $C = acl_\sigma(Ea_1b_1) \cap acl_\sigma(Ecd)$.

We claim that the canonical base of $tp(c, d/Ea_1b_1)$ contains a_1b_1. Indeed, let (c', d') be a realisation of $tp(c, d/Ea_1b_1)$, independent from (a_1, b_1, c, d) over Ea_1b_1. Then a_1, b_1, c, c' are independent over E. However (a_1, b_1) belongs to the field generated by (c, d, c_1, d_1). As (a_1, b_1) does not belong to $acl_\sigma(Ecd)$, this implies that (a_1, b_1) and (c, d) are not independent over $C = acl_\sigma(Ea_1b_1) \cap acl_\sigma(Ecd)$.

5.20. **Sets of SU-rank** 1. Let us again concentrate on sets S of SU-rank 1, defined over E. Because all our tuples have SU-rank 1, we get a pre-geometry on S, where the closure operator is simply $acl(E, -)$: given $A \subset S$ and $b \in S$,

either $b \in acl(E, A)$, or b is independent from A over E. The exchange principle holds, and the SU-rank of a set is the dimension of this set, etc.

Definition. A SU-rank-1 type p over E is called *trivial* if whenever $\bar{a}_1, \ldots, \bar{a}_n, \bar{a}$ realise p, then either $\bar{a} \notin acl_\sigma(E, \bar{a}_1, \ldots, \bar{a}_n)$, or $\bar{a} \in acl_\sigma(E\bar{a}_i)$ for some i. In other words, if P is the set of realisations of p, then $acl_\sigma(EP) = \bigcup_{\bar{a} \in P} acl_\sigma(E\bar{a})$.

5.21. **Exercise 14**. Show that a trivial type is modular.

5.22. **Some additional properties of modular types in models of ACFA**.

(1) If the type p is non-orthogonal to a modular type of SU-rank 1, then p is non-almost-orthogonal to a (modular) type of SU-rank 1.
(2) If p is a non-trivial modular type of SU-rank 1, then p is non-orthogonal to the generic of a group of SU-rank 1 defined over the same set as p (see the definition of generic in the next chapter).

§6. Groups, generic types, stabilisers. In this section, contrary to my promise, I will use some results on simple theories. You may very well replace everywhere "simple", or "supersimple", by complete theory extending ACFA. The notion of generic is meant to be the analogue of a generic of an algebraic group (so, generic in the sense defined in 1.10). A good reference for generics and stabilisers in simple theories is Pillay's paper [16]. But see also Wagner's book [19].

6.1. **Generics in groups**. Let G be a group (maybe with extra structure), whose theory is simple [Or: let G be a group definable in some model of ACFA]. We call a type p over some set $E = acl(E)$ a *generic type of* G, if p is realised in G, and whenever $a \in G$ and b realising p are independent over E, then $b \cdot a$ is independent from a over E. An element of G is *generic over* E if it realises a generic type over E.

Let H be a definable subgroup of G, let $a \in G$, consider the coset $a \cdot H$ and let $E = acl(E)$ be a set over which $a \cdot H$ is defined. We say that b is a *generic of the coset* $a \cdot H$ *over* E if $b \in a \cdot H$ and whenever $h \in H$ is independent from b over E, then $b \cdot h$ is independent from h over E.

Some facts.

(1) Generics exist. A non-forking extension of a generic type is generic.
(2) Assume that $tp(b/E)$ is generic, and let $a \in G$ be independent from b over E. Then $a \cdot b$ is independent from a over E, and $a \cdot b$ and $b \cdot a$ realise generic types over E. (The definition described a generic element of G in terms of its action on G by multiplication on the left. This shows that it can be defined also in terms of the action by multiplication on the right, and that a "left" generic is also a "right" generic.)

Below we will give some examples illustrating this notion. First we need some definitions from algebraic geometry.

6.2. **Projective space, projective varieties**. Let n be an integer, and consider the set of lines through the origin O in affine $n+1$-space $\mathbb{A}^{n+1}(\Omega)$. This set can be viewed as the set of equivalence classes of $\mathbb{A}^{n+1}(\Omega) \setminus O$ for the

equivalence relation

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff \exists \lambda \neq 0 \bigwedge_{i=0}^{n+1} x_i = \lambda y_i.$$

We denote this set by $\mathbb{P}^n(\Omega)$, and call it the projective n-space. The equivalence class of $(x_0, \dots, x_n)$ is usually denoted by $(x_0 : \cdots : x_n)$.

If $F(x_0, \dots, x_n)$ is a homogeneous polynomial over Ω, i.e., for some d all monomials appearing in F have total degree equal to d, then the equation $F(x_0, \dots, x_n) = 0$ is compatible with the equivalence relation, and defines a subset of $\mathbb{P}^n(\Omega)$. The topology whose closed sets are finite intersections of sets of this form, is called the Zariski topology.

Note that we can view $\mathbb{P}^n(\Omega)$ as the union of $n+1$ copies of affine n-space. Indeed, for $i = 0, \dots, n$, define

$$U_i = \{(x_0 : \cdots : x_n) \mid x_i \neq 0\}.$$

Then the map $f_i : (x_1, \dots, x_n) \mapsto (x_1 : \cdots : x_{i-1} : 1 : x_i : \cdots : x_n)$ defines a bijection between $\mathbb{A}^n(\Omega)$ and U_i. Moreover, $\mathbb{P}^n(\Omega) = \bigcup_{i=1}^n U_i$. Each U_i is open for the Zariski topology, and the maps f_i are homeomorphisms (for the Zariski topology on $\mathbb{A}^n(\Omega)$ and the induced topology on U_i).

Closed subsets of projective n-space are called projective sets. If X is closed and irreducible (i.e., for each i, $U_i \cap X$ is a variety), then we call X a projective variety. One can show that the product of two projective varieties is a projective variety.

Morphisms between projective varieties are defined locally using the covering by affine spaces.

6.3. **Algebraic groups.**

We say that G is an *algebraic group* if G is an open subset of a projective variety, and we have a group operation $G \times G \to G$ which is an morphism, i.e., is everywhere defined, and is locally defined by rational functions. We also require that the inverse map $G \to G$ is a morphism.

Here are some examples:

— The additive group, usually denoted $\mathbb{G}_a$ to distinguish it from the affine line $\mathbb{A}$ (with no structure). It is an open subset of $\mathbb{P}^1$.

— The multiplicative group $\mathbb{G}_m$ (so $\mathbb{G}_m(K) = K \setminus \{0\}$).

— Also, some projective group varieties (i.e., closed for the Zariski topology), which are called *abelian varieties*. Some examples are elliptic curves, and also certain groups of the form $\mathbb{C}^n/\Lambda$, where Λ is a $2n$-dimensional lattice subgroup of $\mathbb{C}^n$ generating the $\mathbb{R}$-vector space $\mathbb{C}^n$.

6.4. **Some elementary facts about algebraic groups**. We did not require in our definition that G be irreducible (by which I mean, that the Zariski closure of G in the projective space we are working in, is a variety).

If G is not irreducible, then one can verify that the irreducible components of G are disjoint, so that there is a unique irreducible component of G, denoted G^0 and called the *connected component of* G, which contains the identity element e of G. One has $[G : G^0] < \infty$.

Let G be an algebraic group, and H a subgroup of G, $\bar{H}$ its Zariski closure. Then $\bar{H}$ is also an algebraic group.

6.5. **Examples of generics**. We let K be an algebraically closed field, sufficiently saturated, and G an algebraic group defined over some subfield E of K.

The first thing to remark, is that a generic of $G(K)$ for the theory ACF of algebraically closed fields, is simply a generic in the sense of algebraic geometry. This is fairly immediate from the definition: let $d = dim(G)$, assume that g is a generic of G, independent from $h \in G$ over E. We know that $g \cdot h \in E(g, h)$, and (using the inverse map), that $g \in E(g \cdot h, h^{-1}) = E(g \cdot h, h)$. Hence g and $g \cdot h$ are equi-algebraic over $E(h)$. This implies

$$tr.deg(g \cdot h/E(h)) = tr.deg(g/E(h)) = d \leq tr.deg(g \cdot h/E) \leq d = dim(G),$$

so that equality holds and $g \cdot h$ is independent from h over E, as desired.

Let us now assume that K is a model of ACFA, sufficiently saturated, and let H be a definable subgroup of $G(K)$, defined also over $E = acl_\sigma(E)$. Then the σ-closure $\tilde{H}$ of H is a σ-closed subgroup of $G(K)$. Thus there is a natural notion of generic for H: an element $g \in H$ is generic if and only if $I_\sigma(g/E) = I_\sigma(\tilde{H}/E)$. Using the description of generics of algebraic groups, one can show (easily if $\mathrm{SU}(H) < \omega$, with a little more work in the general case) that this definition is the correct one. Furthermore, that $[\tilde{H} : H] < \infty$, so that a generic of H is also a generic of $\tilde{H}$.

One interesting consequence of elimination of imaginaries, is the following: let $\tilde{H}^0$ be the connected component of $\tilde{H}$ (i.e., the irreducible component in the sense of the σ-topology which contains the identity element). Then both $\tilde{H}$ and $\tilde{H}^0$ are defined over E. The cosets of $\tilde{H}^0$ in $\tilde{H}$ are then imaginary elements, and algebraic over E (since $[\tilde{H} : \tilde{H}^0] < \infty$). By elimination of imaginaries, they are defined over E.

6.6. **Lemma**. Let G be a group, H a definable subgroup of G, defined over some $E = acl(E)$, and $g \in G$ a generic of G over E. Then g is a generic of $g \cdot H$ (over $C = E \cup \bar{c}$, where $\bar{c}$ is the code of $g \cdot H$).

Proof. Let h be a generic of H over Eg. We claim that $g' = g \cdot h$ is a generic of $g \cdot H$ over Eg. Indeed, let $h_1 \in H$ be independent from g' over Eg. Then $g' \cdot h_1 \in g \cdot H$, and we need to show that h_1 and $g' \cdot h_1$ are independent over Eg. But, $g' \cdot h_1$ is equi-algebraic with $h \cdot h_1$over Eg, and it is therefore enough to show that h_1 and $h \cdot h_1$ are independent over Eg, which follows because h is a generic of H over Eg. As $C \subset acl(Eg)$, this implies that g' is a generic of $g \cdot H$ over C.

By genericity of g, we know that g' and h are independent over E, so that h is also a generic of H over Eg'. From $g \cdot H = g' \cdot H$ and the previous step, we deduce that g is a generic of $g\dot{H}$ over C.

6.7. **Stabilisers**. Let G be a group (maybe with extra structure), whose theory is simple, let p be a type over $E = acl(E)$. Assume that the independence theorem is satisfied over E: i.e., given a and b independent over E, and any two non-forking extensions p_1 to (E, a) and p_2 to (E, b) of some type p over E, $p_1 \cup p_2$

extend to some type p' over (E, a, b) which does not fork over E. [Or: let G be a group definable in a model of ACFA.]

We define $S(p)$ to be the set of elements $h \in G$, such that **there exists** a realisation g of p such that $h \cdot g$ realises p, and h is independent from g and from $h \cdot g$ over E.

One then defines $Stab(p) = S(p) \cdot S(p)$. By the independence theorem over E, we have that if h_1 and h_2 are independent elements of $S(p)$, then $h_1 \cdot h_2 \in S(p)$. This will imply that $Stab(p)$ is a subgroup of G, with generics in $S(p)$. One can show that $Stab(p)$ is ∞-definable.

6.8. **Example**. Let K be a model of ACFA, G an algebraic group defined over $E = acl_\sigma(E)$, and let p be a type over E, $X \subseteq G(K)$ its set of realisations. By definition, if $h \in S(p)$, then there are $g, g_1 \in X$ such that $g \downarrow_E h$, $g_1 \downarrow_E h$, and $h \cdot g = g_1$. In particular, $h = g_1 \cdot g^{-1}$, so that $h \in X \cdot X^{-1}$. The requirement that h be independent from g and from g_1 over E then implies that necessarily $\mathrm{SU}(h/E) \leq \mathrm{SU}(g/E) = \mathrm{SU}(g_1/E)$.

Let Y be the σ-closure of X. Then Y is irreducible, and g, g_1 belong to Y. This implies in particular that $S(p) \subset Stab(Y) =_{\mathrm{def}} \{h \in G(K) \mid hY = Y\}$. Note that $Stab(Y)$ is clearly a subgroup of $G(K)$, and is quantifier-free definable, so that it is σ-closed. If I am not mistaken, one can then show that $Stab(p)$ is the intersection of all definable subgroup of $Stab(Y)$ which are defined over E and have finite index in $Stab(Y)$.

6.9. **Remarks/Exercise 15**. Let us now assume that p has a unique non-forking extension to any set containing E, and let P be the set of realisations of p. [This hypothesis is verified for instance when p is definable over E and T is stable.]

(1) Then $Stab(p) = S(p)$: this is because the quantifier "there exists" in the definition of $S(p)$ can be replaced by the quantifier "for all".

(2) If $E' \supset E$, and p' is the non-forking extension of p to E', then $Stab(p) = Stab(p')$.

(3) Let $h \in E$. Then $h \in S(p) \iff h \cdot P = P$.

No completion of ACFA is stable. However, in the language of "local stability theory", all quantifier-free formulas are stable. We will see below some of the consequences this has.

6.10. **Proposition**. Let $E = acl_\sigma(E) \subset K$, K a sufficiently saturated model of ACFA.

(1) Let p be a type over E, and assume that whenever F contains E, then p has a unique non-forking extension to F. Then p is definable over E, i.e., given a formula $\varphi(\bar{x}, \bar{y})$, there is a formula (over E) $d_\varphi(\bar{y})$ which defines in K the set of $\bar{c}$ such that $\varphi(\bar{x}, \bar{c})$ belongs to the unique-non-forking extension of p to K.

(2) Let p be a quantifier-free type over E. Given a quantifier-free formula $\varphi(\bar{x}, \bar{y})$, there is a quantifier-free formula (over E) $d_\varphi(\bar{y})$ which defines in K the set of $\bar{c}$ such that $\varphi(\bar{x}, \bar{c})$ belongs to some/all non-forking extensions of p to K.

Proof. (1) is well-known, but we will give the proof. Assume by way of contradiction that p is not definable, i.e., that there is some formula $\varphi(\bar{x}, \bar{y})$ such that the set X of tuples $\bar{c}$ of K such that $\varphi(\bar{x}, \bar{c})$ belongs to the unique non-forking extension of p to K is not definable. Then, for every $\mathcal{L}(E)$-formula $\psi(\bar{y})$, there are $\bar{c}_1 \in X$, $\bar{c}_2 \notin X$ which both satisfy $\psi(\bar{y})$. By compactness, there are $\bar{c}_1, \bar{c}_2$ in K, realising the same type over E, and such that $\bar{c}_1 \in X$, $\bar{c}_2 \notin X$. Let f be an automorphism of K which leaves E fixed and sends $\bar{c}_1$ to $\bar{c}_2$. If q is the unique non-forking extension of p to K, then $f(q)$ is also a non-forking extension of p to K, and so must equal q: but this contradicts the fact that $\varphi(\bar{x}, \bar{c}_1) \in q$, $\varphi(\bar{x}, \bar{c}_2) \notin q = f(q)$.

We now sketch a proof of (2). The crucial point is the following observation: since quantifier-free types correspond exactly to descriptions of the isomorphism type of the "difference field generated by", it follows that if $F = acl_\sigma(F)$ contains E, then there is a unique quantifier-free type q over F which extends p and is such that whenever $\bar{a}$ realises q, then $\bar{a}$ is independent from F over E.

This implies that, given $p = qftp(\bar{a}/E)$ and $\bar{c}$ independent from $\bar{a}$ over E, we have:

$$qftp(\bar{a}/E) \cup qftp(\bar{c}/E) \cup \Sigma(\bar{x}, \bar{y}) \vdash qftp(\bar{a}, \bar{c}/E),$$

where $\Sigma(\bar{x}, \bar{y})$ is the set of quantifier-free formulas over E expressing that the tuples $\bar{x}$ and $\bar{y}$ are independent over E. The proposition follows by compactness.

6.11. **Remarks**. (1) Let $E = acl_\sigma(E)$, $\bar{a}$ a tuple in K. Let C be the set of codes of all (quantifier-free) definitions of $qftp(\bar{a}/E)$. Then certainly $tp(\bar{a}/E)$ does not fork over C. Moreover, if $D \subset E$ and $tp(\bar{a}/E)$ does not fork over D then $acl_\sigma(D) \supset C$. Hence, we are getting that for quantifier-free types, our definition of a canonical base agrees with the classical one.

(2) Let G be a group definable in K by quantifier-free formulas (over some $E = acl_\sigma(E)$), and assume in addition that the group operation and the inverse map are piecewise definable by terms of the language $\{+, -, \cdot, ^{-1}, \sigma, \sigma^{-1}, e(e \in E)\}$, so that if $a, b \in G$, then $a \cdot b \in cl_\sigma(E, a, b)$ and $a^{-1} \in cl_\sigma(E, a)$. [By the multiplication being piecewise defined, we mean that there is a definable finite partition of G^2, and that on each piece of this partition multiplication is defined by a term.] If p is a quantifier-free type over E realised in G, then we may also define $Stab(p)$ to be the set of elements b of G such that whenever a realises p and is independent from b over E, then $b \cdot a$ realises p and is independent from b over E. All remarks made in 6.9 go through to this particular case. Examples of such groups are algebraic groups defined over E.

6.12. **Theorem**. Let G be a group, quantifier-free definable in a model K of ACFA, and assume that G is modular, and the group operation and the inverse map are piecewise defined by terms of the language $\{+, -, \cdot, ^{-1}, \sigma, \sigma^{-1}, e(e \in E)\}$. If X is a quantifier-free definable subset of G, then X is a Boolean combination of quantifier-free definable subgroups of G. Furthermore, if G is defined over $E = acl_\sigma(E)$, then so are these subgroups.

Proof. We will fist show that if p is a quantifier-free type defined over some $A = acl_\sigma(A)$ containing E, then the set P of realisations of p is contained in a coset of some quantifier-free definable subgroup S of G, and p is the generic type

of this coset. Without loss of generality, we will assume that A is the algebraic closure (over E) of the canonical base of p.

Define $S = Stab(p)$, the set of elements $b \in G$, such that there is $a \in P$, independent from b over A and such that $b \cdot a \in P$.

Claim. S is quantifier-free definable (over A).

Let $a \in P$ and consider $I_\sigma(a/A)$. Then $I_\sigma(a/A)$ completely determines p: let $b \in G$. Then

$$I_\sigma(b/A) = I_\sigma(a/A) \iff b \in P.$$

Let $F(X)$ be a tuple of difference polynomials over A generating the σ-ideal $I_\sigma(a/A)$ (as a σ-ideal).

By the piecewise quantifier-free definability of the group operation, there is a quantifier-free formula $\psi(y, x)$ such that, if $a \in P$ is independent from $g \in G$ over A, then

$$K \models \psi(g, a) \iff F(g \cdot a) = 0.$$

Let φ be the formula $F(x) = 0 \wedge \psi(y, x)$. Then S is defined by the formula $d_\varphi(y)$: Let $g \in G$. Then g satisfies $d_\varphi(y)$ if and only if $F(x) = 0 \wedge \psi(g, x)$ belongs to the non-forking extension of p to $A \cup g$, if and only if whenever $a \in P$ is independent from g over A, then $b = g \cdot a$ satisfies $F(x) = 0$. Note that because b and a are equi-algebraic over $acl_\sigma(A, g)$, this implies that b belongs to P and is independent from g over A (because b cannot satisfy "more" equations than $F(x)$ over $acl_\sigma(A, g)$).

[In the classical stable (non-superstable) case, one cannot get S to be definable, only ∞-definable. There the defining formulas are of the form $\forall \bar{z}\, d_\varphi(\bar{z}) \leftrightarrow d_{\varphi^*}(\bar{z}, y)$, where $\varphi^*(\bar{z}, y, x) = \varphi(\bar{z}, y \cdot x)$.]

Fix $a \in P$, and g a generic of G over Aa. Then $b = g \cdot a$ is a generic of G over Aa, and is independent from a over A. Let $G_0 \prec G$ contain A, g, let P_0 be the set of realisations of the non-forking extension of p to G_0, and Q_0 the set of realisations of the non-forking extension q_0 of $qftp(b/Ag)$ to G_0. Then $Q_0 = g \cdot P_0$. If $\tau \in Aut(G_0/A)$, then τ also acts on the set of formulas over G_0. By abuse of notation, if U is an (∞-) definable over G_0 subset of G, we will denote by $\tau(U)$ the (∞-) definable subset of G defined by applying τ to the formulas defining U.

Claim. Let $\tau \in Aut(G_0/A)$. Then $\tau(Q_0) = Q_0 \iff \tau(g \cdot S) = g \cdot S$.

Since p is definable over A, we have that $\tau(P_0) = P_0$, and $\tau(S) = S$. Hence $\tau(Q_0) = Q_0 \iff \tau(g) \cdot P_0 = g \cdot P_0 \iff g^{-1} \cdot \tau(g) \cdot P_0 = P_0 \iff g^{-1} \cdot \tau(g) \in S \iff \tau(g \cdot S) = g \cdot S$.

By elimination of imaginaries of ACFA, we get that the codes of Q_0 and of $g \cdot S$ are equi-algebraic over A. Let $\bar{c}$ be the code of $g \cdot S$. Because g is a generic of G over A, and S is a subgroup of G defined over A, we get that g is a generic of $g \cdot S$ (see Lemma 6.6), and that $\bar{c}$ is equi-algebraic with the canonical base of $qftp(g/acl_\sigma(A\bar{c}))$, so that $\mathrm{SU}(g/A\bar{c}) = \mathrm{SU}(S)$. By the claim, we also get that the canonical base of q_0 is equi-algebraic over A with $\bar{c}$. Since q_0 is the non-forking extension of $qftp(b/acl_\sigma(Ag))$ to G_0, it follows that $\bar{c}$ is equi-algebraic over A with $Cb(b/Ag)$. By modularity, we have:

$$acl_\sigma(A\bar{c}) = acl_\sigma(Ab) \cap acl_\sigma(Ag) \qquad (*)$$

Since g is a generic of G over Aa, we have that a is independent from g and from $b = g \cdot a$ over A, and therefore also over $A\bar{c}$ by $(*)$. Hence, using the symmetry of independence, we have:

$$\mathrm{SU}(P) = \mathrm{SU}(b/Ag) = \mathrm{SU}(b/A\bar{c}) = \mathrm{SU}(b/A\bar{c}a) = \mathrm{SU}(g/A\bar{c}a) = \mathrm{SU}(g/A\bar{c}) = \mathrm{SU}(S)$$

(The fourth equality is because b and g are equi-algebraic over $Aa \subset Aa\bar{c}$). Hence $\mathrm{SU}(P) = \mathrm{SU}(S)$. If $h \in S$ is independent from a over A, then $b = h \cdot a \in P$, and is independent from a and from h over A. Hence the generics of S are of the form $d \cdot e^{-1}$, for $d, e \in P$ independent over A. This implies that $Sd = Sa$ for all $d \in P$, and therefore that $P \subset Sa$. It remains to show that if b is a generic of Sa, then $b \in P$. Let b be a generic of Sa over A, and choose $d \in P$ independent from b over A. Then $Sd = Sa$, so that there is $h \in S$ such that $b = h \cdot d$. From $\mathrm{SU}(S) = \mathrm{SU}(b/A) = \mathrm{SU}(b/Ad) = \mathrm{SU}(h/Ad) \leq \mathrm{SU}(S)$, we deduce that h is independent from d over A, so that $h \cdot d \in P$ (by definition of S).

Hence the type p can be described as follows:

— x belongs to the coset Sa.

— If S' is a definable subgroup of G, and the coset $S'b$ is definable over A and strictly contained in Sa, then x does not belong to $S'b$.

Indeed, if $b \in Sa$ is **not** a generic of Sa, then the realisations of $qftp(b/A)$ are the generics of some $S'b$ strictly contained in Sa and defined over A. It follows, by compactness, that every formula is equivalent to a Boolean combination of formulas of the form "x belongs to a coset of some definable subgroup of G".

We will now show that S is in fact defined over E. By modularity, $tp(g/A\bar{c})$ is definable over $acl_\sigma(Eg)$, and since $g \cdot S$ is a coset of a group, this implies that $g \cdot S$ is also defined over $acl_\sigma(Eg)$. Hence so is $S = g^{-1} \cdot (g \cdot S)$, and we obtain that S is defined over $acl_\sigma(Eg) \cap A = E$.

§7. General results about models of ACFA. We state here some results without proofs. We are working in a model K of ACFA. Let us start with an easy one:

7.1. **Proposition**. Let ϕ be the identity if $char(K) = 0$, and the Frobenius automorphism $x \mapsto x^p$ if $char(K) = p > 0$. Let $m \geq 1$ and n be integers. Then the difference field $(K, \sigma^m\phi^n)$ is also a model of ACFA.

Proof. See below exercise 7.19.

7.2. **The dichotomy theorem**. Using Theorem 4.1, we obtain that, in positive characteristic the fields $Fix(\sigma^m\phi^n)$ are pseudo-finite fields. We will refer to these fields as *the fixed fields of* K.

Assume that $(m, n) = 1$ (or $m = 1, n = 0$), let $F = Fix(\sigma^m\phi^{-n})$. One can then show that $SU(F) = 1$. From this, it follows that if $S \subset F$ is definable and infinite, then $F = a_1S + a_2S + \cdots + a_nS$ for some elements $a_1, \ldots, a_n \in K$. This implies that all non-algebraic 1-types containing the formula $\sigma(x) = x$ [or $\sigma^m(x) = \phi^n(x)$ if the characteristic is positive] are non-orthogonal; since the field F is certainly non-modular, and has no induced structure from K, this implies the following:

A type p which is non-orthogonal to one of the formulas $\sigma^m(x) = \phi^n(x)$ cannot be modular.

In fact, the converse is also true:

Theorem. Let K be a model of ACFA, and let p be a type of SU-rank 1 over $E = acl_\sigma(E) \subset K$. Then p is modular if and only if p is orthogonal to all formulas $\sigma^m(x) = \phi^n(x)$.

If $char(K) = 0$, then p is modular if and only if p has a unique non-forking extension to any set containing E.

7.3. **Discussion/Theorem**. □□□ In characteristic 0, we therefore get that modular types of SU-rank 1 are definable, and hence stable. Using proposition 5.9, one can then show that if a (finite SU-rank) formula $\varphi(\bar{x})$ is orthogonal to $\sigma(x) = x$ (i.e., to all types containing the formula $\sigma(x) = x$), then all types containing $\varphi(\bar{x})$ are stable and definable, the set S defined by φ is *stably embedded*, i.e., all subsets of S^m which are definable in K are definable with parameters from S, so that S with the structure induced from K is **superstable of finite U-rank and one-based**.

In characteristic $p > 0$, if a finite SU-rank formula is orthogonal to all formulas defining fixed fields, then the set it defines is also modular, but is usually not stable. □□□

7.4. For p a prime and q a power of p, consider the difference field $F_q = (\mathbb{F}_p^{alg}, \sigma_q)$, where $\sigma_q : x \mapsto x^q$. Let $\mathcal{U}$ be a non-principal ultrafilter on the set Q of all prime powers.

Theorem (Hrushovski [7], Macintyre [8]). The difference field $\prod_{q \in Q} F_q/\mathcal{U}$ is a model of ACFA.

7.5. One can then show that the theory ACFA coincides with the set of sentences true in all but finitely many of the difference fields F_q. This is the analogue of Ax's theorem, which states that the theory of pseudo-finite fields coincides with the set of sentences true in almost all finite fields. Hrushovski's proof gives more: it gives estimates on the size of finite definable sets. Before stating his result, let me remark that one can replace the scheme of axioms (3) of the theory ACFA by the apparently weaker scheme of axioms

(3') If U and V are varieties **of dimension** d defined over K, with $V \subseteq U \times U^\sigma$, such that the projections of V to U and to U^σ are generically onto, then there is a tuple $\bar{a}$ in K such that $(\bar{a}, \sigma(\bar{a})) \in V$.

Let me explain why this (together with axiom schemes (1) and (2)), will give us an axiomatisation of ACFA. The proof that every difference field K embeds in a model of ACFA actually shows that every difference field embeds in a model L of ACFA, all of whose elements are **transformally algebraic over** K. This means that given a tuple $\bar{a} \in L$, there is an integer m such that $acl_\sigma(K\bar{a}) = K(\bar{a}, \ldots, \sigma^m(\bar{a}))^{alg}$. Hence, every particular instance of axiom (3) is implied by finitely many instances of axiom (3').

7.6. **Theorem** (Hrushovski). Let $F(\bar{X}, \bar{Z})$ and $G(\bar{X}, \bar{Y}, \bar{Z})$ be tuples of polynomials over $\mathbb{Z}$. There is a positive constant C with the following property:

For all prime p and power q of p, and tuple $\bar{c}$ in $\mathbb{F}_p^{alg}$, if the equations $F(\bar{X}, \bar{c}) = 0$ and $G(\bar{X}, \bar{Y}, \bar{c}) = 0$ define varieties U and V satisfying the requirements of axiom (3'), then

$$|Card(\{\bar{a} \in \mathbb{F}_p^{alg} \mid (\bar{a}, \bar{a}^q) \in V\}) - cq^d| \leq Cq^{d-1/2},$$

where

$$d = dim(U) = dim(V), \quad \text{and } c = [K(V) : K(U)]/[K(V) : K(U^\sigma)]_{\text{ins}}.$$

This theorem is a strengthening of a theorem of Lang-Weil for the number of points of varieties defined over finite fields: take U defined over $\mathbb{F}_q$, and V the intersection of the diagonal with $U \times U$. The above formula then gives you an estimate on the number of points of U with their coordinates in $\mathbb{F}_q$.

7.7. **Some applications of these theorems.** You may recall the proof of Ax that if V is a variety defined over $\mathbb{C}$, and $f : V \to V$ is a morphism which is injective on the set $V(\mathbb{C})$ of points of V with their coordinates in $\mathbb{C}$, then f defines a bijection of $V(\mathbb{C})$ (i.e., f is also surjective). This is done as follows: this statement will hold in $\mathbb{C}$ if and only if it holds in all algebraically closed fields of characteristic $p > 0$, if and only if it holds in all $\mathbb{F}_p^{alg}$, p a prime. So, let V be a variety and $f : V \to V$ a morphism, both defined over $\mathbb{F}_p^{alg}$. Then for some $q = p^m$, they are defined over $\mathbb{F}_q$. Thus, for every $n \geq 1$, f is a map $V(\mathbb{F}_{q^n}) \to V(\mathbb{F}_{q^n})$, is injective, and therefore also surjective since $V(\mathbb{F}_{q^n})$ is finite. Because $\mathbb{F}_p^{alg} = \bigcup_n \mathbb{F}_{q^n}$, we get that f defines a permutation of $V(\mathbb{F}_p^{alg})$.

Corollary. Let B be a group of finite SU-rank defined in a model K of ACFA, and assume that f is a definable endomorphism of B. Then

$$[B : f(B)] = Card(Ker(f)).$$

Proof. Without loss of generality, we may assume that K is countable. Let $\varphi(\bar{x}, \bar{u})$, $\psi(\bar{x}, \bar{y}, \bar{u})$ be $\mathcal{L}$-formulas and $\bar{b} \in K$ be such that $\varphi(\bar{x}, \bar{b})$ defines B and $\psi(\bar{x}, \bar{y}, \bar{b})$ defines the graph of f. By 7.4, the difference field K embeds into an ultraproduct $\prod_q F_q/\mathcal{U}$ of the difference fields F_q. Take a representative $(\bar{b}_q)_q$ of $\bar{b}$. Then for almost all q (in the sense of the ultrafilter $\mathcal{U}$), we have that $\varphi(\bar{x}, \bar{b}_q)$ defines a group B_q in F_q, and $\psi(\bar{x}, \bar{y}, \bar{b}_q)$ defines an endomorphism f_q of B_q. Note also that because B is of finite SU-rank, there is an integer m such that every element $\bar{a}$ of B satisfies $\sigma^m(\bar{a}) \in cl_\sigma(\bar{b})(\bar{a}, \ldots, \sigma^{m-1}(\bar{a}))^{alg}$. Hence the same is also true for almost all B_q. By 7.6, the B_q are therefore finite, and we obtain trivially that

$$[B_q : f_q(B_q)] = Card(Ker(f_q)).$$

Thus the same holds in K. Note that $Ker(f)$ is infinite if and only if the size of the $Ker(f_q)$ is unbounded.

7.8. **Application to families of finite simple groups.** With the exception of the sporadic finite simple groups and the alternating groups A_n, the finite simple groups are members of infinite families. Some of these families are of the form $G(\mathbb{F}_q)$ for some linear algebraic group G (for instance $SL_n(\mathbb{F}_q)$). Hence looking at $G(F)$ for F a pseudo-finite field, one gets uniformity results on the family $G(\mathbb{F}_q)$, q a prime power.

Some of these families however do not originate directly from a simple algebraic group, but their definition involves some automorphism of the field $\mathbb{F}_q$. They are the so-called "twisted finite simple groups". And they become definable in the structure $(\mathbb{F}_p^{alg}, \sigma_q)$. Using 7.4, one then also gets uniformity results for these families.

Typical examples of uniformity results: we know that in a finite simple group H, every non-trivial conjugacy class X generates the whole group. The uniformity gives a bound on the number N such that $H = (X \cdot X^{-1})^N$.

7.9. **The Jacobi conjecture for difference fields**.

Let $n \geq 1$, let $u_1(X_1, \ldots, X_n), \ldots, u_n(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]_\sigma$ (K a difference field, and we will assume it is a model of ACFA). The equations

$$u_1(x_1, \ldots, x_n) = \cdots = u_n(x_1, \ldots, x_n) = 0$$

define a σ-closed subset of K^n, and some of the irreducible components of this set will be of finite SU-rank. If Y is an irreducible component of finite SU-rank of this set, let us define the *order of* Y as $Sup\{tr.deg(cl_\sigma(E\bar{a})/E) \mid \bar{a} \in Y\}$, where $E = acl_\sigma(E)$ is such that the elements $u_1, \ldots, u_n$ are defined over E. The Jacobi's conjecture gives an explicit bound H on the order of the irreducible components of finite SU-rank. This bound is defined as follows: for each k and i, define h_k^i to be the order of u_k when viewed as a difference polynomial in x_i (so, it equals m if $x_i^{\sigma^m}$ appears in u_k and $x_i^{\sigma^{m+1}}$ does not). One then sets

$$H = \max_{\theta \in Sym(n)} \sum_{k=1}^{n} h_k^{\theta(k)}.$$

Hrushovski uses the fact that if an irreducible σ-closet set Y has order d, then in a structure F_q, it will have approximately cq^d points for some fixed constant c. Thus the order of Y will be $lim_q \log_q(Card(Y(F_q))$. One uses this remark to reduce the Jacobi's conjecture to a problem about number of points in algebraic sets.

7.10. **Modular subgroups**. One can show that if one has an exact sequence

$$0 \to A \to B \to C \to 0$$

of definable groups (in a model K of ACFA), then B is modular [and stable] if and only if A and C are modular [and stable]. Hence the study of modular definable subgroups of an algebraic group reduces to the study of definable subgroups of simple algebraic groups, i.e., of $\mathbb{G}_a(K)$, $\mathbb{G}_m(K)$, or of a simple abelian variety.

In characteristic 0, one can show that **no** proper definable subgroup of $\mathbb{G}_a(K)$ is definable. Indeed, it is fairly easy to show that such a group is commensurable with one defined by an equation of the form $\sum_{i=0}^n a_i \sigma^i(x) = 0$, with $a_i \in K$ (recall that two definable groups G_1 and G_2 are *commensurable* if $[G_1 : G_1 \cap G_2]$ and $[G_2 : G_1 \cap G_2]$ are both finite). Furthermore the operator $\sum_{i=0}^n a_i \sigma^i$ can be written as a composition of operators of the form $\sigma - b$, and the sets defined by the equation $\sigma(x) - bx$ are non-orthogonal to the fixed field.

Let A be an abelian variety, defined over the fixed field F of the model K of ACFA. Then $\sigma(A) = A$, and therefore, if $f(T) = \sum_{i=0}^n a_i T^i \in \mathbb{Z}[T]$, then the

equation

$$f(\sigma)(x) = \sum_{i=0}^{n} [a_i]\sigma^i(x) = 0$$

defines a subgroup of $A(K)$. (Here, $[a_i]x$ denotes $x + \cdots + x$ a_i times). We will denote this group by $Ker(f(\sigma))$.

A beautiful result of Hrushovski states that in characteristic 0, $f(T)$ is relatively prime to all cyclotomic polynomials $T^m - 1$ if and only if $Ker(f(\sigma))$ is modular, and therefore stable. [He actually has a complete characterisation of the modular definable subgroups of an arbitrary abelian variety.]

A similar statement holds for definable subgroups of $\mathbb{G}_m(K)$: if $f(T) = \sum_i a_i T^i \in \mathbb{Z}[T]$, then the equation $\prod \sigma^i(x^{a_i}) = 1$ defines a subgroup of $\mathbb{G}_m(K)$ (denoted $Ker(f(\sigma))$), and this subgroup is modular if and only if $f(T)$ is relatively prime to all cyclotomic polynomials $T^m - 1$, $m \geq 1$.

7.11. **Application to the Manin-Mumford conjecture**.

The Manin-Mumford conjecture is a conjecture in number theory, of which various versions have been proved by various people. Here I will only state the version of which Hrushovski gives a proof using difference fields. It is weaker than the full Manin-Mumford conjecture, because of the restriction on the field of definition, but is stronger in the sense that the constant M below can be effectively computed from the data. If G is a group, let us denote by $Tor(G)$ the set of torsion elements of G. I will certainly not give the full proof, but will try to indicate the main steps of the proof and some of its ingredients.

Theorem. Let A be a commutative algebraic group defined over some number field k (= finite extension of $\mathbb{Q}$), and let X be a subvariety of A. Then

$$X \cap Tor(A) = \bigcup_{i=1}^{M} a_i + Tor(A_i),$$

where the A_i are group subvarieties of A. The number M is bounded above by $c\,deg(X)^e$, where c and e are constants depending on A, and $deg(X)$ is the degree of X given some embedding of A (and of X) in projective space.

7.12. **A first idea for a proof**. Show that there is $\sigma \in \mathcal{G}al(k^{alg}/k)$ and a functional equation $f(\sigma)(\bar{x}) = 0$ valid on $Tor(A)$ and such that: whenever K is a model of ACFA extending (k^{alg}, σ), then the equation $f(\sigma)(\bar{x}) = 0$ defines a modular subgroup of $A(K)$.

Assume that we have done that. Then:

(1) We get the qualitative version of the result, because of modularity. Indeed, let B be the subgroup of $A(K)$ defined by the equation $f(\sigma)(\bar{x}) = 0$. Then by the results we got above, $X \cap B$ is a Boolean combination of cosets of quantifier-free definable subgroups of B. We can therefore write $X \cap B$ as a finite union of sets of the form $(a + C) \setminus U$, where C is a σ-closed subgroup of B, irreducible as a σ-closed set, and U is a union of cosets which are strictly contained in $a + C$. The σ-closure of $(a + C) \setminus U$ equals $a + C$, and must also be contained in the σ-closed set $X \cap B$. This shows that $X \cap B$ is in fact a finite union of cosets of

definable subgroups of B. Write

$$X \cap B = \bigcup_{i=0}^{n} a_i + B_i.$$

Now, if $a_i + B_i$ intersects $Tor(A)$, then we may take $a_i \in Tor(A)$. Note also that $a_i + B_i \subset X$ implies that $a_i + A_i \subset X$, where A_i is the Zariski closure of the subgroup B_i of A, and therefore is an algebraic subgroup of A. Hence we have that $a_i + Tor(A_i) \subset X$, and this gives the result.

(2) If we have explicit bounds on the degree of f and the absolute values of its coefficients, then we get an explicit bound on the number of irreducible components of the σ-closed set $X \cap B$, and hence on the number M of cosets.

Unfortunately, this strategy needs to be slightly modified. First of all, the commutative algebraic group A may have a vector subgroup, i.e., an algebraic subgroup V which is isomorphic to $\mathbb{G}_a^n$ for some n. As we saw above, no definable subgroup of $\mathbb{G}_a^n(K)$ is modular. So the first step of the proof is to show that it is enough to prove the result for A/V, where V is the maximal vector subgroup of A. This is done using an easy algebraic result, and a more complicated model-theoretic one showing that if B is a definable subgroup of $A(K)$ which is such that $B/B \cap V$ is modular, then the intersection of B with any set is of a special form (see below 7.15). So, one reduces the proof of the theorem to the case where A has no algebraic subgroups isomorphic to $\mathbb{G}_a$ (such an algebraic group is called a *semi-abelian variety*).

Also, it turns out that finding explicit bounds on coefficients and degree of the equation is not effective. One bypasses this difficulty by looking first at $Tor_{p'}(A)$, the prime-to-p torsion subgroup of A, proving the desired result there, and then using another prime ℓ. This produces explicit but very ugly bounds on the number n of cosets.

More precisely: We get a bound for the number of cosets in $X \cap Tor_{p'}(A)$, and this bound only depends on the degree of X. Hence, it also works for $(a+X) \cap Tor_{p'}(A)$, for any $a \in Tor(A)$. Now one uses that $Tor_{p'}(A) + Tor_{\ell'}(A) = Tor(A)$. But there is definitely some work involved. For details, please see [6].

7.13. **Why do we need a bound on the coefficients of the equation?** Let $f(T) = \sum_{i=0}^{\ell} m_i T^i \in \mathbb{Z}[T]$. We are interested in the number of irreducible components of the σ-closed set $X \cap Ker(f(\sigma))$, and we can find a bound on this number as follows. We first look at the Zariski closed sets $Y = (X \times X^{\sigma} \times \cdots \times X^{\sigma^{\ell}})$ and $C = \{(x_0, \ldots, x_\ell) \in A^{\ell+1} \mid \sum_{i=0}^{\ell} m_i x_i = 0\}$. Then the number of irreducible components of $Y \cap C$ is bounded by $deg(X)^{\ell+1} deg(C)$, where the degree is computed via a certain embedding of A in projective space. Unfortunately, the degree of C will depend on the values of the $|m_i|$ (and increase if they do – of course), which means that already to know the number of irreducible components of $Y \cap C$, we need to know things about $f(T)$.

7.14. **Existence of the equation, and some bounds**. Here Hrushovski chooses a prime p of good reduction (for A). Grosso modo, this means that, reducing modulo p the equations defining A, one gets an algebraic group $\bar{A}$ defined over some finite field $\mathbb{F}_q$, and which resembles A. Moreover, let L_p be the

field generated over k by the elements of $Tor_{p'}(A)$. Then L_p is an unramified extension of the field k, i.e., reduction "mod p": $\mathcal{O}_k \to \mathbb{F}_q$ extends to a homomorphism $\mathcal{O}_{L_p} \to \mathbb{F}_p^{alg}$, and this homomorphism defines a 1-1 map on $Tor_{p'}(A)$ (with values in $Tor_{p'}(\bar{A})$).

The automorphism $x \mapsto x^q$ of $\mathbb{F}_p^{alg}$ lifts to an automorphism of L_p fixing k, and one takes for σ any automorphism of $\mathbb{Q}^{alg}$ extending this automorphism.

It then suffices to find the functional equation on $\bar{A}$ (because reduction mod p is injective on the torsion). Observing that if

$$0 \longrightarrow A_1 \longrightarrow A_3 \longrightarrow A_2 \longrightarrow 0$$

is a short exact sequence of (connected) commutative algebraic groups, then $Tor(A_3)$ contains $Tor(A_1)$ and projects into $Tor(A_2)$, reduces to finding such an equation (and bounds on its coefficients and degree) for each of the simple factors of $\bar{A}$: for the abelian ones, its existence and bound on the degree and absolute value of the coefficients are given by a result of Weil. For products of copies of $\mathbb{G}_m$, it is more or less $\sigma(x) - x^q$, and $\mathbb{G}_a(K)$ has no torsion elements, so we do not need to look at what happens in $\mathbb{G}_a(\mathbb{F}_p^{alg})$.

We have therefore taken care of the p'-torsion, and furthermore have shown that there is an effective bound on the number n such that

$$Tor_{p'}(A) \cap X = \bigcup_{i=1}^{n} a_i + Tor_{p'}(A_i)$$

for some algebraic subgroups A_i of A and elements $a_1, \ldots, a_n$. Take now another prime ℓ of good reduction. Proceeding as above, one gets an automorphism τ of $\mathbb{Q}^{alg}$, such that τ satisfies a functional equation $g(\tau)$ on $Tor_{\ell'}(A)$, and therefore also on $Tor_p(A)$ (the p-component of $Tor(A)$). Let $M_p = k(Tor_p(A))$. Then a result of Serre tells us that $L_p \cap M_p$ is a **finite** extension of k, say of degree m. Hence there is an automorphism ρ of L_pM_p, which extends σ^m on L_p and τ^m on M_p. Note the following: write $f(T) = a\prod(T - \alpha_i)$, where $a \in \mathbb{Z}$, the α_i are in $\mathbb{C}$. Then $Ker(f(\sigma))$ is modular if and only if none of the α_i is a root of unity. Also, let $h(T) = \prod(T - \alpha_i^m)$, and choose $b \in \mathbb{Z}$ such that $bh(T) \in \mathbb{Z}[T]$; then $bh(\sigma^m)$ vanishes on $Tor_{p'}(A)$, and is relatively prime to all cyclotomic polynomials, hence defines a modular subgroup of $A(K)$. Reasoning similarly with τ, we get that there is a modular subgroup B of some model of ACFA extending (L_pM_p, ρ), which contains $Tor(A)$. This gives us the qualitative version of Manin-Mumford conjecture: we have shown that $Tor(A) \cap X$ is a finite union of cosets of the torsion subgroups of some connected algebraic subgroups of A. This fact is used in the proof.

Unfortunately, we do not know a priori that the constant m of Serre's result has an effective bound. This means that we do not know a bound on the complexity of the set B defining our modular subgroup, and hence cannot derive a bound on the number of irreducible components of the σ-closed set $B \cap X$. However, we do have explicit bounds (depending on p and ℓ) on the number of cosets appearing in the decompositions of $Tor_{p'}(A) \cap X$ and $Tor_{\ell'}(A) \cap X$, and this will be enough to apply the strategy alluded to at the end of (7.12).

7.15. **The reduction to the semi-abelian variety case**. We will state here the two results which are needed to reduce the problem from the commutative algebraic group A to the semi-abelian variety A/V. We will not state the model-theoretic result in its full generality, only the particular case that is of interest to us.

Definition. Let A be a commutative algebraic group, V its maximal vector group. We call a subvariety X of A *special* if $X = Y + C$, where Y is a subvariety of V, and C is a coset of a (connected) algebraic subgroup E of A.

We call a definable subset D of $A(K)$ *special*, if $X = Y + C$, where Y is a definable subset of $V(K)$, C is a coset of a definable subgroup of $A(K)$.

7.16. **Proposition**. Let A be a commutative algebraic group, and V its maximal vector subgroup, $\pi : A \to A/V$. Let B be a definable subgroup of $A(K)$ of finite SU-rank, and assume that $\pi(B)$ is modular. Then every definable subset of B is a Boolean combination of special sets.

The proof uses the following crucial ingredients:

(1) The fact that any definable subset of $Fix(\sigma)^n$ is definable with parameters from $Fix(\sigma)$ (see 4.3).
(2) The stability and the modularity of $\pi(B)$ with the structure induced by K.
(3) The fact that $B \cap V$ is strongly related to $Fix(\sigma)$. [In fact, there is a definable bijection between $B \cap V$ and $Fix(\sigma)^k$]
(4) The fact that any definable subset of $(V \cap B) \times \pi(B)$ is a Boolean combination of "rectangles", i.e., sets of the form $U_1 \times U_2$ where U_1, U_2 are definable and included in $B \cap V$ and $\pi(B)$ respectively.
(5) If Y is a definable subset of B, then there is a group H, contained in $(Y \cdot Y^{-1})^n$ for some n (and hence definable), such that YH/H is finite. This is a property of groups of finite SU-rank.

7.17. **Corollary**. Let B be as above, and X a subvariety of A. Then $X \cap B$ is contained in a finite union of finitely many special varieties which are contained in X.

Proof. Go to the Zariski closure of $X \cap B$.

7.18. **Lemma**. Let A be a commutative algebraic group, T the group of torsion points of A (or the group of torsion points of order prime to p, for some prime p), and assume that $X \cap T$ is contained in the union of the special subvarieties D_i of X, $i = 1, \ldots, M$. Then the Zariski closure of $X \cap T$ is the union of at most M cosets of connected algebraic subgroups of A.

Proof. It is enough to show that if D is a special subvariety of X, then the Zariski closure of $D \cap T$ is a coset of a group subvariety of A.

Write $D = C + Y$, where C is a coset of the connected group variety E, and Y is a subvariety of V. We will first show that we may assume that Y is contained in an algebraic subgroup V_1 of V which intersects E in (0). Indeed, because V is a vector space, there is a definable endomorphism $\pi : V \to V$, with $\pi^2 = \pi$ and $Ker(\pi) = V \cap E$. Then $E + Y = E + \pi(Y)$ because $Ker(\pi) \subseteq E$, and $C = C + E$ because C is a coset of E. Therefore

$$D = C + Y = C + E + Y = C + E + \pi(Y) = C + \pi(Y),$$

and we may replace Y by $\pi(Y) \subseteq \pi(V) = V_1$, and $V_1 \cap E = (0)$.

Fix $d_0 \in D \cap T$, and for $d \in D \cap T$ define $f(d) = d - d_0$. Then $f(d) \in (E + V_1) \cap T$. Write $f(d) = e + y$, with $e \in E$, $y \in V_1$. Since $f(d)$ is a torsion element and $V_1 \cap E = (0)$, we get that necessarily $y = 0$ (V has no torsion elements), so that $f(d) \in E$, and $d \in E + d_0$. Hence

$$D \cap T = (E + d_0) \cap T = (E \cap T) + d_0.$$

The only thing remaining to be shown, is that the Zariski closure B of $E \cap T$ is a connected subgroup of A. Let B^0 be the connected component of B. Because $E \cap T$ is divisible, $E \cap T$ has no subgroup of finite index, which implies that $B^0 \cap T = B$, so that $B = B^0$.

7.19. **Exercise 16**. Let (E, σ) be an algebraically closed difference field, let $m \geq 1$ and let (L, τ) be a difference field extending (E, σ^m)). For each $i = 1, \ldots, m-1$, choose L_i realising $\sigma^i(tp_{ACF}(L/E))$, linearly disjoint from the composite field of $L_0 = L, \ldots, L_{i-1})$ over E. Let $f_0 = id_L$, and for $i = 1, \ldots, m-1$ let $f_i : L \to L_i$ be an isomorphism extending σ^i. For $i = 0, \ldots, m-2$, define $\sigma_i : L_i \to L_{i+1}$ by

$$\sigma_i = f_{i+1} f_i^{-1}$$

and define $\sigma_{m-1} : L_{m-1} \to L_0$ by

$$\sigma_{m-1} = \tau f_{m-1}^{-1}.$$

(1) Show that the σ_i agree with σ on E.

(2) Show that $\sigma_{m-1} \cdots \sigma_0 = \tau$.

(3) Show that there is a difference field (M, σ) containing (E, σ) and such that M contains L, and σ^m agrees with τ on L.

(4) Deduce that if K is a model of ACFA, then $(K, \sigma^m \phi^n)$ is also a model of ACFA ($m \geq 1, n \in \mathbb{Z}$).

(5) Deduce that if K is a model of ACFA, and $F = Fix(\sigma^m \phi^n)$, then F is a pseudo-finite field.

(6) Let F be as in (5). Show that every definable (in K) subset of F^k is definable with parameters from F. If furthermore $m = 1$, then show that the structure induced on F is the pure field structure. [Repeat the proof of Proposition 4.3. This result does not extend to the case $m > 1$, as σ defines then an automorphism of F, which is not definable in the pure field language.]

References

Algebraic results

[1] R.M. Cohn, Difference algebra, Tracts in Mathematics 17, Interscience Pub. 1965.

[2] S. Lang, Introduction to algebraic geometry, Addison-Wesley Pub. Co., Menlo Park 1973.

Model theoretic results on difference fields

[3] A. Macintyre, Generic automorphisms of fields, APAL 88 Nr 2-3 (1997), 165 – 180.

[4] Z. Chatzidakis, E. Hrushovski, Model theory of difference fields, Trans. Amer. Math. Soc. 351 (1999), pp. 2997-3071.

[5] Z. Chatzidakis, E. Hrushovski, Y. Peterzil, Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics, preprint 1999. To appear in Proc. of the LMS

[6] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, APAL 112 Nr 1 (2001), 43 – 115.

[7] E. Hrushovski, The first-order theory of the Frobenius, preprint (1996).

[8] A. Macintyre, Nonstandard Frobenius, in preparation.

The papers [5] to [7] definitely fall into the category of "further advanced reading". Some of the easy parts of [6] appear in survey papers, see below.

Related model-theoretic results on finite fields.

[9] J. Ax, The elementary theory of finite fields, Annals of Math. 88 (1968), 239 – 271.

[10] E. Hrushovski, Pseudo-finite fields and related structures, manuscript 1991.

[11] E. Hrushovski, A. Pillay, Groups definable in local fields and pseudo-finite fields, Israel J. of Math. 85 (1994), 203 –262.

[12] E. Hrushovski, A. Pillay, Definable subgroups of algebraic groups over finite fields, J. reine angew. Math. 462 (1995), 69 –91.

The proofs of many of the results of the first few chapters of these notes are essentially translations of proofs appearing in [10]. See also [11]. In [12], one uses results of [11] to obtain very pretty results on groups definable in finite fields.

Other model-theoretic results

[13] L. van den Dries, K. Schmidt, Bounds in the theory of polynomials rings over fields. A non-standard approach. Invent. Math. 76 (1984), 77 – 91.

[14] U. Hrushovski, A. Pillay, Weakly normal groups, in: Logic Colloquium 85, North Holland 1987, 233 – 244.

[15] B. Kim, A. Pillay, Simple theories, APAL 88 Nr 2-3 (1997), 149 – 164.

[16] A. Pillay, Definability and definable groups in simple theories, JSL 63 (1998), 788 – 796.

Stability is a vast subject, with an abundant literature. Here are some books for the interested reader, but there are many others.

[17] S. Buechler, Essential stability theory, Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1996.

[18] A. Pillay, An introduction to stability theory, Oxford Logic Guide 8, Clarendon Press, Oxford, 1983.
[19] F. Wagner, Simple theories, Kluwer Academic Pub., Dordrecht 2000.

Survey papers

[20] E. Bouscaren, Théorie des modèles et conjecture de Manin-Mumford, [d'après Ehud Hrushovski], Séminaire N. Bourbaki exposé 870 (Mars 2000), to appear in Astérisque.
[21] Z. Chatzidakis, Groups definable in $ACFA$, in: Algebraic Model theory, B. Hart et al. ed., NATO ASI Series C 496, Kluwer Academic Publishers 1997, 25 – 52.
[22] Z. Chatzidakis, A survey on the model theory of difference fields, Proc. Workshop, Haskell, Pillay, Steinhorn Ed., MSRI Publications **39**, Cambridge University Press, 65 – 96.
[23] A. Pillay, $ACFA$ and the Manin-Mumford conjecture, in: Algebraic Model theory, B. Hart et al. ed., NATO ASI Series C 496, Kluwer Academic Publishers 1997, 195 – 205.

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